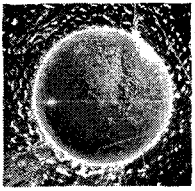
МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА:
сучасні виклики та загрози

Міжнародна інформаційна безпека:
СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ



Київ
"Центр вільної преси"
2006

УДК 327.5+351.746.1
ББК 4239
М43

Рекомендовано
до друку Вченою Радою Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка
(протокол №5 від 29 листопада 2006 р.)

Рецензенти: доктор політ. наук, професор Б.І. Канцелярук
Інститут світової економіки і міжнародних відносин НАН України;
доктор політ. наук, професор Г.М. Перепелиця
Інститут зовнішньої політики Дипломатичної академії України при МЗС України.

М43 **Міжнародна інформаційна безпека: сучасні виклики та загрози.** – К.: Центр вільної преси, 2006. – 916 с.
ISBN 966-7181-95-2

Колективна праця присвячена проблемам теорії і практики міжнародної інформаційної безпеки та протидії маніпулятивним технологіям у сфері зовнішньої політики. У праці представлено наукові дослідження, в яких висвітлюються стан і тенденції розвитку міжнародної системи підтримання миру в інформаційному суспільстві, планування і здійснення спеціальних інформаційних операцій, сутність і методи протидії маніпулятивним технологіям, прикладні аспекти інформаційної безпеки у різних сферах суспільного життя.

Видання продовжує наукову серію "Інформаційне суспільство, політика, право", до якої входять дослідження з актуальних проблем міжнародних інформаційних відносин. Для науковців, викладачів, аспірантів, фахівців з інформаційної безпеки, парламентарів, урядовців, представників мас-медіа.

УДК 327.5+351.746.1
ББК 4239

ISBN 966-7181-95-2

ПЕРЕДМОВА

Політика безпеки у сучасному світі: феномени інформаційної доби

Інформаційна безпека належить до тих різновидів безпеки, де національний та інтернаціональний моменти нерозривно пов'язані між собою. Це означає, що йдеться про той вид національної безпеки, який водночас є суто національним й відносно наднаціональним за своїм змістовним наповненням й за своїми формами, забезпечуючи таким чином самозбереження нації та її прогресивний розвиток на шляхах розвитку інформаційного довкілля у його глобальному контексті.

Президент України Віктор Ющенко, виступаючи на медіа-форумі "Україна на інформаційній карті світу" 15 листопада 2006 року, виважуючи "полюси загроз і можливостей" сучасного світу, особливо виокремив проблему інформаційного суспільства: "Світ XXI століття існує поміж двох полюсів загроз і можливостей, які за своєю глобалізованою природою вимагають реакції кожного - від найвпливовіших до найменших учасників міжнародних відносин. Широке поле загроз формують разюча нерівномірність світового розвитку, політична і безпекова нестабільність, масштабний виклик тероризму, рецидиви силового мислення часів "холодної війни". У площині можливостей постають міжнародні об'єднавчі процеси, глобальне поширення принципів демократії, вдосконалення норм економічної кооперації, інтегральне усвідомлення світовою спільнотою відповідальності за соціальні, гуманітарні та екологічні проблеми планети. На тлі цих явищ роль

України заслуговує на зважену і об'єктивну оцінку. В тому числі - з точки зору інформаційного суспільства".

Світове співтовариство визнало факт існування глобальної проблеми міжнародної інформаційної безпеки, у системі якої ключове значення має фундаментальна проблема обмеження військового застосування досягнень науки й техніки. Особливо негативну роль відіграють чисельні факти військового застосування спеціальних інформаційних засобів, які часто називають "інформаційною зброєю". За наявними даними, така зброя розробляється в 120 країнах (тоді як розробки у сфері ядерної зброї ведуть не більше 20 країн). Деякі країни відкрито проголосили курс на ведення "інформаційних війн", створивши із цією метою спецпідрозділи в структурі збройних сил.

Існують різні підходи до розуміння й розв'язання проблем міжнародної інформаційної безпеки. Один із них зводить суть справи до боротьби зі злочинністю в інформаційній сфері, ігноруючи при цьому факти існування "інформаційної зброї" і ведення інформаційних спецоперацій з її застосуванням, тобто суто військовий аспект проблеми. Ймовірно, у цьому випадку йдеться про те, щоб уникнути міжнародно-правових обмежень в процесі розробки й застосуванні засобів "інформаційної війни", у чому зацікавлені розвинені країни світу.

Інший підхід, більше властивий країнам на шляху розвитку ("третього світу") констатує реальну загрозу розв'язання "інформаційних війн", але пропонує ідеалістичний варіант повної заборони "інформаційної зброї".

Третій підхід пропонує системне збалансоване вивчення проблеми міжнародної інформаційної безпеки із виокремленням її аспектів військового й цивільного.

Актуальними проблемами міжнародної інформаційної безпеки є:

- формування належної соціальної бази інформаційної безпеки та подолання інформаційної нерівності із нерівністю освітньою включно;
- практична реалізація потенційних можливостей інформаційної безпеки для різних соціальних верств населення з метою забезпечення їхньої нормальної діяльності й інтеграції у світову систему;
- ефективне використання національних й наднаціональних структур інформаційної безпеки у системі вільного міжнародного обміну інформацією й знаннями, співробітництва в різних сферах життя з метою формування міжнародного клімату взаєморозуміння й довіри й попередження міжнародних та регіональних конфліктів;
- переорієнтація систем інформаційної безпеки від виконання завдань суто охоронних й захисних на завдання конструктивної модернізації структур національної свідомості й формування єдиної планетарної свідомості як "інфраструктури" збереження цивілізації й забезпечення виживання людства.

Серед нових міжнародних реалій безпеки - якісно нове бачення архітектури міжнародної безпеки під впливом подвійного використання інформаційно-комунікаційних технологій, зокрема, маніпулювання, викривлення інформаційної реальності, деструктивне використання соціальних комунікацій, невизначеність правового поля інформаційної безпеки, інформаційний тероризм.

Один із сумних уроків 11 вересня 2001 року полягає, напевно, в тому, що міжнародний тероризм з усіма його "національними відгалуженнями" має на меті, передусім, маніпулювання масовою свідомістю, активно експлуатуючи передусім національні й цивілізаційні соціальні стереотипи. А тому самоочевидною є необхідність поглибленого дослідження природи та технологій психологічних маніпулятивних впливів, що передбачає постановку низки дедалі конкретніших завдань у напрямі розкриття змістовних особливостей як дозволених, так і недозволених, як прийнятних, так і неприйнятних маніпуляцій та способів їх нейтралізації й знешкодження. Йдеться про процес сходження від абстрактного до конкретного, який насправді може означати плідний союз теорії з практикою.

Найдемонстративніші прийоми маніпулювання у міжнародних відносинах пов'язані із застосуванням "політики батога і пряника". Йдеться про різноманітні форми несанкціонованих міжнародним правом та усталеною міжнародною практикою винагород або покарань задля якомога ефективнішого впливу на рішення, дії і поведінку лідерів й провідних політичних сил окремо взятих країн і навіть цілих регіонів світу. На одному кінці цієї маніпулятивної шкали, - погрози, залякування, тиск на лідера і його оточення (компромат, карикатуризація, демонізація і т.п.), використання інших прийомів "чорного PR". На іншому, - улесливі характеристики, політичні аванси, запрошення на престижні форуми і зустрічі "без краваток", присудження міжнародних премій тощо.

Однак, далеко не всі маніпуляції можна визнати шкідливими й тим паче "терористичними". Саме тому надзвичайно важливо досліджувати маніпуляції не абстрактно, а в конкретних ситуаціях й сферах комунікацій як традиційного, так і нетрадиційного типу, - політичній, релігійній, педагогічній тощо, а також у контекстах тих соціальних процесів та явищ, які нині зазнають бурхливих перетворень в українському суспільстві за умов його демократизації.

Мішенню маніпуляцій, як відомо, є стереотипи почуттів, мислення й поведінки, завдяки яким відбувається необхідне ущільнення інформаційних та ідеологічних процесів у свідомості. Вони відображають типове емоційне настановлення людини до певних об'єктів і явищ. Йдеться, власне, не тільки про інформацію і мислення, а про складний соціально-психологічний процес на багатьох рівнях та у багатьох вимірах світосприймання сучасної людини.

Специфіка маніпулювання стереотипами розкривається через активне використання соціальних стереотипів, які реально існують в суспільстві у вигляді спрощених схематизованих уявлень про соціальні об'єкти, усталених уявлень певних соціальних груп про предмети, факти та події дійсності. Зазначимо, що нинішні міжнародні ЗМІ втратили здатність бути засобом діалогу для різних суспільств та держав й дедалі частіше виконують суто пропагандистські ролі, маніпулятивний "рефлекс" також властивий багатьом вітчизняним ЗМІ, що значною мірою знижує позитивні ефекти свободи слова, здобутої ними після подій на Майдані.

Цензура у її найбільш демонстративних формах типу сумнозвісних "темників", практично зникла, але не зник маніпулятивний стиль вітчизняних засобів масової інформації, що сприяло значному зниженню потягу масової ауди-

торії до самостійного критичного мислення. Суспільству пропонується символічна політика у коментарях ЗМІ, що призводить до виняткового споглядання політичних "шоу", пасивного відстеження подій та відчуження суспільства від активної політичної діяльності.

Потрібно визнати, що ЗМІ не можуть функціонувати в суспільстві без наперед визначених правил виробництва "штучної реальності", тому скасувати правила, керуючись етичними принципами, навряд чи можливо за умов, коли існують реально багатомільйонні суспільства "масового споживання", коли фактом життя стали потужні економічні і технологічні ринки, коли об'єктивною реальністю став тісний взаємозв'язок економіки і держави, коли прихована керованість суспільною думкою за участю ЗМІ перетворилася у факт реального життя, який доводиться брати до уваги так само, як береться до уваги ринкова конкуренція, чесні (або нечесні) парламентські вибори, глобалізація тощо. Інша річ, що "брати до уваги" не означає миритися із тими факторами, які створюють реальні загрози національній та міжнародній інформаційній безпеці.

Невизначеність правового поля міжнародної інформаційної безпеки зумовлює недостатню опрацьованість як національних, так і міжнародних правових систем у сфері інформаційного права, враховуючи, що ця галузь права переживає початковий етап формування. Причому інститути інформаційного права формуються не ізольовано, а на засадах систематизації й розвитку різноманітних норм галузевого права, що регулюють інформаційні правовідносини у всіх без винятку сферах життєдіяльності суспільства. В правотворчий процес інтенсивно залучені інституції міжнародного права, що підтверджують, зокрема, резолюції Генеральної Асамблеї ООН з проблематики міжнародної інформаційної безпеки.

Вимагає подальшого уточнення й міжнародно-правового закріплення поняття "інформаційна зброя", "інформаційні озброєння", "інформаційні війни", оскільки уже існує досвід застосування як "інформаційних озброєнь", так і здійснення спеціальних інформаційних операцій на підставі прогностичних оцінок можливих глобальних наслідків неконтрольованого використання наступальних озброєнь.

Так само юридичного оформлення потребує поняття "інформаційний тероризм", оскільки 11 вересня 2001 року стало справжньою точкою відліку нового XXI століття й дало підставу історію сучасного людства поділяти на два періоди - "довересневий" і "поствересневий", коли людство стало свідком жорстокої акції, яку фахівці окреслили як асиметричну відповідь на надзвичайну потугу єдиної поки що в сучасному світі наддержави.

Дипломатичні методи й засоби регулювання відносин інформаційної безпеки між державами передусім стосуються питань міжнародно-правових обмежень в сфері розробки й застосування деструктивних інформаційних впливів, розвитку організаційних структур забезпечення інформаційної безпеки, підготовки національних кадрів. Зрештою, йдеться про спільні дії у конкретних загрозливих ситуаціях.

Політика України у сфері міжнародної інформаційної безпеки вирізняється достатньо високою активністю й системністю, про що свідчать зовнішньо-

політичні ініціативи нашої держави, пропозиції, які вона вносить на форумах ООН та ЮНЕСКО. Ключове значення має офіційне визнання того очевидного факту, що інформаційні технології й засоби потенційно можуть бути використані як з метою забезпечення міжнародної стабільності й безпеки, так і з метою протилежною, спрямованою на примноження загроз і викликів.

Надзвичайно важливими уявляються передусім проблеми захисту соціуму від негативних впливів соціальних комунікацій діалогічного типу, бо саме з ними пов'язані сподівання на побудову в Україні інформаційного суспільства. Час інформаційної доби виразно вказує на разючі зміни архітектури світової безпеки, які потрібно аналізувати й прогнозувати із належними висновками щодо реальної політичної практики, оскільки йдеться про безпеку Українського суспільства й Української держави, про їхню ідентифікацію й самовизначення у бурхливому сьогоденні "нового світового порядку".

У такому суспільстві провідна роль належить особистості контрманіпулятивного типу із розвиненим критичним мисленням. Ростити й плекати таку особистість як необхідну передумову формування інформаційного суспільства є найпочеснішою місією освітньої системи й тієї її вершинної ланки, якою є університети сучасного типу.

Серед науково-дослідних установ й навчальних закладів України, які проводять дослідження й підготовку кадрів з питань інформаційної безпеки, чільні позиції посідає Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка. Дипломатичні, політичні, економічні, бізнесові, правові, науково-технічні, освітні, власне інформаційні, а також спеціальні методи й засоби забезпечення різноманітних аспектів інформаційної безпеки є предметом уваги кафедр Інституту.

Відтак, доречно ставити питання про практичне залучення і використання знань із досліджуваної проблематики, накопичених конкретними дисциплінами, що, у кінцевому підсумкові і визначить провідні вектори руху України до сучасного інформаційного суспільства.

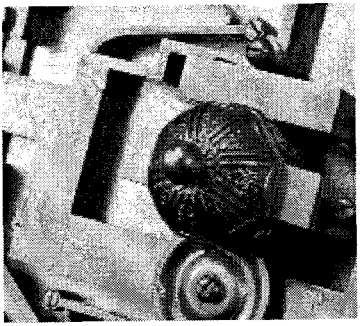
У пропонованій монографії досліджуються актуальні проблеми теорії і практики міжнародної інформаційної безпеки та протидії маніпулятивним технологіям у сфері зовнішньої політики, висвітлюються стан і тенденції розвитку міжнародної системи підтримання миру в інформаційному суспільстві, планування, здійснення та протидія спеціальним інформаційним операціям, прикладні аспекти інформаційної безпеки у різних сферах суспільного життя.

Автори сподіваються, що ця праця слугуватиме важливій справі підготовки фахівців в галузі міжнародної інформаційної безпеки, подальшій розробці проблем безпеки у сучасному світі.

Л.В. ГУБЕРСЬКИЙ,
директор Інституту міжнародних відносин
Київського національного університету ім. Тараса Шевченка, академік НАН України,
доктор філософських наук, професор.

РОЗДІЛ 1

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА: КОНЦЕПЦІЇ, ДОКТРИНИ, СТРАТЕГІЇ



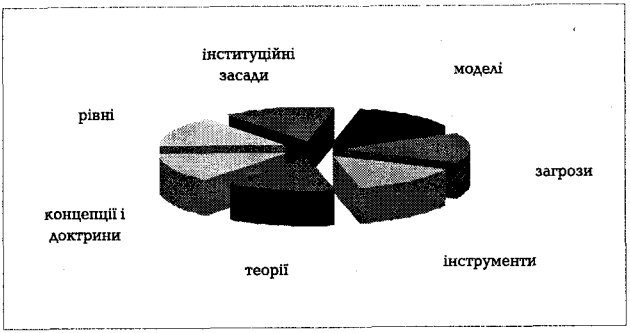
1.1. Міжнародна інформаційна безпека у глобальній системі підтримання миру і стабільності (концептуальний вимір)

У відкритому глобальному світі XX-XXI століття нові закономірності перебігу цивілізаційних процесів, вплив інформаційної революції та інших високих технологій на прискорену інтеграцію міжнародного співтовариства обумовлюють появу і необхідність вирішення нових проблем життєдіяльності людства, узгодження нових міжнародних принципів взаємодії та правил поведінки акторів міжнародних відносин.

Серед глобальних проблем сучасності, до яких привернуто увагу ООН, інших авторитетних міжнародних організацій (ОБСЄ, НАТО, ЄС), політичних лідерів, науковців, широкої громадськості, є проблема об'єктивного ускладнення структури міжнародних відносин, проникаючі контакти цивілізацій і відповідно проблема глобальної міжнародної безпеки, тобто підтримання сталого миру, попередження конфліктів, уникнення нової гонки озброєнь із використанням новітніх науково-технологічних досягнень.

Проблеми глобальної безпеки посідають особливе місце в структурі міжнародної інформаційної політики, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світопорядку, реалізацію стратегій становлення глобального інформаційного (інтелектуального) суспільства, навіть саме існування цивілізації. Глобальна безпека як чинник міжнародних відносин, вплив якого має універсальний характер і врахування якого в діяльності міжнародного співтовариства та в зовнішній політиці окремих держав призводить до радикальних змін у поведінці акторів міжнародних відносин, до трансформації самої сутності проблеми безпеки після закінчення *"холодної війни"* і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах інформаційної складової міжнародної безпеки.

Структура міжнародної інформаційної безпеки охоплює: теорії, концепції, доктрини інформаційної безпеки, інформаційних воєн та інформаційних озброєнь; інституційні засади та моделі міжнародної інформаційної безпеки; інформаційні загрози та інструменти інформаційних атак (див. діаграма 1).



Теорії. Політичні та наукові дискусії щодо проблем глобальної безпеки відображені у працях Д. Гудбі, Г. Кісінджера, З. Бжезинського, А. Гора, У. Вейєрмейера, Дж. Ная, У. Оуенса, М. Клея, Д. Томаса, Б. Берковича, Л. Джонсона, Б. Шварца, Б. Бузана, А. Гіршмана, М. Хоффмана, Х. Ласвелла, С. Хатінгтона, В. Плетта, Дж. МакКінлі, К. Аннана, Б. Галі, У. Швартоу, С. Ланцова, П. Циганкова, М. Лукашука, Є. Камінського, Б. Канцелярука, Г. Перепелиці, І. Ніколаєнка, М. Ожевана, А. Гуцала, Г. Почепцова, В. Бруза, М. Лебедєвої, О. Расторгуєва, А. Крутских, Г. Хозіна, В. Манжоли, М. Білоусова, І. Бінька, О. Литвиненка, О. Бодрука, Ю. Мацейка та ін. виявили наявність широкого діапазону нових загроз, джерела яких перебувають поза межами національних кордонів і за своїми характеристиками переважають можливості протидії суверенних держав [1-26].

Теоретичною базою концепції глобальної безпеки в інформаційну добу є теорії сталого миру, що орієнтують міжнародне співтовариство в умовах триваючого процесу глобалізації та розширення можливостей міжнародного співробітництва на попередження загрозливих конфліктних ситуацій на всіх рівнях – глобальному, регіональному і національному. Провідна ідея концепції – врахування всіх конструктивних ініціатив, філософських і політичних принципів, морально-етичних цінностей, релігійних і суспільних норм різних цивілізацій у забезпеченні існування і життєдіяльності людства. В концепції глобальної безпеки виділяються такі компоненти, як політичний, економічний, інформаційний, військовий, гуманітарний, екологічний, антитерористичний, зважаючи, що кількість цих компонентів та їх важливість і пріоритетність для міжнародного співробітництва трансформується відповідно до стану миру, суспільного розвитку, вдосконалення науково-технологічного прогресу, досвіду міжнародної інтеграції, визначення нової типології загроз.

Так, у концепції глобальної безпеки, яку викладено в науковому дослідженні американського політолога Д. Гудбі "Europe Undivided. The New Logic of Peace" (Wash., 1998), запропоновано наступну класифікацію стану миру:

1) нестабільний мир ("холодна війна"), досвід якого полягає в детальному аналізі співвідношення сил у світі, стриманості у кризових ситуаціях, у пошуку консенсусу з політичних, військових, економічних, гуманітарних позицій;
2) обумовлений мир (напружена конфліктна взаємодія між державами), в якому усвідомлення глобальних загроз має вирішальне значення для попередження конфліктів. З огляду на особливості історичного розвитку держав, що становлять сучасну систему міжнародних відносин, їх політичну культуру та ідеологію, суспільну свідомість, формування глобальної безпеки і стабільності має, до деякої міри, прогностичний характер;
3) сталий мир (забезпечення глобальної безпеки), при якому жоден з акторів міжнародних відносин не розглядає використання силових принципів переваги як засіб вирішення конфліктів і попередження загроз. Дж. Гудбі підкреслює, що на початку XXI століття концепція "сталого миру" стане реальністю для держав західної моделі цивілізації, близьких за політичними стратегіями і політичними процедурами державних інститутів, які входять до відомих у системі міжнародної безпеки воєнних блоків *НАТО, АСЕАН, ЗЕС/ЄС, АНЗЮС.*

Поділяючи погляди на класифікацію Дж. Гудбі, все ж необхідно підкреслити відносність положень про незастосування силових методів розв'язання або попередження міжнародних конфліктів.

Більшість дослідників вважає, що глобальна система міжнародних відносин буде розвиватися під впливом різнопланових факторів: "шестиполюсного світу" з центрами сили у США, Європі, Китаї, Японії, Росії, Індії (Г. Кіссінджер, М. Лібіцкі), трансформації і протиборства цивілізацій на основі концепції національної і культурної самобутності (С. Хантінтон), "однополюсного світу" (американоцентристська модель) як визнання лідерства США у становленні нового глобального світопорядку (Б. Бузан, А. Гіршман, З. Бжезинський), впровадження концепції "*м'якої сили*" (soft power) як інструменту вирішення майбутніх конфліктів (Б. Беркович Л. Джонсон Р. Шафрански, Дж. Най, У. Оуенс, О. Шерман), безконфліктності міжнародного розвитку і відмови від доктрини раціональності воєн і збройних конфліктів, забезпечення транспарентності всієї системи міжнародних відносин та її складових ресурсів для безпечного і безупинного прогресу глобальної спільноти (К. Аннан, Ф. Фукуяма, Ч. Шаохуа, Р. Інглегарт).

Концепції, доктрини. Суперечливі тенденції світових інтеграційних процесів, вибух етнічних, соціальних та інших конфліктів як міжнародних загроз спричиняють проблеми у визначенні еволюції змісту і характеру глобальної безпеки, потребують перегляду підходів до засобів підтримання міжнародного миру. Політичні дискусії в рамках ООН (Рада Безпеки, ГА ООН, Перший комітет ГА ООН, Конференція із роззброєння) засвідчили посилену ува-

гу міжнародного співтовариства до концепції стратегічної стабільності XXI століття, пов'язаної з викликами інформаційної революції і впливом інформаційних чинників проблеми безпеки.

Об'єктивними передумовами таких дискусій були принципово нові потенціальні загрози для міжнародного миру, обумовлені науково-технологічним прогресом та глобальною взаємозалежністю всіх сфер життєдіяльності міжнародного співтовариства. Представники різних країн наголошували, що використання нових інформаційних технологій і засобів впливу високорозвинутих країн на менш технологічні країни світу призвело до зміни глобального і регіонального балансів сили, обумовило нові сфери конфронтації між традиційними і новими центрами глобального протистояння, уможливило досягнення переваг в інформаційних технологіях і засобах маніпулювання суспільною свідомістю для широкомасштабної експансії із застосуванням не обмежених міжнародним правом видів озброєнь. Разом з тим, зазначалося на сесії, до нових інформаційних видів зброї проявляють інтерес як політичні угруповання, так і терористичні та кримінальні організації, що загрожує новим витком гонки озброєнь, втратою міжнародних ресурсів для вирішення глобальних проблем бідності, стихійних лих, техногенних катастроф, голоду, епідемій тощо [27].

За останнє десятиріччя XX століття міжнародне співтовариство усвідомило на прикладі спеціальних інформаційних операцій, в тому числі військових (в умовах збройних конфліктів "Морський ангел", 1991 р.; "Буря в пустелі", 1991-1992 рр.; "Відродження нації", 1992 р.; "Грім у пустелі", 1993 р.; "Об'єднаний щит", 1995 р.; "Спільні зусилля", 1996 р.; "Лис у пустелі", 1998 р.; "Союзницька сила", 1999 р.; "Помста" 2001 р.; "Шок і тремтіння" 2003 р. тощо), сутність реальних загроз інформаційного протиборства, визначило підходи до розуміння концепції міжнародної інформаційної безпеки, до дилеми війни і миру в інформаційну добу. Свідченням цього розуміння став запропонований Генеральним секретарем ООН Б. Бутросом Галі у 1992 році "Порядок денний для миру" (нова система глобальної безпеки), який містив концепцію превентивної дипломатії, миротворчості, підтримання миру і миробудівництва в постконфліктний період як першоджерело міжнародної інформаційної безпеки.

Доктрина превентивної дипломатії передбачає широкий спектр заходів, спрямованих на попередження і врегулювання конфліктів на основі інформаційно-аналітичного забезпечення прийняття рішень з проведення переговорного процесу, превентивного розгортання контингентів, створення демілітаризованих зон та відновлення демократичних інститутів. Інформаційний фактор доктрини визначає можливість превентивних заходів ООН лише за умови забезпечення об'єктивної, наукової, аналітично достовірної інформації і врахування та детального вивчення політичних, економічних і соціальних тенденцій в світі та регіонах, що можуть призвести до кризових ситуацій.

За змістом і характером заходи превентивної дипломатії поділяють на політичні, економічні, дипломатичні, воєнні, гуманітарні. Серед політичних заходів інформаційної безпеки – з'ясування односторонніх та багатосторонніх інтересів шляхом обміну інформацією та проведення переговорів; об'єктивне висвітлення сутності конфліктів та кризових проблем засобами масової комунікації; створення умов для професійної діяльності ЗМК у зонах напруженості для забезпечення достовірною інформацією міжнародного співтовариства і формування відповідної світової думки; інформаційне супроводження політичних (референдумів) та виборчих процесів, проведення аналітичних моніторингів за дотриманням основних прав і свобод людини; інформаційні контакти з опозиційними групами, неурядовими організаціями з метою ефективності досягнення консенсусу між сторонами протиборства.

Інформаційні чинники економічних заходів передбачають надання матеріальної та фінансової допомоги вільним і незалежним (опозиційним) засобам масової комунікації, забезпечення інформаційної безпеки національних інституціональних мереж та систем, виявлення економічних факторів впливу на перебіг кризових процесів. Специфіка дипломатичних заходів полягає у вивченні інформації про ситуацію в зоні конфлікту, в інформаційному супроводженні переговорів, в тому числі обмін інформацією дипломатичного характеру, поширення позиційних матеріалів у міжнародних інформаційних потоках та проведення інформаційних кампаній в країнах перебування з метою інформування дипломатичного корпусу інших країн та міжнародної спільноти про врегулювання конфлікту.

Військовий аспект превентивної дипломатії включає такі інформаційні аспекти, як обмін інформацією військового призначення, створення запобіжних систем від несанкціонованого втручання в автоматизовані (комп'ютерні) системи управління військами та військовою технікою, проведення навчань з інформаційних операцій; забезпечення відновлення демократичних прав і свобод у постконфліктний період.

Суто інформаційними факторами превентивної дипломатії вважаються аналіз багатоаспектних даних про потенційні або триваючі конфлікти, підготовка рекомендацій для прийняття рішень на рівні Ради Безпеки ООН, реалізація прийнятих рішень у формі міжнародних механізмів врегулювання конфліктів, впровадження ідеї толерантності і культури миру в міжнародних відносинах.

Практика діяльності ООН у напрямку застосування заходів превентивної дипломатії виявила необхідність з'ясування як теоретичних, так і прикладних підходів до встановлення глобальної безпеки і сталого миру, обумовила розгляд проблеми інформаційної безпеки на рівні міжнародних універсальних, міжурядових регіональних організацій та національних інститутів [28].

Зважаючи на глобальність проблеми інформаційної безпеки, розвинуті країни розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту критично важливих інформаційних структур, а з

1996 року проблему міжнародної інформаційної безпеки було винесено на політичний та міжнародно-правовий рівень:

а) концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 р.);

б) у спільному комюніке зустрічі на найвищому рівні США – Російська Федерація було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної складової глобального процесу інформатизації;

в) на 53-ій сесії ГА ООН було консенсусом прийнято резолюцію 53/70 від 4 грудня 1998 р., в якій зазначалося, що міжнародне співтовариство визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у глобальному світі. Зокрема, в Резолюції 53/70 пропонувалося державам-членам ООН розглянути конкретну типологію інформаційних загроз, визначити критерії проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем, внести пропозиції до комплексної доповіді Генерального секретаря ООН для створення міжнародного механізму протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн.

Термінологія. Під час дискусій та розгляду прикладних аспектів міжнародної інформаційної безпеки було визначено специфіку, істотні характеристики та типологію інформаційних загроз, узгоджено термінологію та зміст основних понять в новій сфері міжнародного співробітництва.

"***Міжнародна інформаційна безпека***" класифікується як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз.

"***Інфосфера***" визначається як міжнародний інформаційний простір, що охоплює інформаційні потоки, інформаційні ресурси та всі сфери життєдіяльності цивілізації.

"***Міжнародні інформаційні операції***" характеризуються як форма міждержавного протиборства, яка реалізується з використанням інформаційного впливу на системи управління різного призначення інших держав, а також на політичну владу і суспільство в цілому, на інфраструктуру і засоби масової комунікації для досягнення переваги і кінцевої мети інформаційної операції з одночасним захистом національної інфосфери від аналогічних дій.

"***Інформаційна війна***" розглядається як інформаційне протиборство з метою впливу на критично важливі структури противника, зруйнування політичної та соціальної систем, а також для дестабілізації суспільства і державності противної сторони.

"***Інформаційна зброя***" визначається як комплекс технічних та інших заходів, методів і технологій, спрямованих на встановлення контролю над

інформаційними структурами потенційного противника, втручання у роботу його систем управління, інформаційних мереж та комунікацій з метою знищення або модифікації даних, дезінформації, поширення інформації спеціального призначення у системах формування громадської думки і прийняття рішень, а також як сукупність засобів впливу на свідомість і психологічний стан політичних і військових структур, спецслужб та населення для протидії можливим інформаційним впливам іншої сторони. Конкретизація цих понять зумовлена потребою подальшого дослідження проблеми глобальної інформаційної безпеки.

Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації комунікації як: у більшості індустріально розвинутих країн проводяться дослідження і розробки нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках прямо впливати на них. За даними аналітичних центрів США, розробки такої зброї ведуться в 120 країнах світу: для порівняння розробки в галузі ядерної зброї проводяться не більш, як в 20 країнах; в деяких країнах завершено розробку засобів інформаційного протиборства (війни) з можливим противником як в умовах воєнних конфліктів різної інтенсивності, так і у мирний час на стратегічному, оперативному, тактичному рівнях та в польових умовах з метою захисту національної інфосфери від агресії і несанкціонованого втручання; в розвинутих країнах концепція інформаційної війни є складовою воєнної доктрини, що обумовлює спеціальну підготовку особового складу і окремих підрозділів для проведення інформаційних операцій; практика міжнародних, регіональних та етнічних конфліктів виявила унікальність застосування інформаційної зброї для впливу на міжнародне співтовариство та для боротьби за геополітичні інтереси.

Здійснення інформаційних операцій та спеціального інформаційного супроводження воєнних конфліктів на Близькому Сході (Ізраїль — Палестина), в Південно-Східній та Центральній Європі (Югославія, Македонія, Косове), в Африці (Сьєрра-Леоне, Замбія, Сомалі, Ефіопія, Конго), в Азійсько-Тихоокеанському регіоні (Східний Тимор, Індія-Бангладеш, Китай-Тайвань), на території колишнього Радянського Союзу (Чечня, Молдова, Закавказзя) викликало політичні і громадські акції протесту, несанкціонований вплив на державні Internet-сайти тих чи інших країн, міжнародних організацій військового характеру з метою зруйнування або блокування стратегічних інформаційних мереж і систем.

За повідомленнями міжнародних інформаційних агентств Reuters, BBC, Wired News, Associated Press та ін., під час арабо-ізраїльської інформаційної війни з боку хакерів арабського світу було здійснено блокування і модифікація сайтів урядових структур, зламано системи захисту одного з основних Internet-провайдерів Ізраїлю Net Vision, який підтримує 70 відсотків мережевого трафіка країни: розгорнуто кампанію кіберджихаду для впливу на всю інфрас-

труктуру ізраїльського сегменту мережі Internet. З боку Ізраїлю було створено коаліцію Ізраїльське Інтернет-підпілля (Israel Internet Underground – IIU) для захисту національної інфраструктури від хакерської злочинності, запроваджено національний проект SODE для протиборства з пропалестинськими та арабськими організаціями, зокрема, з відомою пропалестинською хакерською організацією LG Force Pakistan.

Подібна ситуація склалася навколо проблеми Кашміру, де несанкціонована агресія проти сайтів урядових структур набула масового і загрозливого для функціонування державних інститутів Індії характеру і стала приводом для з'ясування відносин між Індією, Пакистаном та Бангладеш. Міністерство національної оборони Тайваню розпочало підготовку спеціальних заходів захисту інформаційних ресурсів від китайської експансії і прийняло програму спеціальної підготовки особового складу військ для інформаційного протиборства з Китаєм, зважаючи на численні порушення в інформаційному просторі країни.

Інтервенція CNN проти американського уряду та формування відповідної міжнародної громадської думки обумовили втручання США у внутрішні події в Сомалі ("Відродження надії" (1992 р.), "Спільний щит" (1995 р.), а засоби масової комунікації Югославії, застосовуючи доктрину вибіркового інформування, сприяли ескалації етнічного конфлікту на Балканах; інформаційна блокада щодо перебігу конфлікту в Чечні вплинула на характер рішень Ради Безпеки ООН, ОБСЄ та НАТО щодо Росії.

Істотні прояви інформаційних чинників міжнародної безпеки кардинально змінили оцінку доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал інформаційних загроз і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства.

Політичні дискусії на Міжнародному семінарі з проблем інформаційної безпеки (Женева, 1999 р.), який відбувся під егідою Інституту ООН з проблем роззброєння (ЮНІДІР) за участю департаменту з питань роззброєння Секретаріату ООН та представників більш як 50-ти країн світу, підтвердили актуальність проблеми та своєчасність її розгляду в рамках ООН. Проте у визначенні підходів до її вирішення виявилися різні позиції, які відповідали стратегічним інтересам учасників дискусії. Позиція розвинутих країн передбачала визнання проблеми міжнародної інформаційної безпеки як гіпотетичного силового протистояння; перенесення розгляду концепції міжнародної інформаційної безпеки на регіональний або тематичний рівень; виділення з комплексної проблеми міжнародної інформаційної безпеки таких складових, як кримінальні та терористичні міжнародні інформаційні загрози і створення міжнародного механізму контролю подібних інформаційних злочинів. Позиція країн, які не належать до західної моделі цивілізації, передбачала пропозиції щодо встановлення міжнародно-правової норми про заборону застосування засобів впливу на інформаційні ресурси та інформаційний потенціал

міжнародного, регіонального та національного призначення; створення спеціального Міжнародного суду з інформаційної злочинності; спільні розробки технології глобального захисту від інформаційної агресії. У Заяві міжнародної зустрічі було проголошено про узгодження Програми дій з попередження інформаційних війн та обмеження гонки інформаційних озброєнь [29].

Особливу позицію "наздоганяючого лідера" з проблеми міжнародної інформаційної безпеки зайняла Росія, представники якої активно лобіюють в ООН та інших міжнародних Форумах ініціативи щодо протидії потенційним загрозам нових інформаційних технологій, підкреслюючи новий фактор дисбалансу сил і домінування в глобальній інфосфері однієї країни (США) або альянсу країн (ЄС).

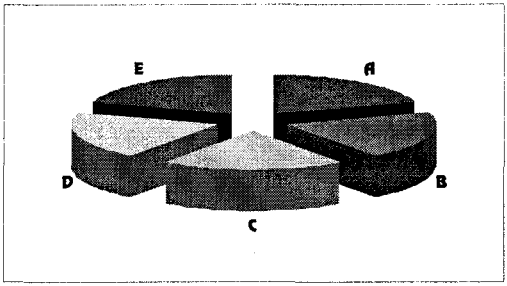
Суть пропозиції Російської Федерації – створення міжнародного механізму під егідою ООН та загальних принципів забезпечення міжнародної інформаційної безпеки, які були б закріплені поетапно в багатосторонній декларації, масштабній концепції міжнародної інформаційної безпеки, міжнародному договорі або конвенції комплексного характеру з врахуванням структури інформаційних загроз (військових, кримінальних, терористичних, цивільних).

Для реалізації пропозицій Росія запропонувала розробити систему понять для аналізу і обговорення проблеми, визначити технологічні джерела та характер інформаційних загроз; розробити основні принципи побудови глобальної системи міжнародної інформаційної безпеки; прийняти в рамках ООН багатосторонні декларації, конвенції з міжнародної інформаційної безпеки на основі розроблених принципів; узгодити принципи протидії міжнародному інформаційному тероризму та злочинності з принципами функціонування міжнародних організацій в галузі інформації, телекомунікацій, ЗМК та прав людини; розробити основні принципи для гармонізації національних законодавств з відповідною міжнародною нормою; розробити основні принципи організації механізму контролю безпеки міжнародної інфосфери та його взаємодію з міжнародними системами регулювання глобальної комунікації та економічного контролю (інформаційні продукти та послуги подвійного застосування, а також засоби для виробництва психотронної зброї); таким чином гарантувати міжнародному співтовариству вирішення нових складних проблем в добу становлення глобальної цивілізації та інформаційного суспільства і реальне забезпечення глобальної та міжнародної інформаційної безпеки.

Женевська зустріч (1999 р.) виявила стратегічну проблему міжнародної інформаційної безпеки – проблему домінування в глобальній інфосфері із застосуванням інформаційних озброєнь, тобто прагнення до контролю значних територій та соціумів, проблему інформаційного дисбалансу сил міжнародного світопорядку.

Моделі. Слід підкреслити, що стратегії глобального інформаційного протиборства лежать в основі аналітичних розробок дослідницьких інституцій

різних країн, метою яких є саме забезпечення інформаційного лідерства у сфері міжнародної безпеки. За результатами досліджень аналітики виділяють наступні моделі системи глобальної інформаційної безпеки (див. діаграма 2).



Модель А – створення абсолютної системи захисту країни-інфолідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Погляд на такий розвиток подій викладено у відомому дослідженні Дж. Ная та У. Оуенса "America's Information edge strategy and force planning", 1996 р. *("Головна сила Америки – її інформаційні можливості")*, в якому стверджується домінуюча роль США в інформаційній революції, тобто у використанні надважливих засобів комунікації та інформаційних технологій (супутникового спостереження, прямого мовлення, швидкісних комп'ютерів, унікальних можливостей в інтегруванні складних інформаційних систем), у політиці стримування і нейтралізації традиційних воєнних загроз та нових видів озброєнь.

У сучасному світі, де трансформовано поняття *"ядерної парасольки"* та стратегії неядерного стримування, зазначають автори дослідження, наявність інформаційних переваг обумовлює інтелектуальний зв'язок між зовнішньою політикою США та їх військовим потенціалом, збереження світового лідерства за допомогою нових засобів впливу та закріплення домінуючої ролі в альянсах і тимчасових коаліціях. Інформаційне лідерство посилює ефект американської дипломатії як інструменту "м'якої сили", уможливлює використання інформаційних ресурсів для конструктивного діалогу із потенційними противниками – Китаєм, Індією, Росією та іншими інформаційно розвинутими країнами з проблем міжнародної безпеки, і одночасно інфолідерство США забезпечує протидію нарощуванню інформаційних озброєнь в потенційно агресивних країнах (Іран, Ірак, Пакистан).

Переваги США в інфосфері, на думку експертів, сприятимуть попередженню і врегулюванню регіональних конфліктів, вирішенню проблем,

пов'язаних із глобальними загрозами, які виникли після закінчення "холодної війни", такими, як міжнародна злочинність, тероризм, поширення зброї масового знищення, глобальна екологічна деградація.

Концепція глобальної інформаційної безпеки з точки зору політичних інтересів США полягає у впровадженні доктрини "*інформаційної парасольки*", що замінить доктрину "ядерної парасольки", на основі взаємовигідного обміну інформацією різного характеру (переважно військового) для міжнародного співробітництва і підтримання миру.

В умовах сучасної інформаційної революції переваги "*м'якої сили*" США, вважають Дж. Най та У. Оуенс, можуть бути використані для остаточного становлення демократичної системи в інших країнах світу, для попередження регіональних конфліктів, для протидії новим загрозам глобального масштабу. Разом з тим, у дослідженні підкреслено концептуальні проблеми осмислення міжнародної інформаційної безпеки:

1) психологічний стереотип політичних, ділових та військових сил і коаліцій, що не дозволяє якісно оцінити роль інформації як сили, оскільки такі традиційні фактори, як військовий потенціал, ВНП, чисельність населення, енергетичні ресурси, розмір території та наявність природних запасів копалин домінують у дискусіях про баланси сил;
2) нерозуміння природи інформації, наслідків інформаційної інтеграції та системних зв'язків інформаційної складової з іншими військовими, політичними, економічними, соціальними складовими, що утворюють міць держави і суспільства;
3) усвідомлення у США та інших інформаційно розвинутих країнах стратегічної ролі міжнародної інформаційної безпеки та непередбачуваних наслідків застосування інформаційних озброєнь для існування цивілізації [30].

Модель В – створення значної переваги держави – потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту держави-противника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації будь-яких джерел і типів інформаційних загроз.

Практичне втілення другої моделі спостерігається в перебігу інформаційної операції "Союзницька сила" (1999 р.), яку США та країни-члени НАТО здійснили проти Союзної Республіки Югославії. Більшість експертів, які аналізували конфліктну ситуацію, підкреслюють формування безпрецедентної за масштабами системи управління інформаційними потоками для проведення військових операцій (спроможність надавати розвідувальну інформацію безпосередньо кожному з учасників бойових дій), масованих пропагандистських кампаній з широким спектром інформаційних методик (від технологій PR для формування сприятливої світової громадської думки, вибіркового інформування із заданим ефектом сприйняття контенту до

всебічної дискредитації політики противника, і навіть відвертої дезінформації світової громадськості), спрямованого інформаційно-психологічного впливу (основні завдання психологічних операцій здійснювали спецпідрозділи армії США, які брали участь у всіх міжнародних інформаційних операціях останньої чверті XX століття), потужного використання Internet та комп'ютерного протиборства для модифікації національного інформаційного простору і контролю за інфоінфраструктурою Югославії. Нові стратегії і тактика проведення інформаційних операцій, продемонстровані США та їх союзниками по НАТО на Балканах, засвідчили як могутність інформаційних озброєнь розвинутих країн, так і необхідність міжнародного вирішення проблеми інформаційної безпеки [31].

Модель С – наявність кількох країн – інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Дослідження ЦРУ 90-х років та на перспективу до 2020 року визначали як основні джерела загроз в кіберпросторі для США тільки дві країни – Росію і Китай. У новій військовій доктрині збройних сил США (Концепція Force XXI, 1996 р.), де було запропоновано дві складові театру воєнних дій – традиційний простір і кіберпростір, основними об'єктами впливу, крім відомих у теорії війн, стали інформаційна інфраструктура і психологічна сфера (human network) потенційного противника.

На сучасному етапі експерти США відзначають, що стратегію різних видів інформаційних операцій, спрямованих проти країни, планують і здійснюють більше 20 країн світу, а конфронтуючі зі США держави включають інформаційну війну у свої воєнні доктрини. Тому стратегія "Force XXI" як фактор стримування експансії в міжнародному інформаційному просторі виступає інструментом інформаційної переваги США в потенційному глобальному протиборстві [32].

Модель D – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій.

Завершення доби *"холодної війни"* та постхолодного миру і початок нової тривалої доби цивілізаційного стримування впливає на трансформацію традиційної конструкції міжнародної безпеки, що полягає у превентивних інформаційно-силових стратегіях, у посиленні контролю над глобальними фінансовими потоками у зміні структури союзників, а також в інформаційно-психологічному впливі на політичні еліти учасників конфлікту.

На стратегічному рівні мета сучасних інформаційних операцій – це формування нової системи міжнародних відносин і запобігання ефективному використанню інформаційних систем у процесах прийняття військових рішень та координації воєнних дій. Театр інформаційних операцій в умовах постбіполярного миру включає різнорівневий вплив на системи забезпечення учасників конфлікту: блокування рахунків та руху платежів у міжнародних банківських інститутах, вплив на регіональні та локальні системи управління військового призначення, системи енергопостачання, системи формування громадської думки, психологічний вплив на моральний стан суспільства.

У рамках міжнародної антитерористичної операції *"Помста"* (Афганістан, 2001 р.) мета спеціалізованих центрів США, відповідальних за проведення інформаційних операцій, полягала у плануванні психологічних кампаній, реагуванні на зміну ситуації, у підтримці інформаційних ресурсів та безпеки військових сил і цивільного населення. "США мали намір нейтралізувати і знищити всю терористичну мережу, яка загрожує Америці і решті цивілізованого світу, – заявив на прес-конференції для міжнародних масмедіа тодішній держсекретар США К. Пауелл.

Мета операції *"Помста"* полягала не тільки у боротьбі проти тероризму, а й у переконанні певних режимів, які підтримують політику тероризму в тому, що така стратегія не відповідає їх власним інтересам. США задоволені реакцією світової спільноти та політичних лідерів більшості країн на пропозиції щодо глобальної боротьби з тероризмом".

Так, Північний Альянс вперше в історії застосував статтю 5 Статуту НАТО, яка спрямована на забезпечення загального захисту країн Організації перед викликами зовнішніх загроз; держави ЄС підтвердили підтримку дій США в акції "Помста"; країни-учасниці ГУАМ засвідчили підтримку дій США і консолідацію зусиль міжнародного співтовариства у протиборстві з міжнародним тероризмом у спільній заяві та меморандумі дій; політичний лідер Росії В. Путін запропонував розробити нову систему глобальної безпеки, враховуючи, що тероризм і його різновиди медіа- та кібертероризм стали глобальною загрозою для міжнародного миру XXI століття.

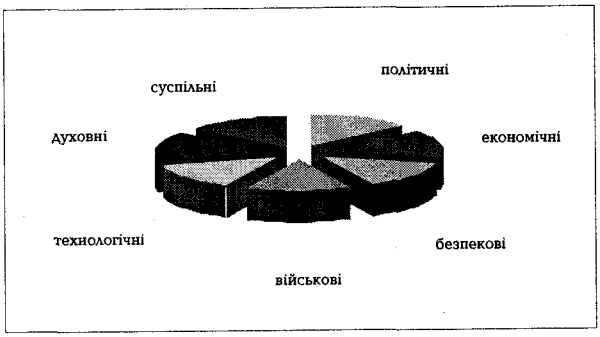
За теорією інформаційних війн, індустріальні чи навіть аграрні суспільства передбачають наявність електронних навігаційних систем, електронних рахунків у зарубіжних банках, використання сучасних телекомунікаційних засобів, функціонування національних або зарубіжних засобів масової комунікації. Газета *"USA Today"* подає модель інформаційної війни проти режиму Талібан, яка включає проведення психологічної операції в інформаційному просторі Афганістану з одночасним блокуванням національних радіостанцій, поширенням пропагандистських матеріалів з уривками з Корану, розрахованих на протидію закликів до джихаду та формування у суспільній свідомості відчуття невідворотної перемоги антитерористичного альянсу в ході операції "Помста". "Ми наближаємося до такого ступеня розвитку, коли всі є учасниками бойових дій. Завдання полягає не в знищенні жи-

вої сили, а в руйнації цілей, поглядів і світогляду населення, суто соціуму", – наголошував керівник Виконавчої ради з інформаційних війн при Міністерстві оборони США Д. Уайт [33].

Модель Е – протиборство світової спільноти та міжнародної організованої злочинності (терористичних угруповань), здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в аналітичному дослідженні Національної ради розвідки США „Mapping the global future" – 2020 у версії *„Коло страху"* („Cycle of fear"), яка є найбільш песимістичним сценарієм майбутнього світової спільноти.

Враховуючи високу здатність інформаційних озброєнь до інтеграції з іншими традиційними і технологічно новими видами військових засобів, потенційні наслідки безконтрольного застосування багатошарового страту можуть виявитися катастрофічними для існування людства. Тому тільки широке багатостороннє співробітництво може гарантувати світові вирішення нових складних проблем інформаційної доби і забезпечити реальну міжнародну інформаційну безпеку.

Загрози. Концепція міжнародної інформаційної безпеки визначає критичні структури, які, в першу чергу, зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства (існують інші класифікації) (див. діаграма 3).



У політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення.

Перебіг міжнародних інформаційних операцій *"Спільні зусилля"* (1996 р.), *"Союзницька сила"* (1998 р.) свідчать про інтенсивний психологічно-пропагандистський тиск на політичного лідера Югославії С. Міло-

шевича та політичні структури країни з метою дискредитації югославського керівництва та заміни, як наголошувалося у зверненнях до населення СФРЮ, "військового злочинця" і передачі його Міжнародному трибуналу.

За розпорядженням президента США Б. Клінтона, було здійснено ряд інформаційних заходів на підтримку югославської опозиції, зокрема, президента Чорногорії М. Джукановича, поїздки якого до західних держав та критичні висловлювання щодо політичного курсу Белграду широко висвітлювались і підтримувались у світових засобах масової комунікації.

Політичною перевагою США та країн НАТО, дипломатичним виміром інформаційної могутності коаліції стало підписання Дейтонської угоди по Боснії (1996 р.), врегулювання політичного і збройного конфлікту в Македонії (2001 р.), де політична влада на чолі з Б. Трайковскі погодилася на внесення змін до Конституції країни для вирішення гуманітарних проблем албанської меншини.

Ідеологічна операція "*Perestroika*" (1980-1990 рр.) підтвердила стратегію глобальних інформаційних операцій США у забезпеченні лідируючих позицій в системі міжнародної безпеки та світової політики. За словами Б. Клінтона, США, вплинувши на ідеологічні основи СРСР, вивели із війни за світову гегемонію державу – основного конкурента Америки, а наступні інформаційно-психологічні операції та політичні рішення були спрямовані на встановлення західної моделі демократії у нових суверенних державах Центральної та Східної Європи.

Відомі також інформаційні операції проти політичних лідерів та політичних режимів на Гаїті, в Афганістані, Індії, Індонезії, Африці та на Близькому Сході. США здійснили потужний інформаційний вплив на світову громадську думку, виступаючи з жорсткими політичними заявами щодо президентських виборів у Республіці Бєларусь (2001 р.). У заяві Білого Дому підкреслено, що "Лукашенко як останній диктатор Європи не лише викрав вибори у білоруського народу, він викрав у народу можливість повернутися на шлях демократії і ринкової економіки", тому США будуть співробітничати з європейськими союзниками та міжнародними організаціями для захисту демократій і верховенства права в Бєларусі різними засобами.

Для економічної сфери критичними вважаються системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж та систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі).

Досвід інформаційно розвинутих країн свідчить, що економічні переваги ґрунтуються в сучасному світі на прогресивній інформаційній експансії, і саме ті країни, які найбільше просунулися у напрямку інформаційної

цивілізації, будуть переважати у світовій господарській системі та в міжнародній конкуренції з технологічно відсталими країнами і регіонами.

Економічні аспекти інформаційних операцій простежуються у світовій фінансовій системі, що стала головною ареною глобального інформаційно-психологічного протиборства між провідними країнами світу. Відомий у світі Інститут аналізу фінансових ринків Дж. Сороса розробив і здійснив інтервенції в Азійсько-Тихоокеанському регіоні, Російській Федерації та Європі (1992, 1997, 1998 рр.), які супроводжувалися спеціальними інформаційно-психологічними операціями: виступи і заяви Дж. Сороса у "*Financial Times*" та інших мас-медіа про невизначеність валюти "євро", необхідність девальвації російського рубля, трансформацію ринку цінних паперів у Японії, про залежність німецької марки від девальвації фінансового ринку Росії. За оцінками британських і французьких експертів, чистий прибуток Сороса в результаті інформаційної акції та інтервенції на ринках склав близько 300 млн. дол.

Здійснення несанкціонованих інформаційних атак проти банківських мереж і систем Іспанії, коли найбільші іспанські банки "*Drety Bank*", "*Retwods Bank*", "*Tyten Bank*" втратили понад 127 млн. дол. США, змусило в подальшому уряд Іспанії розпочати загальнонаціональну програму боротьби з міжнародною комп'ютерною злочинністю в економічній сфері, об'єднати свої зусилля для протидії транснаціональним угрупованням з іншими країнами у Європі, Латинській Америці, Азії в рамках Інституту глобальних інформаційних досліджень (Мілан, Італія). Специфікація діяльності Інституту — захист інформаційно-комунікаційних систем банківської сфери, телекомунікацій, страхового бізнесу, урядових структур та систем національної безпеки. Завдяки спільному проекту "*ПАРС*" вдалося досягти сталої безпеки банківських систем, взаємодії країн та регіонів світу у боротьбі з промисловим шпигунством, хакерством та міжнародним інформаційним тероризмом.

Як елемент впливу на урядові структури Югославії було використано інформаційну загрозу превентивної економічної блокади. Держсекретар адміністрації Б. Клінтона з проблем зовнішньої політики М. Олбрайт з цього приводу заявила, що країни НАТО та їх союзники розглядають можливості обмеження поставок енергоносіїв в Югославію, а хакерам ЦРУ було поставлено завдання розкрити секретні рахунки С. Мілошевича в зарубіжних банках як мотив притягнення його до Міжнародного Суду за економічні злочини перед своїм народом [34].

Корпоративні війни в інформаційній сфері позначені інтенсивним злиттям ТНК, домінуванням в інформаційному секторі світової економіки групи інформаційно розвинутих країн, використанням стратегії інформаційного імперіалізму та значним обмеженням розвитку економічної системи країн незахідної цивілізації. Діяльність корпорацій Японії на ринку високих технологій за участю "Номура ресерч", (філії якої у всіх країнах світу відстежують ринок високих технологій, інтелектуальної власності та ноу-хау), стала однією із складових потужного економічного зростання країни в повоєнний період і

жорсткої конкуренції на міжнародній арені із застосуванням маніпулятивних технологій мас-медіа для дискредитації потенційних конкурентів.

Суспільна сфера виступає найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, інформаційно-організаційні структури політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну ідеями та інформацією.

У рамках операції НАТО "*Союзницька сила*" було застосовано засоби впливу проти інфоінфраструктури Югославії, проурядових ЗМК, системи формування громадської думки: від бомбардування телерадіостанцій, жорсткого контролю національного інформаційного простору, заборони на мовлення в аналоговому форматі до заміни і виведення інформаційного простору за межі національної території за допомогою технологій Internet і створення нової інформаційної реальності для національного суспільства.

Сербський парламент у відповідь на загострення косівської кризи прийняв Закон про суспільну інформацію, за яким було заборонено трансляцію зарубіжних програм на території країни через національні канали комунікації. Зокрема, дискримінаційні штрафи, які потрібно було сплатити протягом доби, і заборона інформаційної і професійної діяльності торкнулися таких засобів масової комунікації, як "*Danas*", "*Nasa Borba*", "*Dnevni Telegraf*", "*Europ/Janin*".

Перебіг подій виявив нові форми, методи та елементи інформаційних озброєнь, підтвердив, що в умовах збройного конфлікту досконале управління інформаційними кампаніями обумовлює досягнення переваг. В результаті інформаційної війни в Чечні (Росія) було сформовано систему відповідної суспільної думки в країні про необхідність саме воєнного силового розв'язання проблеми [35].

Глобального характеру набули інформаційні загрози в науково-технологічній сфері: від феномену транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково-технологічного характеру на біологічних носіях до міжнародних систем спостереження, аналізу та прогнозування тенденцій науково-технологічного розвитку в різних країнах з метою доступу до конфіденційних баз і банків даних.

Критичними для безпеки у сфері науки та технологій є структури накопичення науково-технічної інформації, інституції та структури фундаментальних і прикладних досліджень, об'єкти інтелектуальної власності, ноу-хау. Інформаційно-технологічний аспект безпеки зорієнтований на реалізацію системних заходів, спрямованих на максимальне вдосконалення науково-технологічної сфери, ефективний захист інтелектуальних ресурсів. Проблема інформаційної безпеки в цій сфері тісно пов'язана з діяльністю промислової розвідки, несанкціонованим втручанням у конфіденційні мережі та системи, кібернетичними (хакерськими) війнами спеціалізованих підрозділів окремих країн, конкуренцією на світових ринках.

Відомими стали інформаційні операції в галузі цифрового мобільного телебачення, "нейронних" комп'ютерів, новітнього програмного забезпечення, біотехнологій Японії США, Ізраїлю, країн ЄС, де системи аналізу науково-технологічної інформації є елементом державної політики та доктрини воєнної безпеки. Аналітичні дослідження науково-технологічного потенціалу країн Європи за допомогою методик "*Моссад*" дали змогу Ізраїлю скерувати технологічний розвиток країни, розширити ринки збуту інформаційних продуктів та біотехнологій, усунути конкурентів (викрадення технологій проекту "*Міраж*", Франція).

Аналіз системи наукових грантів, які поширювалися в Україні зарубіжними фондами, свідчить про особливу зацікавленість провідних країн світу до науково-технологічних розробок Інституту Патона, Інституту надтвердих матеріалів, Інституту біотехнологій, Інституту проблем матеріалознавства тощо. Так, представництвом Deutsche Bank в Україні протягом 1992-1998 років було здійснено широкомасштабне дослідження ходу реформ в Україні, аналіз діяльності банківської системи, використано можливості для перспективного придбання ліцензій та патентів на винаходи, які віднесені до категорії національного надбання і не мають аналогів у світі. З одного боку це свідчить про наявність інтелектуального потенціалу України, з іншого про міжнародну конкуренцію з боку західних країн у галузі високих технологій та наукових досягнень.

У військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, ВПК, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, розвідувального характеру. Наприклад, США використали свої інформаційні можливості за допомогою системи "*Echelon*" (код 1947 "UKUSA Agreement") для виявлення програми розробки ядерної зброї в Кореї і для укладення детальної угоди з її ліквідації; для оперативного з'ясування і попередження співробітництва Росії та Китаю з Іраном в ядерній та ракетній галузях: для забезпечення механізму контролю ООН з інспектування іранських ядерних об'єктів, а також для вивезення ядерного потенціалу і тактичної зброї з України, викриття контракту "*Thomson CSF*" – поставки французької зброї до Бразилії, операції з відмивання грошей за продаж зброї в треті країни.

Система "*Echelon*" і нова система спостереження і перехоплення комунікацій „Око світу" як засіб доступу до будь-яких видів інформації у глобальному вимірі (телекомунікаційні мережі і системи, супутниковий, мобільний та високочастотний зв'язок, Internet) орієнтовані на перехоплення інформації урядових, комерційних, приватних структур в будь-якому регіоні світу. За допомогою системи здійснюється доступ до всіх основних компонентів глобальної інфоінфраструктури.

Під час операції "*Союзницька сила*" у відповідь на бомбардування інфраструктури Югославії сербські хакери заблокували за допомогою атаки

ping of death офіційний сервер НАТО, ряд інших військових та урядових сайтів країн-членів Альянсу повідомленнями з макровірусами, що підтвердило прогнози про перенесення військових операцій у кіберпростір, на рівень інформаційного протиборства. А керівництво СФРЮ розсекретило через мережу Internet інформацію про американський план "Корені", яким планувалася етнічна та воєнна дестабілізація на Балканах з метою закріплення тенденції необоротних змін на посттоталітарному просторі [36].

Духовна сфера стає критичною в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей. Проявом критичності духовної сфери (Ірландія, Алжир, Ізраїль, Афганістан, Китай, Іран) на міжнародному рівні стала проблема, пов'язана з рішенням керівництва ісламського радикального руху "Талібан" (Афганістан) про руйнування неісламських релігійних пам'яток, що віднесені до глобальної культурної спадщини і перебувають під охороною ЮНЕСКО.

У терміновому порядку було схвалено резолюцію ГА ООН, заяву голови Ради Безпеки та Генерального директора ЮНЕСКО (16 березня 2001 р.), в якій було засуджено вандальні акти руйнування пам'яток з причин релігійного фанатизму.

До сучасних інформаційних загроз відносять також *кібер-*, *медіа-* та *психотероризм* як протиправні дії, спрямовані на руйнування життєво важливих інфраструктур, систем управління державою, морального стану суспільства та війська, порушення прав людини (див. діаграма 4).

Відповідно до критичних сфер міжнародного співробітництва класифікуються загрози для інформаційної безпеки. Існують різні типології загроз, але, узагальнюючи, можна виділити: інформаційно-технологічні, інформаційно-комунікаційні, інформаційно-психологічні. Інформаційні загрози реалізуються через порушення інфраструктури, вільного обігу інформації, неправомірні дії щодо використання інформації; через невідповідність інформаційної політики, засобів інформування громадськості та ЗМК життєво важливим інтересам суспільства.

Широке використання маніпулятивних технологій, тенденційна модифікація інформаційних ресурсів, формування викривленої інформаційної реальності призводить до зруйнування глобального інформаційно-психологічного середовища, трансформації ціннісних орієнтацій суспільства, порушення фундаментальних прав і свобод як складових міжнародної інформаційної політики.

Феномен міжнародної інформаційної безпеки обумовлюється стратегічною спрямованістю інформаційних озброєнь проти критично важливих структур життєдіяльності і функціонування міжнародного співтовариства, визнання інформаційної зброї як нового глобального виду зброї масового ураження, катастрофічного за наслідками свого застосування (деякі дослідники називають інформаційні озброєння "інформаційним апокаліпсисом"), необхідністю створення міжнародного механізму протидії і попередження глобальних інформаційних війн в рамках політичної компетенції ООН, регіональних міжнародних організацій з проблем безпеки та оборони, політичних рішень на національному рівні.

Таким чином, проблема міжнародної інформаційної безпеки є вагомою складовою загальних проблем національної, регіональної та глобальної політики у сфері міжнародних інформаційних відносин і проявом тенденцій нових глобальних викликів і глибинних процесів глобалізації комунікацій.

1.2. Міжнародне право інформаційної безпеки: динаміка і проблеми завершення переговорного процесу в рамках ООН

Формування нової геостратегічної структури міжнародних відносин під впливом глобалізації та швидкоплинного розвитку високих технологій зумовило нові підходи та окреслення нових параметрів сучасної системи міжнародної безпеки. Багатогранність інформаційно-комунікаційних технологій (ІКТ) у політичному, економічному, безпековому, соціальному та культурному плані, визнання руйнівного чинника нових технологічних озброєнь змусило ООН та інші впливові міжнародні організації включити проблему міжнародної інформаційної безпеки у сферу своїх інтересів.

Головним форумом для конкретної практики права міжнародної безпеки є ООН – універсальна міжнародна організація з безпеки і співробітництва держав, яка відповідно до Статуту є центром для узгоджених дій всіх націй у досягненні своїх цілей. Практично діяльність ООН охоплює всі сфери міжнародної безпеки: військову, політичну, економічну, гуманітарну, екологічну, інформаційну тощо. В резолюції 42/93 (1987р.) ГА ООН відзначила, що з часу прийняття Статуту організації у світі відбулися значні трансформації, зумовлені процесами політичної, економічної та технологічної глобалізації, зросла взаємозалежність держав та їх зацікавленість у підтриманні сталого миру і безпеки, що зумовлює необхідність спільних зусиль всіх акторів міжна-

родних відносин у сфері безпеки, мирного врегулювання конфліктів та кризових ситуацій, захисту прав людини і основних свобод [37]. ГА ООН у Резолюції 44/21 (1989р.) закликала всі держави примножувати їх практичні зусилля в усіх напрямах забезпечення міжнародної безпеки, підтвердила дієвість і значення Статуту ООН, необхідність дотримання основних його принципів, висловилась за співробітництво в рамках Організації та її основних структур з метою знайти різноманітні підходи до зміцнення принципів і систем міжнародної безпеки на основі нормативних документів ООН. Міжнародно-правове співробітництво свідчить, що міжнародні угоди проходять тривалий шлях через ухвалення резолюцій і декларацій, але саме угоди є основою правового регулювання міжнародних відносин у сфері безпеки [38].

Сучасна міжнародна безпека є визначеною системою міжнародних відносин держав з метою підтримання міжнародного миру і безпеки, що регламентується принципами і нормами статуту ООН. Ця система охоплює:

1) основні принципи міжнародного права;
2) процедури мирного вирішення спорів;
3) спільні дії та миротворчі операції для попередження загрози миру;
4) повноваження ГА ООН та Ради Безпеки ООН з питань роззброєння та обмеження озброєнь.

Нормотворча практика ООН внаслідок трансформацій сучасного світу та досягнень нових технологій здійснюється шляхом розробки нових угод та рекомендацій з різних конкретних питань міжнародних відносин, зокрема питань міжнародної безпеки. Норми таких угод та резолюцій складають вторинний відносно Статуту ООН конкретний шар міжнародного правопорядку, який базується на цілях і принципах Статуту ООН і є регуляторною основою міжнародних відносин в галузі міжнародної безпеки. Стан договірних норм у системі міжнародної безпеки має різноманітний характер: існують міжнародні договори, з імперативними положеннями, деякі принципи, прийняті у вигляді резолюцій і потребують кодифікації, щоб їх сучасний зміст набув зобов'язального характеру, окрім того виникають нові принципи міжнародного права, які не зафіксовані в Статуті ООН і які потребують розробки і юридичного закріплення.

Усвідомлення необхідності суворого дотримання принципів незастосування сили, невтручання у внутрішні справи держав, забезпечення фундаментальних прав і свобод, невикористання високих ІКТ – технологій з протиправною метою, невідповідність статуту ООН зумовило розгляд проблеми міжнародно-правового регулювання інформаційної безпеки і встановлення міжнародного контролю за інформаційними озброєннями. Передбачалося: з'ясувати позиції світового співтовариства щодо проблеми потенційного воєнного використання ІКТ-технологій для вдосконалення існуючих і створення нових систем озброєнь; визначити основні поняття у сфері міжнародної інформаційної безпеки; розглянути можливість створення міжнародної системи моніторингу інформаційних загроз; розробити міжнародно-правовий ре-

жим інформаційної безпеки. Конструктивне обговорення проблеми визначило пріоритети ООН щодо інформаційної безпеки, зокрема, було підкреслено, що в інформаційній сфері необхідна кодифікація спеціальних принципів і норм, що склалися на основі Статуту ООН, і досягнення нових угод, щоб упорядкувати і стабілізувати відносини держав, спрогнозувати їх подальший розвиток, а також інших відносин, пов'язаних з проблемою інформаційної безпеки, зокрема політичних, соціальних, економічних, гуманітарних, екологічних тощо. У зв'язку зі значенням міжнародних договорів, які входять до системи міжнародної безпеки, особливий інтерес виникає з таких питань, як тривалість чинності міжнародних договорів, можливість виходу з них, їх універсальність і забезпечення механізму виконання положень договору.

Протягом 1998-2006 рр. питання міжнародної інформаційної безпеки постійно обговорювалось на ГА ООН з метою розробки відповідного міжнародного документу на основі ухвалених резолюцій, в яких зафіксовано глобальність проблеми, наявність тісного зв'язку між її різними аспектами, такими, як сталий розвиток, боротьба з бідністю, зміцнення демократичного управління, подолання цифрового розриву, тобто ідей, зафіксованих у Декларації тисячоліття.

Нормотворча діяльність ООН має першочергове значення для вирішення проблеми міжнародної інформаційної безпеки. Вперше ця проблема розглядалася на 53 сесії ГА ООН коли було проголосовано резолюцію 53/73 ***„Роль науки і техніки в контексті міжнародної безпеки і роззброєння"*** (1999 р.) - за – 77, переважно держави Південної Америки, Африки, Тихоокеанського регіону та Близького Сходу, тобто, країни, що розвиваються; проти – 43, переважно держави Північної Америки, Європи, Балтії, Австралії та Нової Зеландії, утримались – 16, переважно держави СНД, Японія, деякі країни Південної Америки та ПАР [39]. В ній зазначалися положення про подвійну природу досягнень науки і техніки (як у цивільній, так і у воєнній сферах), про застосування новітніх досягнень у модернізації сучасних озброєнь, зокрема зброї масового ураження, про здатність досягнень науки і техніки здійснювати негативний вплив на міжнародну безпеку. В резолюції підкреслюється, що новітні технології (пристрої, послуги „ноу-хау" подвійного призначення) мають важливе значення для економічного і соціального розвитку держав, і водночас висловлюється занепокоєність щодо розповсюдження спеціальних та особливих режимів та механізмів регулювання експорту продуктів і технологій подвійного призначення, здатних негативно вплинути на країни так званого *„третього світу"*.

Зважаючи на необхідність регулювання передачі новітніх технологій подвійного призначення було запропоновано встановити жорсткі обмеження на експорт новітніх матеріалів, обладнання та технологій у країни, що розвиваються, для використання у мирних цілях. У резолюції вказується на застосування узгоджених, на багатосторонній основі, загальноприйнятних, недискримінаційних керівних принципів, які мають врахувати законні оборонні по-

треби всіх держав і потреби з підтримання міжнародного миру та безпеки, сприяти використанню досягнень науки і техніки на основі передачі технічних знань та обміну ними в мирних цілях.

Резолюція закликала держави-члени ООН вжити додаткових заходів із застосування досягнень науки і техніки з метою роззброєння та передачі технологій відповідного характеру, розробити керівні принципи щодо регулювання міжнародної передачі новітніх технологій подвійного призначення та високих технологій воєнного застосування. Виклики високих технологій для міжнародної безпеки у XXI ст., враховуючи неможливість їх вирішення однією або кількома державами, зумовили необхідність проведення багатосторонніх переговорів на рівні ООН та ухвалення резолюцій про міжнародну інформаційну безпеку. Під час 53 сесії ГА ООН було підтримано ініціативу про активізацію спільних зусиль з протидії транснаціональним загрозам із застосуванням ІКТ та інших високих технологій, вирішення проблеми міжнародної інформаційної безпеки з максимальним врахуванням інтересів усіх держав світу. На основі дискусії було прийнято резолюцію ГА ООН 53/70 *„Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки"* (1999 р.), в якій підкреслюється необхідність розробки міжнародно-правової бази та вироблення документів на рівні конвенції і закріплення міжнародних принципів в національних законодавствах.

Резолюція 53/70 стала основою предметного розгляду проблеми міжнародної інформаційної безпеки на рівні ООН, формування нового міжнародно-правового режиму, суб'єктом якого є ІКТ-технології та методи їх використання [40; 41].

Позиції Великої Британії, Російської Федерації, Куби, Катара, Омана, Саудівської Аравії засвідчили, що держави вбачають потенційну загрозу в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства, підкреслюють необхідність розробки та ухвалення концепції міжнародної інформаційної безпеки, принципів спрямованих на посилення безпеки глобальних і телекомунікаційних систем, попередження інформаційного тероризму і злочинності, створення спеціального міжнародного суду зі злочинів в інформаційній сфері. Позиції США та Австралії підкреслюють, що міжнародна інформаційна безпека охоплює різні аспекти мереж (воєнно-політичні, технічні, економічні, соціальні, правові, культурні), е-торгівлю, тероризм, хакерство, маніпулятивний вплив, ЗМІК, спеціальні інформаційні операції тощо, тому до вироблення міжнародних документів потрібно залучити відповідні комітети ООН, внести зміни у чинні законодавства держав, особливо розглянути положення щодо загроз терористичного та злочинного характеру.

З ініціативи Росії (у 1996 році Федеральне агентство урядового зв'язку та інформації при Президентові РФ опублікувало аналітичну довідку *„Інформаційні озброєння як загроза національній безпеці Росії"*, у 1997-1998 рр. Державна Дума РФ, потім Міжпарламентська Асамблея СНД звернулись

до ООН, ОБСЄ та РЄ з пропозицією прийняти міжнародну конвенцію про заборону інформаційних воєн та обмеження обігу інформаційної зброї) на 54 сесії ГА ООН було ухвалено оновлену резолюцію 54/49 (1999 р.) *„Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки"*, на підставі якої концепцію міжнародної інформаційної безпеки було визнано глобальною проблемою сучасності. Об'єктивними умовами її прийняття було усвідомлення принципово нових потенційних загроз для міжнародного миру, зумовлених науково-технологічним прогресом та глобальною взаємозалежністю всіх сфер життєдіяльності міжнародного співтовариства. В резолюції запропоновано державам-членам висловитися щодо загальних проблем інформаційної безпеки, розглянути конкретну технологію інформаційних загроз, в тому числі несанкціоноване втручання та неправомірне використання інформаційних і телекомунікаційних систем та інформаційних ресурсів, розробити міжнародні принципи, спрямовані на зміцнення безпеки глобальних інформаційних та комунікаційних систем та на боротьбу з інформаційним тероризмом і злочинністю[42; 43].

Генеральна Асамблея ООН продовжила роботу над резолюцією „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки" протягом 55 сесії, обговоривши доповіді Генерального Секретаря та представника Першого комітету Р. Габріеля, в яких містився аналіз позицій держав-членів у відповідь на вербальну ноту Генерального секретаря ГА ООН щодо міжнародної інформаційної безпеки. Так, позиція Польщі щодо загальної оцінки проблем інформаційної безпеки та визначення основних понять полягає у констатації впливу ІКТ на світовий розвиток, які стимулюють економіку, полегшують вільні потоки інформації, сприяють зміцненню демократії та свободі слова, формуванню громадянського суспільства.

Польща вважає за необхідне заохочувати та забезпечувати подальший розвиток ІКТ та цивільне їх використання. Разом з тим Польща визнає наявність потенційних загроз несанкціонованого втручання або неправомірного використання ІКТ-систем, цілісності критично важливих інфоінфраструктур та інформаційних ресурсів урядових, неурядових, комерційних установ та приватних банків даних. У відповіді зазначається, що інформаційна безпека охоплює широкий спектр проблем, зокрема проблем доступу, конфіденційності, наявності і збереження інформації у процесі обробки. Недостатній захист інформаційних ресурсів та ІКТ-систем, що мають життєво важливе значення для національної безпеки держав, може розглядатися і як загроза для міжнародної безпеки. *Ці загрози неможливо класифікувати виключно як цивільні* або воєнні, оскільки ІКТ можуть бути використані окремими особами, терористичними організаціями та злочинними угрупуваннями. Тому міжнародне співтовариство, на думку польської сторони, має сконцентруватися на захисті інформаційних ресурсів та інформаційних систем. Польща виступає за ефективне і багатостороннє міжнародне співробітництво, розробку нових законодавчих актів та за суворе виконання чинного внутрішнього законодавства:

1) на міжнародному рівні було запропоновано підтвердити керівну роль ООН щодо розробки міжнародних принципів з інформаційної безпеки, сприяти координації діяльності міжрегіональних та регіональних структур з попередження злочинного використання ІКТ;
2) на національному рівні визначено за доцільне прийняти відповідні закони, зокрема про захист секретної інформації, приватної інформації в процесі автоматизованої обробки даних, встановити кримінальну відповідальність за руйнування, модифікацію та викрадення комп'ютерних даних, або передачі інформації щодо питань національної безпеки, безпеки ІКТ-систем та функціонування органів державної влади;
3) укласти двосторонні міжнародні угоди (Польща веде переговори з ФРН, Угорщиною, Словаччиною, Україною, Францією, Естонією) про захист інформації щодо медичних даних, інтелектуальної власності, наукових досліджень від будь-якого несанкціонованого втручання, включаючи незаконні банківські та фінансові операції.

У цьому зв'язку підкреслюється важливість ефективного міжнародного співробітництва у правовій сфері, дотримання чинного міжнародного законодавства і необхідність розвитку міжнародного права з врахуванням концепції міжнародної інформаційної безпеки.

Йорданія та Катар також підтвердили необхідність розробки міжнародно-правових принципів щодо інформаційної безпеки, включивши до переліку загроз: *„шпіонаж"* (попередження несанкціонованого доступу до змісту ІКТ-систем); *„саботаж"* (попередження часткового або повного знищення ІКТ-систем); *„підробку"* (попередження підробки інформації в глобальному кіберпросторі). Від імені урядів цих держав було запропоновано ухвалити концепцію міжнародної інформаційної безпеки і сприяти підтриманню системи сталого миру.

Найбільш розгорнута відповідь на вербальну ноту Генерального секретаря ООН та пропозиції надійшли від Російської Федерації, що представила на розгляд Асамблеї типологію термінів з міжнародної інформаційної безпеки (інформаційний простір, інформаційні ресурси, інформаційні війни, інформаційна зброя, інформаційна безпека, загрози інформаційної безпеки, міжнародна інформаційна безпека, неправомірне використання ІКТ-систем та ресурсів, несанкціоноване втручання в ІКТ-системи та ресурси, критично важливі структури, міжнародний інформаційний тероризм, міжнародна інформаційна злочинність) та принципи взаємодії держав у сфері міжнародної інформаційної безпеки. Принципи, за визначенням пропозиції РФ, – це робочий варіант кодексу поведінки держав у міжнародному інформаційному просторі, основа для міжнародних переговорів під егідою ООН з цієї проблематики. П'ять базових принципів міжнародної інформаційної безпеки визначають роль і права, зобов'язання і відповідальність держав у міжнародному інформаційному просторі, визначають заходи, спрямовані на обмеження загроз у сфері міжнародної інформаційної безпеки, а також роль ООН у міжнародному співробітництві в контексті цієї проблеми.

- Принцип 1 проголошує, що діяльність кожної держави та інших суб'єктів міжнародного права в міжнародному інформаційному просторі повинна сприяти загальному соціальному та економічного розвитку і здійснюватися таким чином, щоб відповідати завданням підтримання сталого миру і безпеки, суверенних прав інших держав, інтересам безпеки, принципам мирного врегулювання спорів та конфліктів, незастосування сили, невтручання у внутрішні справи, поваги до прав і свобод людини. Така діяльність повинна відповідати праву кожного шукати, отримувати та поширювати інформацію та ідеї, як це зафіксовано у документах ООН, з врахуванням того, що таке право може бути обмежене законом з метою захисту інтересів національної безпеки кожної держави. При цьому кожна держава та інші суб'єкти міжнародного права повинні мати рівні права на захист своїх інформаційних ресурсів та критично важливих структур від неправомірного використання; несанкціонованого інформаційного втручання і можуть сподіватися на підтримку світового співтовариства в реалізації цих прав.
- Принцип 2 підкреслює, що держави повинні прагнути до обмеження загроз у сфері міжнародної інформаційної безпеки і з цією метою утримуватися від розробки, створення і використання засобів впливу і завдання шкоди інформаційним ресурсам і системам іншої держави; спрямованого інформаційного впливу на критично важливі структури іншої держави; інформаційного впливу з метою руйнування політичної, економічної та соціальної системи інших держав і задля дестабілізації суспільства; несанкціонованого втручання в інформаційно-телекомунікаційні системи та інформаційні ресурси, їх неправомірне використання; дій, що сприяють домінуванню і контролю в інформаційному просторі; протидії доступу до новітніх ІКТ, створення умов технологічної залежності у сфері інформатизації як загрозу іншим державам; заохочення дій міжнародних терористичних, екстремістських і злочинних угрупувань, які загрожують інформаційним ресурсам та критично важливим структурам інших держав; розробки та ухвалення планів, доктрин, які передбачають ведення інформаційних воєн, здатних спровокувати гонку озброєнь, а також викликати напруженість у відносинах між державами і самих інформаційних воєн; використання ІКТ проти основних прав і свобод людини, які реалізуються в інформаційній сфері; транскордонного поширення інформації, що суперечить принципам і нормам міжнародного права, а також внутрішньому законодавству конкретних країн; маніпулювання інформаційними потоками, дезінформації та засекречування інформації з метою викривлення психологічного і духовного середовища суспільства, ерозії традиційних культурних, моральних та етичних і естетичних цінностей; інформаційної експансії, монополії в національних інформаційних системах інших держав, включаючи умови їх функціонування в міжнародному інформаційному просторі.

- Принцип 3 встановлює, що ООН та її спеціалізовані установи сприятимуть міжнародному співробітництву, метою якого є обмеження загроз у сфері міжнародної інформаційної безпеки і формування відповідної міжнародно-правової бази для визначення ознак та класифікації інформаційних воєн; визначення ознак і класифікації інформаційних озброєнь і засобів відповідного призначення; обмеження обігу інформаційних озброєнь; заборони розробки, поширення і використання інформаційної зброї; попередження загрози виникнення інформаційної війни; визнання безпеки застосування інформаційної зброї щодо критично важливих структур як зброї масового ураження; створення умов для рівноправного і безпечного міжнародного інформаційного обміну на основі загальновизнаних норм і принципів міжнародного права; попередження використання інформаційних технологій і засобів впливу на суспільну свідомість з метою дестабілізації суспільства і держави; розробки процедури взаємного інформування та попередження транскордонного несанкціонованого інформаційного впливу; створення системи міжнародного моніторингу для відстеження загроз в інформаційній сфері; створення міжнародної системи сертифікації технологій і засобів інформатизації і телекомунікацій (в тому числі програмно-технічних) щодо гарантій їх інформаційної безпеки; створення механізму контролю виконання умов режиму міжнародної інформаційної безпеки; створення механізму врегулювання конфліктних ситуацій у сфері інформаційної безпеки; розвитку систем міжнародної взаємодії правоохоронних органів з попередження і припинення правопорушень в інформаційному просторі; гармонізації на добровільній основі національних законодавств для забезпечення міжнародної інформаційної безпеки.
- Принцип 4 визначає, що держави та інші суб'єкти міжнародного права повинні нести міжнародну відповідальність за діяльність в інформаційному просторі, яка здійснюється ними, під їхньою юрисдикцією або в рамках міжнародних організацій, членами якої вони є і за відповідність такої діяльності принципам, які містяться у цьому документі.
- Принцип 5 стверджує, що будь-які спори між державами та іншими суб'єктами міжнародного права, які виникають при застосуванні цих принципів, регулюються за допомогою встановлених процедур мирного врегулювання спорів [41; 44].

Дискусії з проблематики міжнародної інформаційної безпеки виявили різні підходи розвинених країн та країн, що розвиваються. Одні країни активно підтримали позицію Російської Федерації, вбачаючи загрозу ізоляції від активної участі у вирішенні проблеми, залежності у випадку інформаційної агресії, інші – розглядали ініціативу РФ як політичний хід і вбачали вирішення проблеми у переговорах між США та РФ, треті – вважали, що необхідні радикальні заходи повної заборони використання інформаційних озброєнь як зброї масового ураження. В цілому міжнародне співробітництво сприйняло

аргументи про актуальність і глобальність проблеми міжнародної інформаційної безпеки і необхідність прийняття узгодженого рішення в рамках ООН.

Тому, 55-та сесія ГА ООН прийняла Резолюцію 55/28 (2000 р.) „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки", в якій, посилаючись на попередні резолюції про роль науки і техніки в контексті міжнародної безпеки та відзначаючи відповіді держав щодо оцінки проблем інформаційної безпеки, закликає всі держави-члени ООН сприяти на багатосторонній основі подальшому розгляду концепцій глобальної інформаційної безпеки та загроз у сфері ІКТ для завершення дискусії і ухвалення міжнародної конвенції з інформаційної безпеки [45].

Подальший перебіг міжнародних дискусій визначила 56-та сесія ГА ООН, яка розглянула доповіді Генерального Секретаря та представника Першого комітету С. Екундайо Рове щодо визнання інформаційної безпеки глобальною проблемою, обговорила відповіді держав про загальну оцінку, визначення основних критеріїв і змісту відповідних міжнародних концепцій і прийняла резолюцію 56/19 (2001р.) ***„Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки"***. В резолюції зазначено, що поширення і використання інформаційних технологій та засобів стосується інтересів всього міжнародного співтовариства. Ці технології та засоби потенційно можуть бути використані з метою нестабільності міжнародної безпеки як у воєнній, так і у цивільній сферах, тому необхідно провести міжнародну зустріч експертів для конкретизації сутності проблеми міжнародної інформаційної безпеки та її правового забезпечення [46].

Серед відповідей держав (Болівія, Мексика, Філіппіни та Швеція) особливу увагу привертає позиція держав Європейського Союзу, в якій підкреслюється, що країни ЄС підтримали ухвалену консенсусом резолюцію 55/28 ГА ООН „Досягнення у сфері інформації і телекомунікацій в контексті міжнародної безпеки". Щодо загальної оцінки проблеми інформаційної безпеки то ЄС вважає, що ІКТ сприяють вільному потоку інформації, демократизації суспільства та економічному прогресу. ЄС визнає, що існують потенційні загрози неправомірного та несанкціонованого використання ІКТ у різних сферах життєдіяльності держав, що створює загрозу для міжнародної безпеки. Оцінюючи зміст міжнародних концепцій про безпеку глобальних ІКТ-систем, ЄС підкреслює, що, незважаючи на ефективність міжнародного співробітництва у сфері інформаційної безпеки, в першу чергу кожна держава має право і несе відповідальність за захист власних інформаційних ресурсів та інформаційних систем. Існуючі ризики мають транскордонний характер, і будь-які превентивні заходи, спрямовані на обмеження потенційних втрат від злочинного чи терористичного нападу, зокрема і для міжнародної безпеки, повинні здійснюватися з урахуванням захисту ІКТ-ресурсів та систем. ЄС вважає, що саме ООН має стати основним форумом з обговорення проблем міжнародної інформаційної безпеки. Водночас у відповіді підкреслюється, що

форумом для обговорення проблеми міжнародної інформаційної безпеки можуть бути, крім ООН, інші міжнародні організації.

У відповідях урядів Мексики, Гватемали та Болівії представлені різні підходи до проблеми глобальної інформаційної безпеки. Зокрема, Болівія не передбачає виробництва інформаційних озброєнь або оснащення ними своїх збройних сил у найближчому майбутньому. Разом з тим Мексика та Філіппіни внесли пропозиції і щодо оцінки проблеми інформаційної безпеки, визначення основних понять в цій сфері, конкретизувавши як загрози, зокрема міжнародний інформаційний тероризм, кіберзлочинність, так і заходи протидії цим загрозам. Так, Мексика підкреслила, що підтримує положення резолюції 51/210 (1996р.) щодо міжнародного тероризму та можливості використання ІКТ-систем і ресурсів для злочинних протиправних дій і сприятиме попередженню такого роду злочинності на основі узгоджених міжнародних підходів на різних рівнях.

Філіппіни визнали інформаційні озброєння такою ж загрозою, як і зброя масового ураження, підкресливши, що всі досягнення у сфері науки і техніки можуть бути використані з протиправною метою, тому ця проблема є глобальною і для розвинутих в технічному відношенні країн, і для країн, що розвиваються. Серед понять (несанкціоноване втручання, проникнення, санкціоноване втручання, несанкціоноване використання інформації, протиправне використання ІКТ, інформаційні ресурси, інформаційна зброя, інформаційна війна, інформаційний тероризм, електронні кіберзлочини, кібернетичні злочинці, технологічно передові держави) новим є термін „інформаційна колонізація", яка визначається як дії однієї держави або держав проти інших з метою встановлення монополії та контролю в інформаційній сфері, попередження доступу до новітніх технологій або встановлення технологічної залежності в інформаційній сфері, акти інформаційної експансії і встановлення монополії над національними ІКТ, інфраструктурами іншої держави з метою створення умов залежності і контролю. РФ висловила занепокоєння у зв'язку з різними підходами та неузгодженістю позицій і наголосила, що важливо розглядати глобальну і всеохоплюючу проблему міжнародної інформаційної безпеки в рамках єдиного міжнародного органу [41; 46]

Констатація необхідності обговорення міжнародних концепцій з інформаційної безпеки зумовила принципове продовження дискусій на 56 сесії ГА ООН. У Резолюції 56/19 (2001р.) схвалено ідею створення у 2004р. спеціальної групи урядових експертів держав-членів ООН для вивчення проблеми міжнародної інформаційної безпеки, зокрема з'ясування реальних та потенційних загроз у сфері інформаційної безпеки і спільних заходів з їх попередження, визначення заходів, спрямованих на зміцнення безпеки глобальних мереж і систем.

ГА ООН проголосувала також резолюцію 56/121 (2001р.) під загальною назвою ***„Боротьба зі злочинним використанням інформаційних технологій"*** в якій запропоновано різні заходи боротьби з тероризмом у

зв'язку з використанням терористичними та злочинними угрупованнями високих технологій. Серед заходів: удосконалення національних законодавств у сфері боротьби з кіберзлочинністю; співробітництво правоохоронних органів у разі транскордонного злочинного використання ІКТ; обмін інформацією щодо проблем боротьби із злочинним використанням ІКТ; правовий захист конфіденційності, цілісності і доступності даних; захист комп'ютерних систем від несанкціонованого втручання; покарання за неправомірне зловживання ІКТ; режим взаємодопомоги у розслідуванні злочинів з ІКТ; інформування громадськості щодо попередження злочинів; вдосконалення ІКТ з превентивною складовою; необхідність захисту основних прав і свобод приватного життя [47; 49].

57-ма сесія ГА ООН на підставі Доповіді Генерального Секретаря та представника Першого комітету М. Самсара, посилаючись на попередні резолюції з питань ролі науки і техніки в контексті міжнародної безпеки, підкреслюючи значний прогрес у розробці та впровадженні високих технологій, відзначаючи, що бачить у цьому процесі широкі позитивні можливості взаємодії держав задля підвищення інтелектуального потенціалу людства і обміну інформації у глобальному співтоваристві, підтвердила важливість проблеми міжнародної інформаційної безпеки і ухвалила Резолюцію 57/53 (2002р.) про необхідність обговорення існуючих та потенційних загроз у сфері інформаційної безпеки, можливі заходи з їх попередження, а також дослідження міжнародних концепцій на рівні урядових експертів з цієї проблеми. У додатку (відповідь Уряду Гватемали) запропоновано заходи на національному рівні, пов'язані з правовим забезпеченням інформаційної безпеки (при передачі інформації сучасними ІКТ-мережами, порушенні зв'язку, модифікації і заміни інформації), для чого було внесено зміни до ст. 295, 274, 274 „К", 274 „Д", 274 „Е", 274 „F", 274 „G" Кримінального кодексу країни за такі порушення, як *„порушення зв'язку", „порушення авторських і суміжних прав", „збирання забороненої (конфіденційної) інформації", „маніпулювання інформацією", „злочинні програми"*, тощо. Разом з тим було гарантовано свободу слова та обміну інформацією, невтручання у приватні бази даних, заборону цензури згідно зі ст. 13 Американської конвенції про права людини.

Резолюція 57/53 розвинула і поглибила положення попередніх резолюцій з міжнародної інформаційної безпеки, підтвердила неможливість використання ІКТ-технологій і засобів з метою негативного впливу на інфраструктуру інших держав, закликала до активної діяльності групи експертів під егідою ООН [50].

Нова ініціатива РФ з проблеми діяльності групи експертів охоплювала організаційно-практичні та змістові аспекти проблеми міжнародної інформаційної безпеки, зокрема: узгодження політичного аспекту у сфері міжнародної інформаційної безпеки, визначення чинників, що впливають на стан міжнародної інформаційної безпеки, з врахуванням загроз воєнного,

цивільного, терористичного та злочинного характеру, виокремлення узгоджених заходів з попередження використання ІКТ-технологій у терористичних цілях, обмеження використання інформаційних озброєнь, координації дії правоохоронних органів з попередження інформаційної агресії, аналіз проблеми координації національних законодавств з проблеми інформаційної діяльності, оцінка можливостей допомоги країнам-жертвам інформаційної агресії.

РФ наполягала на розробленні міжнародного документа з міжнародної інформаційної безпеки, згідно з яким держави та інші суб'єкти міжнародного права зобов'язуються відповідати на основі міжнародних правових принципів за діяльність у глобальному інформаційному просторі, яка здійснюється з їхніх територій чи територій їхньої юрисдикції, тобто створити універсальний режим міжнародної інформаційної безпеки.

Враховуючи, що проблеми інформаційної безпеки пов'язані із сучасними формами тероризму, ГА ООН у розвиток резолюцій про *„Досягнення ІКТ у контексті міжнародної безпеки"* ГА ООН ухвалила резолюцію 57/239 (2003р.) ***„Створення глобальної культури кібербезпеки"***, до преамбули якої увійшли посилання на резолюції ГА ООН з міжнародної інформаційної безпеки і боротьби із злочинним використанням ІКТ, що підкреслює багатогранність проблеми інформаційної безпеки і наявність тісного зв'язку між її різними аспектами. У резолюції, зокрема, йдеться про те, що кібербезпека залежить не тільки від дій державних чи правоохоронних органів, а й превентивних заходів і підтримки всього світового співтовариства. У додатку ***„Елементи для створення глобальної культури кібербезпеки"*** міститься перелік „складових", на основі яких має забезпечуватися безпека мереж — від етики і демократії до відповідальності, реагування, оцінки ризиків та управління безпекою — і які сприятимуть державам-членам ООН у розробці міжнародно-правової бази інформаційного суспільства. За наполяганням США, пріоритетом позиції якої є проблема боротьби з міжнародним тероризмом в усіх аспектах міжнародного співробітництва, зокрема боротьби з інформаційним тероризмом, інформаційною злочинністю та безпека комп'ютерних мереж, ГА ООН ухвалила резолюцію 567/27 ***„Заходи з ліквідації міжнародного тероризму"*** (2003 р.). У резолюції підкреслюється важливість розгляду проблеми в рамках ООН, засуджуються прояви тероризму та їх згубні наслідки для суспільств у різних країнах світу, підкреслюється, що боротьба держав з тероризмом має здійснюватися згідно зі Статутом ООН, нормами міжнародного права і відповідними міжнародними конвенціями, пропонується терміново розробити проект міжнародної конвенції з ліквідації тероризму і стверджується провідна роль ООН та її спеціалізованих установ у попередженні терористичних загроз різного характеру, зокрема усіх форм інформаційного тероризму (медіа-, кібер- та психотероризму, лінку, чіпінгу тощо) [41; 51; 52].

58-ма (2003 р.) та 59-та (2004 р.) сесії ГА ООН закликали держави-члени сприяти і в подальшому розробці міжнародних документів у сфері

міжнародної безпеки з метою включення цих норм до національних законодавств і регулювання міжнародних відносин в інформаційній сфері. В обговоренні було підкреслено, що наукові та технологічні розробки потребують міжнародного контролю за їх поширенням, оскільки можуть бути застосовані як в мирних, так і воєнних цілях, водночас підтримуючи вільний розвиток науки та вільний обмін науковою інформацією. Проблемним є забезпечення вільного доступу до новітніх технологій в інформаційній сфері в умовах необхідності інформаційної безпеки та запобігання тероризму. Саме воєнний аспект використання ІКТ-технологій виступає першочерговим і найбільш вагомим за потенційними наслідками застосування інформаційних озброєнь.

Міжнародне співтовариство також зацікавлено в поширенні та використанні ІКТ та технологічних інновацій, бо це впливає на інтереси всього світу і вимагає максимальної ефективності дій всієї глобальної спільноти. ІКТ, зазначається у резолюціях, створюють принципово нові моделі діяльності в науці, глобальному управлінні, проектуванні, медицині, валютно-банківських операціях, стають вирішальним чинником трудових ресурсів та трудового потенціалу, стрімкого зростання творчої праці. Саме ІКТ-технології забезпечують соціальні, економічні, правові, культурні і технологічні умови зберігання та активізації нових ідей та їх широкого використання[1].

60-та сесія ГА ООН розглянула як доповідь Генерального секретаря про модернізацію Резолюції 59/61 *„Досягнення у сфері інформатизації і телекомунікацій у сфері міжнародної безпеки"*, так і відповіді урядів Чилі, Мексики, Бразилії, Канади, в яких подано погляди та загальні оцінки щодо проблеми міжнародної інформаційної безпеки у сучасному світі, визначення основних понять з інформаційної безпеки, включаючи сучасні загрози — кібер-, медіа- та психотероризм, змісту відповідних міжнародних концепцій про безпеку глобальних інформаційних телекомунікаційних систем.

У доповіді було наголошено, що країни Центральної та Південної Америки, Бразилія, Мексика та Чилі переконані, що інформація та системи телекомунікацій є стратегічними сферами, важливість яких необхідно врахувати у системі підтримання міжнародної безпеки. Уряди цих країн переконані, що ці сфери мають стати предметом консультації між державами в інтересах постійного міжнародного співробітництва, захисту вільного поширення інформації та для сприяння мирного використанню інформаційно-комунікаційних технологій в контексті роззброєння і нерозповсюдження високотехнологічних озброєнь.

Особливий акцент було зроблено у відповіді уряду Бразилії на вербальну ноту Генерального секретаря ГА ООН щодо широкомасштабного використання ІКТ-технологій та систем штучного інтелекту (озброєнь кібервійни) у збройних конфліктах сучасності. Було наголошено, що у збройних силах деяких країн створено спеціальні військові підрозділи для проведення мобільних спеціальних інформаційних операцій, наслідком яких є руйнування життєвоважливих об'єктів інфраструктури (від часткового порушення систем уп-

равління військами, систем державного політичного та економічного управління до практично повного руйнування систем життєзабезпечення всієї держави), тому кібервійна в найближчому майбутньому розглядається як головний вид бойових дій, нападу та наступальних озброєнь під час воєнних міждержавних конфліктів. Досягнення кіберозброєнь також можуть бути використані терористичними організаціями, що призведе до непередбачуваних негативних наслідків. Визнаючи важливість проблеми міжнародної інформаційної безпеки Бразилія пропонує такі шляхи її вирішення:

1) міжнародне співтовариство повинно створити ефективний механізм протидії злочинній та терористичній діяльності на основі ІКТ-технологій;
2) міжнародному співтовариству необхідно розглянути питання про можливі наслідки кібервійни в контексті роззброєння і нерозповсюдження та міжнародного права про збройні конфлікти і звичаї ведення війни.

Наголошуючи саме на загрозі кібертероризму Бразилія запропонувала державам-членам ООН на основі співробітництва вжити наступних заходів з метою: створення резервних та альтернативних мереж для захисту життєвоважливих структур; визначення нових ефективних методів захисту, які дозволяють виключити або мінімізувати наслідки кібератак; взаємодії між державним та приватним секторами для досягнення необхідного рівня захисту та обігу інформації; проведення переговорів щодо ухвалення міжнародної конвенції з кіберзлочинності; гарантування спільноті доступу до інформаційних ресурсів та технологій в рамках суспільних та комерційних потреб; розробки процедур про повідомлення компетентних національних органів про кіберзагрози на взаємній основі; підвищення рівня інформування населення про значення кібербезпеки.

Визнаючи ефективність використання інформаційних озброєнь в міждержавних конфліктах Бразилія запропонувала ГА ООН широко пропагувати ідею підготовки конвенції з міжнародної інформаційної безпеки, яка охоплювала б проблеми ідентифікації, характеристики і класифікації засобів ведення інформаційної війни, ідентифікації і класифікації інформаційних озброєнь, попередження використання кіберозброєнь і знань терористичними групами, гарантії рівності всіх країн щодо їх прав на захист від кібератак, створення міжнародних механізмів, які б регулювали конфлікти з елементами кібераг-ресії, створення глосарію ООН щодо визначення основних понять у сфері *міжнародної інформаційної безпеки.*

У відповіді уряду Канади підкреслено, що інформаційна інфраструктура держави, яка включає сектори енергетики, комунального господарства, ІКТ, фінансів, охорони здоров'я, водопостачання, продовольства, транспорту, державного управління та промисловості, є ключовим компонентом життєзабезпечення держави. У 2003 р. було створено спеціальну урядову структуру з питань суспільної безпеки та надзвичайних ситуацій, до компетенції якої віднесено відповідальність за попередження та аналіз кіберзагроз для урядових си-

стем, для національної безпеки, безпеки суспільних та комерційних комунікацій, а також за розробку оперативних стандартів для сертифікації і акредитації систем та ступеня їх безпеки.

У 2004 р. Канада вперше опублікувала програмний документ *„Національна політика у сфері безпеки"*, в якому представлена комплексна стратегія та план дій боротьби із сучасними та майбутніми інформаційними загрозами, пропозицію щодо створення національного координаційного центру реагування на кіберінциденти. Канада є учасником багатосторонніх ініціатив з проблем кібербезпеки і розглядає питання про підготовку національних, регіональних та міжнародних законів щодо кібербезпеки з врахуванням стандартів міжнародного співробітництва прав людини та попередження злочинності [53; 54].

60-та сесія ГА ООН, попри пропозиції групи урядових експертів ухвалити проект міжнародної конвенції з інформаційної безпеки, ухвалила резолюцію 60/45 *„Досягнення у сфері інформатизації і телекомунікацій у сфері міжнародної безпеки"*, в якій підкреслила необхідність продовжити багатосторонні консультації щодо існуючих та потенціальних інформаційних загроз та створення міжнародних концепцій щодо безпеки глобальних інформаційних та телекомунікаційних систем [55].

При розгляді проекту документу з міжнародної інформаційної безпеки на засіданні Першого комітету ООН за проголосували 163 країни Азії, Африки, Латинської Америки, Європи, СНД, проти 1 країна – США.

Проблема не ухвалення документу з міжнародної інформаційної безпеки на 60 сесії ГА ООН пов'язана з неузгодженістю позицій групи урядових експертів (до неї увійшли представники 15 держав, зокрема РФ, Китаю, США, Франції, Великої Британії, Іорданії, Білорусії, Малі, Малайзії, Мексики, Кореї, ПАР – голова групи представник РФ А.В. Крутських) з таких питань, як практичні заходи з попередження розробки, виробництва, використання та поширення інформаційних озброєнь в рамках глобального режиму міжнародної інформаційної безпеки. Загальні параметри такого режиму, запропоновані на основі пропозицій РФ, охоплюють відмову від розробки, створення і використання інформаційних озброєнь; спрямованого нападу за допомогою інформаційних озброєнь на інші держави; несанкціонованого втручання в інформаційні системи та неправомірного їх використання, монополії в міжнародному інформаційному просторі; протидії доступу до новітніх ІКТ-технологій, створення технологічної залежності у сфері ІКТ від інших держав, заохочення терористичних, екстремістських та злочинних угруповань до використання інформаційних озброєнь, розробки планів та доктрин ведення інформаційних воєн, інформаційної експансії (маніпулювання, викривлення, порушення основних прав і свобод, встановлення контролю над інформаційно-комунікаційними структурами) тощо.

До міжнародного договору передбачалося додати положення про: ознаки і класифікацію інформаційних озброєнь та дотичних засобів; заходи з обме-

ження обігу інформаційних озброєнь (розробки, виробництво, застосування); заходи з попередження загрози інформаційних воєн, визнання інформаційних озброєнь зброєю масового ураження, забезпечення свободи міжнародних інформаційних потоків, попередження використання інформаційних озброєнь терористичними угрупованнями, механізм контролю, моніторингу, спостереження та вирішення конфліктних ситуацій, координація правоохоронних дій держав, сертифікація ІКТ та гарантії їх інформаційної безпеки, гармонізація міжнародного права та національних законодавств з міжнародної інформаційної безпеки [55].

Паралельно з розглядом проблем міжнародної безпеки в галузі інформатизації та телекомунікацій Перший комітет ООН запропонував провести ревізію резолюції 53/73 „Роль науки і техніки в контексті міжнародної безпеки і роззброєння" (1999р), враховуючи необхідність міжнародного узгодження керівних принципів щодо передачі високих технологій подвійного використання, зокрема ІКТ-технологій військового призначення, для законних оборонних потреб всіх держав та підтримання міжнародного миру і безпеки [56].

61-ша сесія ГА ООН підтвердила зацікавленість держав у розгляді проекту міжнародної конвенції з інформаційної безпеки, оскільки значний прогрес у сфері нових інформаційних технологій та засобів телекомунікацій, таких, як: Інтернет, факсовий, мобільний, бездротовий, космічний, кабельний та мультимедійний (інтегрований) зв'язок, відкрив необмежений доступ світового співтовариства до глобальних інформаційних ресурсів і, зокрема до потенційно конфіденційної інформації. Підкреслюючи, що цей процес сприяє прогресивному розвитку цивілізації, інтелектуалізації виробництва та загального добробуту держав ГА ООН підкреслює проблему забезпечення інформаційної безпеки на національному рівні та участі у міжнародному співробітництві в цій сфері шляхом ухвалення відповідних міжнародних концепцій.

Серед заходів для зміцнення інформаційної безпеки в глобальному масштабі ГА ООН запропонувала національним урядам, експертам аналітичних центрів, силовим структурам ООН здійснити компетентний аналіз проблем у сфері інформаційної безпеки на міжнародному рівні, визначити основні критерії щодо безпеки інформації і телекомунікацій або незаконного використання цих систем за допомогою Інтернет, розробити міжнародні принципи безпеки інформаційних та телекомунікаційних систем світу в контексті боротьби з тероризмом та торгівлі конфіденційною інформацією, враховуючи, що такі технології можуть бути використані для дестабілізації безпеки держав, впровадити у військовій та оборонній сфері телекомунікаційні системи на основі новітніх досягнень технологій інформаційної безпеки. У рекомендації зазначено, що саме в рамках політики на основі національного законодавства в сфері телекомунікацій, повинна забезпечуватися інформаційна безпека держави.

Концепцію спільної відповідальності держав та міжнародного співтовариства за забезпечення міжнародної інформаційної безпеки було запропоно-

вано КНР, яка вважає, що використання ІКТ-технологій має відповідати цілям статуту ООН та основним принципам міжнародних відносин, серед яких виділяє: гарантування безперешкодного потоку інформації з врахуванням національного суверенітету і безпеки та поваги до історичних, культурних і політичних традицій різних країн; права кожної країни на використання власного кіберпростору на основі національного законодавства; активізації міжнародного співробітництва у сфері ІКТ для подолання асиметрії інформаційного розвитку країн та використання переваг новітніх технологій для економічного зростання.

КНР підтримує ідею створення під егідою ООН групи урядових експертів для проведення досліджень щодо загроз і проблем в сфері інформаційної безпеки та вироблення відповідної міжнародної політики регулювання. Міжнародне співробітництво є необхідною умовою, оскільки кіберзлочинність не визнає кордонів і боротися з нею традиційними методами неможливо [57; 58].

Україна як держава-засновниця ООН підтримує розгляд проблеми міжнародної інформаційної безпеки в рамках організації, у своїй діяльності виходить з концепції актуальності міжнародного співробітництва в інформаційній сфері, стратегію на майбутнє визначає як необхідність подолання глобальної напруженості між інформаційно розвиненими та інформаційно бідними країнами, запобігання міжнародним конфліктам із застосуванням інформаційних озброєнь, забезпечення основних прав і свобод людини, протидії впливу на моральні цінності світової спільноти.

За ініціативи України в ООН та її спеціалізованих установах були обговорені проблеми узгодження міжнародної стратегії інформаційної політики та національні інформаційні програми, міжнародно-правові аспекти функціонування мережі Internet (захист конфіденційності, інфоетика, поширення ідей забороненого змісту тощо). На національному рівні було ухвалено низку законів та інших документів правового характеру щодо проблеми інформаційної безпеки („Про національну систему конфіденційного зв'язку" (2002), „Про державну таємницю" (1994), „Про захист інформації в автоматизованих системах" (1994), „Про концепцію технічного захисту інформації в Україні" (1997), „Про телекомунікації" (2004), „Про першочергові завдання щодо впровадження новітніх ІКТ-технологій" (2005), „" (2006), „" (2006), в яких зафіксовано принципи міжнародних угод, підписаних Україною в рамках ООН та її спеціалізованих установ, визначено національні пріоритети з інформаційної безпеки, зокрема впровадження національних стандартів з питань криптографічного захисту інформації, розробка нормативних актів з попередження інформаційної злочинності, боротьби з інформаційним тероризмом, внесення змін до Концепції національної безпеки та оборони з урахуванням чинника міжнародної інформаційної безпеки тощо [59; 68].

Водночас Україна підтримує міжнародну діяльність ООН, моральний авторитет Організації, її провідну роль у врегулюванні сучасних глобальних

проблем та визнання її як міжнародного форуму для ухвалення спільних рішень в добу інформаційних трансформацій.

1.3. Міжнародні політичні конфлікти: інтереси, потенціали, загрози, моделі

Проблеми досліджень політичних конфліктів та криз в міжнародних відносинах, аналіз та прогнозування розвитку конфліктів на початку XXI століття набуває все зростаючої актуальності. Глобальні зміни на світовій арені, різке загострення конфлікту на Близькому Сході, не затухаючі конфлікти в Європі та Латинській Америці, Африці, Азії і, нарешті, теракти 11 вересня 2001 р. в США та в жовтні 2002 р. в Москві, події в Афганістані та Іраку, інші численні приклади свідчать, що рівень нестабільності у світі і на початку XXI століття є дуже високим і тенденцій до його зниження не спостерігається. В цьому зв'язку першочерговою проблемою стає розробка методів, механізмів і засобів, які дозволяють заздалегідь розпізнати конфліктну ситуацію або потенціальний конфлікт, сформувати досить надійний прогноз його виникнення, розвитку та виробити ефективні рекомендації щодо його розв'язання або врегулювання. Все це вимагає розробки та використання відповідного інструментарію.

У працях автора [69; 70] визначені методологічні засади аналізу міжнародних політичних конфліктів сучасності, [71] класифіковано чинники, що визначають стан держави, її положення на світовій арені, оцінку рівня досягнення національних інтересів, а також наведені дані та методика оцінки конфліктного потенціалу держави в цілому і за кожною із сфер життєдіяльності, а також конфліктної напруженості у міждержавних відносинах або між державами та блоками і союзами держав, міждержавними організаціями.

Основна модель для аналізу внутрішнього розвитку суб'єкта міжнародних відносин (держави, блоку, союзу держав) в певній і-й сфері життєдіяльності A_i полягає в **оцінюванні рівня досягнення її національного інтересу** $I^0_{Ai}(t)$ в будь-який момент часу t через складові циклів цивілізаційного та локального виміру - довгострокового, середньострокового, короткострокового:

$$I^0_{A_i}(t) = 0{,}5 - I^0_d \cos\left(2\pi \frac{t - t_d}{T_d}\right) - I^0_c \cos\left(2\pi \frac{t - t_c}{T_c}\right) - I^0_k \cos\left(2\pi \frac{t - t_k}{T_k}\right) \quad (1)$$

де I^0_d, I^0_c, I^0_k - амплітуди, T_d, T_c, T_k - періоди, t_d, t_c, t_k - значення аргументів, при яких досягаються мінімуми відповідно довгострокового, середньострокового та короткострокового циклів.

При значеннях амплітуд $I^0_d = 0{,}25\ \ 0{,}1$; $I^0_c = 0{,}1\ \ 0{,}05$; $I^0_k = 0{,}05$ **[75], значення оцінки рівня досягнення суб'єктом міжнародних відносин національних інтересів в певній сфері** $I^0_{A_i}(t)$ буде знаходитись в діапазоні [0...1], де 0 відповідає найгіршому (невигідному, небажаному) стану, а 1 - найкращому (бажаному, ідеальному) стану розвитку.

Величина

$$P^0_{A_i}(t) = 1 - I^0_{A_i}(t) \qquad (2)$$

визначає ступінь незадоволення суб'єктом міжнародних відносин A своїм внутрішнім станом у i - ій сфері, тобто визначає **конфліктний потенціал** суб'єкта A у цій сфері на момент часу t. В цілому для суб'єкта A внутрішній конфліктний потенціал $P^0_A(t)$ можна визначити із співвідношення

$$P^0_A(t) = \sum_{i=1}^{m} \alpha_i(t) P^0_{A_i}(t), \qquad (3)$$

де m - кількість врахованих сфер;

$\alpha_i(t)$ - функція впливу i-ої сфери на загальний конфліктний потенціал. В будь-який момент часу t повинна виконуватися умова: $\sum_{i=1}^{m} \alpha_i(t) = 1$. В загальному випадку $\alpha_i(t)$ - нелінійна функція від часу t. В найпростіших випадках $\alpha_i(t) = \alpha_i$, тобто є константою, ваговим коефіцієнтом.

Для аналізу **конфліктної напруженості** $U_{AB}(t)$, $U_{BA}(t)$ у відносинах двох суб'єктів міжнародних відносин A та B використаємо співвідношення

$$\begin{aligned} U_{AB}(t) &= P_A(t) - P_B(t); \\ U_{BA}(t) &= P_B(t) - P_A(t). \end{aligned} \qquad (4)$$

Очевидно, що $U_{AB}(t) = -U_{BA}(t)$. Знаки (+) або (-) визначають суб'єкта з більшим конфліктним потенціалом.

Але наявність конфліктної напруженості у стосунках між суб'єктами міжнародних відносин ще не є ознакою виникнення конфлікту. Згідно з висновком В.Свєтлова конфлікт, із-за своєї багатофакторної природи, є системним явищем, яке визначає його структурні та динамічні властивості [76].

Згідно з термінологією системного аналізу, конфлікт - це такий вид зворотного зв'язку, який визначає:

- нездатність системи зберігати свою якість в попередніх якісних межах свого буття, тобто - виконувати своє призначення;
- втрату системою базисної стабільності (стійкості) розвитку в попередньому напрямі з попереднім набором і залежністю причинних змінних [76].

Функціонально конфлікт - стан системи, коли вона нездатна асимілювати, компенсувати, нейтралізувати наслідки негативного зворотного зв'язку між причинними змінними, який суттєво дестабілізує її нормальну життєдіяльність в попередній якості.

У міжнародних відносинах **міжнародний політичний конфлікт** визначається в сприйнятті сторонами (суб'єктами) зіткнення протилежних інтересів, цілей, цінностей, поглядів як **загрози** національній безпеці, і пов'язаних з їх реалізацією дій окремих держав, груп держав, об'єднаних у союзи, коаліції, або організацій, що їх представляють.

З системних позицій причиною конфлікту може бути виникнення негативного зворотного зв'язку між елементами системи або між елементами системи і зовнішнім середовищем. В першому випадку конфлікт визначають як внутрішній, в другому - як зовнішній. Однак, в дійсності, зовнішній конфлікт - це прояв внутрішніх протиріч, і зовнішні конфлікти також впливають на внутрішні, підсилюючи чи послаблюючи їх, або одночасно визначаючи одне й інше [76].

Помилковим є ототожнювання конфлікту з антагонізмом у відносинах між суб'єктами, наприклад державами чи блоками держав. Незалежно від форм прояву антагонізму: ворожі почуття, спори, санкції, агресія, насилля, війна - це специфічні форми вирішення конфлікту, реакція на його виникнення, яка може бути не менш сприятливим чи стійким засобом його вирішення, ніж синергизм (переговори, угоди, поступки, компроміси тощо). Таким чином, системна природа конфлікту полягає в тому, що він надає необхідні умови появи, знищення, диференціації, зміни саморегульованих систем [76].

Структурна модель конфлікту або безконфліктної ситуації визначає наявність в ній наступних компонентів [76]:

- непорожня множина елементів системи;
- непорожня множина відношень між елементами системи;
- позначення кожного відношення як позитивного (доброзичливе ставлення, прямопропорційний вплив тощо) або негативного (недоброзич-

ливе ставлення, оберненопропорційний вплив) з можливою числовою або функціональною залежністю ступеня позитивності чи негативності відношення;

- циклів позитивного або негативного зворотного зв'язку.

Таким чином, структурною моделлю міжнародних відносин може бути дираф - орієнтований граф **G(X,U)** з множиною вершин **X**, що відповідають суб'єктам міжнародних відносин, та множиною означених дуг (ребер) **U**, що позначають взаємозв'язки між суб'єктами. Так, наприклад, в якості найпростішої структурної моделі взаємодії суб'єктів **A** і **B**, можна запропонувати диграф (рис. 1):

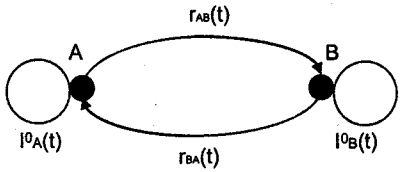


Рис.1. Структурна модель взаємодії суб'єктів міжнародних відносин **A** і **B**.

На рис. 1 дуга **AB** позначає вплив суб'єкта **A** на суб'єкт **B**, а ступінь і знак впливу в момент часу **t** визначає значення величини **rAB(t)**. Дуга **BA** позначає вплив суб'єкта **B** на суб'єкт **A**, ступінь і знак впливу визначає значення величини **rBA(t)**. Оцінка рівня внутрішнього розвитку суб'єкта **A** (без урахування взаємодії з **B**) визначається петлею (циклом) з характеристикою **I0A(t)**, оцінка рівня внутрішнього розвитку суб'єкта **B** (без урахування взаємодії з **A**) визначається петлею (циклом) з характеристикою **I0B(t)**.

Значення оцінки рівня розвитку **IA(t)** суб'єкта **A** та оцінки рівня розвитку **IB(t)** суб'єкта **B** з урахуванням їх взаємодії, тобто взаємного впливу, можна визначити з системи рівнянь:

$$\begin{cases} I_A(t) = I_A^0(t) + r_{BA}(t) I_B(t) \\ I_B(t) = I_B^0(t) + r_{AB}(t) I_A(t) \end{cases} \qquad (5)$$

Розв'язок цієї системи має вигляд:

$$\begin{cases} I_A(t) = \dfrac{I_A^0(t) + r_{BA}(t) I_B^0(t)}{1 - r_{BA}(t) r_{AB}(t)} = \dfrac{I_A^0(t) + r_{BA}(t) I_B^0(t)}{1 - R(t)}; \\ I_B(t) = \dfrac{I_B^0(t) + r_{AB}(t) I_A^0(t)}{1 - r_{BA}(t) r_{AB}(t)} = \dfrac{I_B^0(t) + r_{AB}(t) I_A^0(t)}{1 - R(t)}; \end{cases} \qquad (6)$$

при виконанні умов:

$$0 \le I_A(t) \le 1 \quad ; \quad 0 \le I_B(t) \le 1. \tag{7}$$

Добуток $R(t) = r_{AB}(t) * r_{BA}(t)$ є функцією (коефіцієнтом) зворотного зв'язку циклу (**AB, BA**). Таким чином, властивості такої системи визначаються структурно та динамічно оцінками власних (внутрішніх) процесів $I^0_A(t)$ суб'єкта **A** та $I^0_B(t)$ суб'єкта **B**, а також знаками та значеннями величин відношень $r_{AB}(t)$ та $r_{BA}(t)$.

З позицій структурного аналізу необхідно з'ясувати: чи є система структурно конфліктною або безконфліктною (збалансованою). Динамічний аналіз (дослідження поведінки системи в часі) повинен дати відповідь, чи є система стабільною, стійкою.

Дираф **G(X,U)** називають незбалансованим, якщо його елементи знаходяться у відношенні негативного зворотного зв'язку. Незбалансованість дирафу структурний аналог конфліктного стану системи.

Необхідною і достатньою умовою незбалансованості дирафа, і тим самим конфліктності системи, є наявність в ньому непарного числа негативних відношень (відношень, які мають в момент часу t знак (-)) [76]. Це означає, що система знаходиться в конфліктному стані, якщо і тільки якщо:

- вона не збалансована;
- щонайменше один її цикл має знак (-), тобто добуток знаків дуг, що належать циклу, має знак (-);
- існує щонайменше один елемент, який зв'язаний з іншим елементом системи шляхами, що мають знаки (+) та (-) одночасно.

Наслідки цього визначення для системи міжнародних відносин:

1. Якщо серед елементів деякої системи (підсистеми) міжнародних відносин існують негативні відношення, то це не означає, що система (підсистема) знаходиться в конфліктному стані. Тільки асиметрія негативних відношень в циклі робить систему конфліктною.
2. Будь-яка система міжнародних відносин, розподілена більш ніж на два взаємонегативні полюси (блоки) знаходиться в стані конфлікту.
3. У безконфліктній системі (підсистемі) міжнародних відносин кожен елемент (суб'єкт) відчуває позитивне ставлення до себе з боку інших елементів системи (підсистеми).
4. У безконфліктній системі (підсистемі) кожен елемент (суб'єкт) знаходиться у позитивному зворотному зв'язку з самим собою.
5. Незалежно від складності системи (числа елементів n), кількість можливих як безконфліктних, так і конфліктних станів дорівнює 2^{n-1}.
6. Максимальна кількість можливих способів вирішення конфлікту дорівнює кількості способів вирішення для її максимального циклу.

Ступінь конфліктності реальної системи в певний момент часу t визначають із співвідношення:

$$M = \frac{b^-}{b} = 1 - \frac{b^+}{b} \qquad (8)$$

де b - загальна кількість циклів диграфу $G(X,U)$;

b^+ - кількість *збалансованих циклів*;

b^- - кількість незбалансованих циклів.

Для диграфа $G(X,U)$, як моделі відносин двох реальних суб'єктів (рис.1), ступінь конфліктності M може приймати значення 0 або 1, оскільки $b = 1$, $b^- = 0$ або 1. Кількість можливих структурно конфліктних або безконфліктних станів дорівнює $2^{2-1} = 2$.

Система вважається динамічно стабільною якщо, і тільки якщо, для кожного скінченого зовнішнього імпульсу існує межа (границя) змін значень її змінних, тобто існує точка насичення [76]. Динамічно стабільні системи *складають множину лінійних, а динамічно нестабільні системи - множину* нелінійних систем.

Дослідити динамічні властивості системи міжнародних відносин двох суб'єктів (рис.1), це значить дослідити динамічні властивості функції (коефіцієнта) зворотного зв'язку $R(t)$. З динамічної точки зору як конфліктні, так і безконфліктні системи потребують подальшої конкретизації.

Проведемо аналіз розв'язків (6,7) з використанням наступних умов:

1. Оскільки значення змінних $I_A(t)$ та $I_B(t)$ повинні належати діапазону $[0...1]$, то і значення конфліктних потенціалів $P_A(t) = 1 - I_A(t)$ держави **A** та $P_B(t) = 1 - I_B(t)$ світової спільноти **B** також повинні знаходитись в діапазоні $[0...1]$.
2. Відношення $r_{AB}(t)$, $r_{BA}(t)$ можуть бути визначені:

   - константами:

$$r_{AB}(t) = \pm r_{AB}^0;$$
$$r_{BA}(t) = \pm r_{BA}^0; \qquad (9)$$

   - лінійними функціями від конфліктної напруженості:

$$r_{AB}(t) = \pm r_{AB}^0 \pm a[P_A(t) - P_B(t)];$$
$$r_{BA}(t) = \pm r_{BA}^0 \pm b[P_B(t) - P_A(t)]; \qquad (10)$$

- функціями перемикання:

$$r_{AB}(t)=\begin{cases}\pm r_{AB}^{01} & при \quad P_A(t)-P_B(t)<U_{Œ};\\ \pm r_{AB}^{02} & при \quad P_A(t)-P_B(t)\geq U_{Œp};\end{cases}$$

$$r_{BA}(t)=\begin{cases}\pm r_{BA}^{01} & при \quad P_B(t)-P_A(t)<U_{Œ};\\ \pm r_{BA}^{02} & при \quad P_B(t)-P_A(t)\geq U_{Œp};\end{cases} \qquad (11)$$

- гістерезисними функціями

$$r_{AB}(t)=\begin{cases}\pm r_{AB}^{01}\pm a[P_A(t)-P_B(t)] & при\ зростанні \quad U_{AB}(t);\\ \pm r_{AB}^{02}\pm a[P_A(t)-P_B(t)] & при\ зменшенні \quad U_{AB}(t);\end{cases}$$

$$r_{BA}(t)=\begin{cases}\pm r_{BA}^{01}\pm b[P_B(t)-P_A(t)] & при\ зростанні \quad U_{BA}(t);\\ \pm r_{BA}^{02}\pm b[P_B(t)-P_A(t)] & при\ зменшенні \quad U_{BA}(t);\end{cases} \qquad (12)$$

- експоненційними функціями:

$$r_{AB}(t)=r_{AB}^{0}e^{a[P_A(t)-P_B(t)]};$$

$$r_{BA}(t)=r_{BA}^{0}e^{b[P_B(t)-P_A(t)]}; \qquad (13)$$

- логарифмічними функціями:

$$r_{AB}(t)=r_{AB}^{0}\ln(a[P_A(t)-P_B(t)]);$$

$$r_{BA}(t)=r_{BA}^{0}\ln(b[P_B(t)-P_A(t)]); \qquad (14)$$

- тригонометричними функціями:

$$r_{AB}(t)=r_{AB}^{0}+a\sin\{2\pi[(P_A(t)-P_B(t)]\};$$

$$r_{BA}(t)=r_{BA}^{0}+b\sin\{2\pi[P_B(t)-P_A(t)]\}; \qquad (15)$$

- іншими трансцендентними функціями.

$$\text{а)}\ r_{AB}(t)>0\ ,\ r_{BA}(t)<0\ . \qquad (16)$$
$$\text{б)}\ r_{AB}(t)<0\ ,\ r_{BA}(t)>0\ .$$

Розглядаючи міжнародні відносини в умовах глобалізації, дослідники найчастіше вирізняють її економічну та політичну складові. Згідно з цією логікою, експансія капіталу приводить до того, що економічні процеси, які протікають в будь-якій країні світу, досить швидко впливають на кон'юнктуру ринку в інших країнах або у світі в цілому.

Водночас політичні інтереси держав виходять за межі власної території і поширюються настільки далеко, наскільки далеко сягнули економічні інтереси вихідців з цих країн, або в ряді випадків охоплюють ті регіони світу, в яких сконцентровані виробництва, що суттєво впливають на ситуацію в країнах-метрополіях [77]. Це дає підстави розширити аналіз системи міжнародних відносин, розглядаючи кожну із складових (держави, світову спільноту в цілому) як системи, що складаються із двох підсистем: економічної та політичної. Тоді структурна модель взаємодії суб'єктів **A** і **B** набуде нових форм та змісту (рис.2):

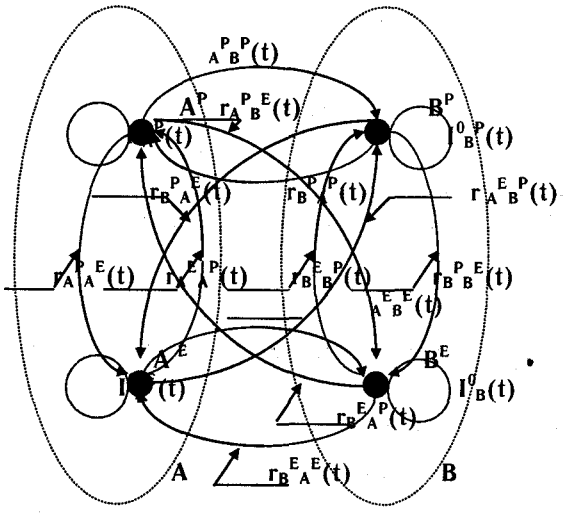


Рис.2 . Структурна модель взаємодії суб'єктів міжнародних відносин **A** і **B** з поданням їх підсистем (політичних A^P , B^P та економічних A^E , B^E)

Збільшення числа досліджуваних причинних змінних, наприклад до 4 (політика, військова сфера, економіка, соціальна сфера), до 8 (політика, інформаційна сфера, військова сфера, науково-технічна сфера, економіка, екологія, соціальна сфера, національно-етнічна сфера), або до 16 (політика, політична еліта, інформаційна сфера, правова сфера, військова сфера, освіта та культура, науково-технічна сфера, демографічна сфера, економіка, природні ресурси, екологія, соціальна сфера, релігійна сфера, національно-етнічна сфера, морально- психологічна сфера, ідеологія) і т.д. ускладнюють аналітику відповідних конфліктних ситуацій. Тому в цих випадках доцільним є комп'ютерний аналіз розв'язку рівнянь, заданих у матричній формі:

$$\left\|I_A\right\|_t = \left\|I_A^0\right\|_t \times \left\|r_{AA}\right\|_t + \left\|I_B^0\right\|_t \times \left\|r_{BA}\right\|_t;$$

$$\left\|I_B\right\|_t = \left\|I_B^0\right\|_t \times \left\|r_{BB}\right\|_t + \left\|I_A^0\right\|_t \times \left\|r_{AB}\right\|_t; \qquad (17)$$

де $\|\mathbf{I_A}\|_t$, $\|\mathbf{I_B}\|_t$ - вектори-стовпці значень причинних змінних, що характеризують стан суб'єктів **A** та **B** у момент часу t;

$\|\mathbf{I_A^0}\|_t$, $\|\mathbf{I_B^0}\|_t$ - вектори-стовпці значень причинних змінних, що характеризують стан суб'єктів **A** та **B** без урахування взаємодії між ними;

$\|\mathbf{r_{AA}}\|_t$, $\|\mathbf{r_{AB}}\|_t$, $\|\mathbf{r_{BB}}\|_t$, $\|\mathbf{r_{BA}}\|_t$ - матриці коефіцієнтів взаємовпливів суб'єктів **A** та **B**, обрахованих на момент часу t.

Таким чином, запропонований автором підхід до аналізу структурної та динамічної конфліктності акторів в системі міжнародних відносин дозволяє оцінити рівні розвитку у різних сферах діяльності акторів, їх конфліктні потенціали, конфліктну напруженість, а також показати шляхи її зниження як за рахунок введення (ліквідації) взаємодії, так і за рахунок зміни знаків та значень величини цих взаємодій.

1.4. Інформаційна безпека в інформаційну добу: два погляди на проблему

Погляд перший. Інформаційна безпека — стратегічне поняття, яке входить складовою у ширші, багатокомпонентні категорії, такі, як ***"міжнародна безпека", "національна безпека", "політика в галузі національної безпеки", "національна стратегія", "національні пріоритети"***. В сучасній зарубіжній і вітчизняній науковій думці існують

декілька підходів до тлумачення поняття "національна безпека". На наш погляд найбільш відповідним ері інформації є розширення самого поняття *національної безпеки* і визначення її як "міри відсутності загрози правам і свободам людини, базовим інтересам і цінностям суверенної національної держави" [80]. При цьому "принциповим" є такий порядок переліку об'єктів інформаційної безпеки: "особистість, суспільство, держава" [81]. Виходячи з цього ми розглядатимемо поняття "інформаційна безпека" саме в широкому розумінні цього концепту, розмірковуючи і про мінімізацію рівня загроз комунікаційним та інформаційним правам і свободам людини [82], і про базові інтереси і національні цінності держави. Тим самим сподіваємося довести, що процеси, які відбуваються в інформаційній сфері, революціонізуючим чином впливають на структурні зміни всіх інших сфер (політичної, економічної, соціокультурної, військової, екологічної тощо) і свідчать про перехід людства на новий рівень цивілізації — від індустріального суспільства до інформаційного.

Сутність цього переходу полягає у тому, що "інформація у різних видах і формах стає найважливішим виробничим ресурсом, який дає змогу економити всі інші види ресурсів, а стрімко зростаючі технічні можливості інформаційно-комп'ютерних технологій, систем і мереж є головним каталізатором швидкого розвитку і широкого впровадження в різні галузі економіки наукоємних, екологічно безпечних енергозберігаючих і ресурсозберігаючих технологій"[83]. Також слід додати, що нові інформаційно-комунікаційні технології (ІКТ) набувають пріоритетного значення самі по собі, перетворюються на найсуттєвіший компонент економічної і фінансової сфери [84-85]. Вони стають вирішальними й в усіх інших сферах, включаючи ідеологію, політику, науку, освіту, культуру, релігію, а також, — що є прикметним саме для інформаційного суспільства, — владно втручаються у приватну сферу людини.

Це дає змогу висунути гіпотезу про те, що чим далі, тим більше інформаційна безпека ставатиме важливим структурним компонентом усіх інших сфер національної безпеки і в цілому вирішальним фактором системи національної безпеки (СТБ) держави, навколо якої вона утворена.

Інформаційна безпека вже набуває значення того стрижня, того структуроутворюючого компонента, на якому будується вся система національної безпеки. Адже в інформаційному суспільстві канали, мережі і системи інформації і комунікації стають, так би мовити, і нервовою, і серцево-судинною системою суспільства водночас. Хочемо ще раз підкреслити, що основні реалії сьогодення детерміновані глобальними трансформаціями інформаційно-комунікаційних систем.

Для розуміння проблем інформаційної безпеки XXI століття слід усвідомлювати, що вони вимагають принципово нового осмислення й системного аналізу. Системний підхід потрібен тому, що "в сучасному світі не існують ізольовано наукові, технічні, технологічні, соціальні, економічні і політичні сфери діяльності людини. Зміни в кожній з цих сфер неодмінно даються взнаки на

інших сферах, проблеми однієї сфери взаємопов'язані з проблемами інших сфер" [84]. Виходячи з цього постулату чітко вимальовується необхідність системного підходу як до вирішення прикладних завдань, так і до теоретичних розробок системи інформаційної безпеки. В ракурсі системного підходу важливим також є врахування ієрархій інформаційно-комунікаційних систем різного рівня — від локального, комунального і національного до регіонального і глобального. Тільки завдяки такому системному аналізу можливі стратегічно виважені підходи до вирішення проблем інформаційної безпеки в інформаційну добу.

Одним із системоутворюючих концептів у розгляді проблем інформаційної безпеки є міжнародний потік інформації [86]. Розуміючи поняття "міжнародний потік інформації", як рух повідомлень через національні кордони між двома або більше національними і культурними системами, слід складати собі звіт, що сучасні ІКТ, розвиток Інтернету і експансія мультимедіаімперій набули глобальних масштабів. Це дає можливість говорити про глобальні інформаційні потоки, про їх силу і наповненість. Нині маємо констатувати, що сила, наповненість і напрями інформаційних потоків "Північ — Південь" характеризуються таким яскраво вираженим переважанням всіх своїх складових, що набули характеру виразної інформаційної загрози. Очевидною стає і релевантна слабкість інших окремих регіональних і національних інформаційних потоків (скажімо, "Південь — Північ", "Південь — Південь"), а також інформаційних потоків цілих континентів (найвиразніший приклад — Африка). Відповідно, можна говорити про те, що значна кількість країн і регіонів світу є постійними об'єктами інформаційної загрози, Неврівноваженість і незбалансованість інформаційних потоків, на яке ЮНЕСКО звернуло увагу ще в 1970-і рр., на межі століть катастрофічно поглиблюється. Прірва між інформаційно-багатими та інформаційно-бідними країнами стає все більшою. Чому так відбувається?

Розглянемо функціонування міжнародного інформаційного потоку в сучасному світі і визначимо його основні складові. Потік інформації в міжнародній системі схематично може бути поділений на дві стадії.

- По-перше, — стадію виробництва, куди входять джерело інформації або комунікатор, формування повідомлень та внутрішньо- і зовнішньомедійні перемінні, до яких, належать володіння, контроль, економічні ресурси, розміщення прибутку, засоби масової комунікації, комп'ютерно-інформаційні технології, апарат службовців, усвідомлення мети, типи змісту.
- По-друге, стадію дистрибуції, до якої належать поширення повідомлення, місце призначення для отримання повідомлення або реципієнт і, такі ж самі, як і на першій стадії, внутрішньо- та зовнішньомедійні перемінні.

За умов глобалізації, зростання міжнародного ринку ІКТ, інтернаціоналізації та конвергенції мультимедіа з інформаційними та телеко-

мунікаційними технологіями особливо важливою для збереження інформаційної безпеки окремої держави-нації стає стадія дистрибуції повідомлень. Держава може виробляти якісний інформаційний продукт, але в разі слабких національних можливостей щодо інфраструктури дистрибуції інформації, вона незмінно залишається незахищеною, бо саме стадія розповсюдження інформації у вигляді потоку вироблених нею повідомлень як у межах держави, такі за її межами дає змогу говорити і про задоволення інформаційних потреб громадян даного суспільства, і про поширення свого впливу на міжнародну спільноту. За Х.Моуланою, якщо тільки держава-нація не має контролю над усіма складовими стадії розповсюдження інформації, її повідомлення можуть бути неефективними.

Вище ми окреслили комунікаційну модель інформаційного міжнародного потоку. Але в сучасних умовах вона немислима без технологічного компонента, який відіграє величезну роль наприкінці XX - початку XXI століть. Комунікаційна вісь міжнародного інформаційного потоку поміж стадією виробництва і стадією дистрибуції перетинається технологічною віссю, яка репрезентує саме центральну, осьову роль, яку відіграють ІКТ в міжнародному комунікаційному процесі. Технологічна вісь складається з двох компонентів: комунікаційного хардвера, тобто фізичних носіїв повідомлень, до яких належать супутники, передаюче і приймаюче сигнал обладнання, мікрохвильові ретрансляційні станції і т. ін.; і комунікаційного софтвера, — широкого спектру ноу-хау і засобів утилізації хардвера.

При дослідженні питань інформаційної безпеки таке розуміння компонентів ІКТ важливо, бо дуже часто, розуміючи провідну роль, яку відіграють мультимедіа-імперії, та онлайнові гіганти (як-от America On-line, Time Warner, Microsoft, Yahoo!), відстежуючи контроль медіа-корпорацій в царині ЗМК, більше уваги приділяється їхньому володінню хардвером (тобто фізичними компонентами комунікаційної системи), тоді як контроль над софтвером є суттєвим у всьому процесі виробництва і дистрибуції повідомлень і їхнього впливу на масову свідомість. Х.Моулана підкреслює в ряді своїх праць, що абсолютна суверенність у формуванні та розповсюдженні повідомлень (*а, звідси, на нашу думку випливає й інформаційна безпека держави-нації — О.З.*) забезпечується тільки тоді, коли держава контролює і канали хардвера, крізь які повідомлення посилаються, і необхідні ноу-хау для програмування цих повідомлень для ефективної дистрибуції [87].

Таким чином, розглядаючи модель міжнародного потоку інформації у всіх її складових, включаючи внутрішньо - та зовнішньомедійні перемінні окремо, як на стадії виробництва, так і на стадії дистрибуції повідомлень, слід зазначити, що відсутність контролю над якимсь одним з акторів цього процесу, призводить до неспроможності ефективного контролю над інформаційним потоком в цілому.

Інформаційні потоки і їхні напрями в еру інформації стали вирішальними факторами світового порядку. В інформаційну еру інформація має таку ж

вагу, як політична, економічна та воєнна влада. Така супердержава, як США, розглядає глобалізацію у сфері інформації і комунікації як наріжний камінь своєї зовнішньої політики. "Для Сполучених Штатів головною метою зовнішньої політики інформаційної доби повинна бути перемога в битві світових інформаційних потоків, домінування над радіохвилями, як колись Велика Британія правила морями". Визнаючи, що в сучасному світі є різні інформаційні потоки, американський політик Д.Роткопф, котрий сповідує ідею світового культурного панування США, зазначає, що вони домінують в глобальному русі інформації та ідей: "Американська музика, американські фільми, американське телебачення, американський софтвер є настільки домінуючими, настільки продуманими і настільки очевидними, що тепер вони доступні, можна сказати, всюди на Землі. Вони впливають на смаки, життя та прагнення по суті кожної держави-нації. Американський політик доходить промовистих висновків і аналогій: "Так само, як Сполучені Штати є єдиною воєнною супердержавою, вони є єдиною в світі інформаційною супердержавою" [87-88].

На думку Д.Роткопфа, в економічних і політичних інтересах Сполучених Штатів забезпечити такий хід подій: якщо світ йде до однієї спільної мови, то це має бути англійська; якщо світ рухається до спільних комунікацій, спільної безпеки і стандартів якості, то вони повинні бути американськими; коли світ стає пов'язаним телебаченням, радіо, музикою, програмуванням, - все це буде американським; і якщо вже розів'ються спільні цінності, - це будуть цінності, з якими американцям буде зручно жити [88]. Як зазначав президент Б.Клінтон, "оскільки ми переходимо від індустріальної до інформаційної ери, від холодної війни до глобального села, в нас є надзвичайна можливість просувати наші цінності вдома і в усьому світі". Операціоналізація доктрини "національної безпеки" в США останніми роками пов'язана із зверненням до системи цінностей, що визначають цілі, засоби і методи взаємодії держав на міжнародній арені [90]. Це не може не непокоїти інші держави, адже зачіпає питання їхніх автентичних культур, національних цінностей і пріоритетів, що в кінцевому підсумку загрожує їх національній безпеці. Ще більше підстав для стурбованості різних країн світу викликає промова президента Дж.Буша, виголошена 1 травня 2001 р. у Національній академії оборони (Вашингтон), в якій він не тільки заявив, що США має намір більше не дотримуватися Договору про обмеження протиракетної оборони (1972 р.), оскільки в них є вже технологічні можливості для розгортання "глобальної системи безпеки". Зрозуміло, що саме стрімкий розвиток інформаційно-комунікаційних технологій є головною, вирішальною складовою для втілення в життя нової воєнно-політичної доктрини Сполучених Штатів.

Розмірковуючи над гуманітарними проблемами нової цивілізаційної ери, зазначимо, що інформаційна революція, яка стрімко відбувається, й під час якої експонентно зростає чисельність користувачів Інтернету, ставить безліч непростих проблем, які щільно пов'язані з питаннями національної

безпеки в тому її розширеному розумінні, про яке йшлося вище, а саме, про збереження демократичних прав людини в новому інформаційному середовищі як запорука дієвості системи національної безпеки.

Першочерговим серед них є "*право на комунікацію*", яке має вихідними передумовами як пасивне, так і активне право реципієнта інформувати і бути поінформованим [91]. Важливість запропонованого Ж.Д'Арсі фундаментального права людини на комунікацію полягає також і в тому, що воно включає як індивідуальні, так і соціальні права та обов'язки людини. Така постановка питання суттєво змінює акценти в підходах до проблем інформаційної безпеки, а також наголошує на багатоаспектній ролі у цьому держави.

Отже, відсутності загроз для такого права людини, як право на комунікацію, означає великою мірою здійснення її інформаційної безпеки. В інформаційну еру право на комунікацію, яке передбачує участь в комунікаційних процесах, набуло розширеного значення і включає в себе як мінімум такі взаємопов'язані ключові складові: доступ до знань, доступ до технології, доступ до мережі, доступ до змісту [92]. Знання в інформаційному суспільстві є головним продуктом праці, головним виробничим ресурсом. Доступ до знань стає запорукою інформаційної безпеки людини. В інформаційному суспільстві доступ до знань набуває яскраво вираженого соціального характеру. Як, мабуть, ніколи, оволодіння ними потребують немалих коштів: комп'ютер, програмне забезпечення, подолання "комп'ютерної неписемності", оволодіння навичками роботи на комп'ютері в обраній сфері діяльності, не кажучи вже про те, що за послуги Інтернету треба платити.

Це особливо гостро відчувають країни "третього світу", намагаючись привернути увагу до загроз глобального дисбалансу між "інформаційно багатими" та "інформаційно бідними" країнами. Президент Південної Африки Нельсон Мандела ще 1995 р. у промові на церемонії відкриття виставки "Телеком 95" в Женеві відзначив: "Подолання розриву між "інформаційно багатими" та "інформаційно бідними" країнами є вирішальним для подолання економічної та інших нерівностей між Північчю і Півднем, а також для поліпшення якості життя всього людства <...>. Але реальність сьогодення — це те, що технологічний розрив між розвиненими країнами та країнами, що розвиваються, швидко збільшується" [93].

Таким чином, інформаційна ера, попри всі її досягнення, містить в собі нові потенційні і реальні соціальні конфлікти, нові дисбаланси і нерівності, нові ризики, нові загрози комунікаційним правам людей тільки тому, що одні народилися в інформаційно-розвинених країнах світу і належать до "золотого мільярду", а інші — переважна більшість землян — ні [94].

До цього потрібно додати, що, опинившись в інформаційному середовищі, з притаманною йому властивістю і технічними можливостями накопичувати персональні дані про кожного громадянина суспільства, важливим питанням інформаційної безпеки стає захист персональних даних й доступ кож-

ної людини до них, що визначається правом людини на самовизначення і законодавчо закріплено як на рівні національних законодавств, так і на рівні міжнародних європейських організацій в низці документів: Конвенції Ради Європи "***Про захист прав фізичних осіб при автоматизованій обробці персональних даних***" (1981 р.) і в ряді Директив Європейського Союзу (95/46/ЕС; 97/46/ЕС).

У Сполучених Штатах Америки стурбовані користувачі Інтернету вже б'ють на сполах, вимагаючи від Конгресу негайного посилення правил щодо захисту персональних даних користувачів, особливо, тих, які мають Web-компанії [95]. Так, американська компанія *Double-Click Inc.* займається накопиченням і обробкою демографічних даних користувачів Інтернету, а також даних щодо їхньої поведінки в кіберпросторі. Її служба "*Intelligent Targetting service*" надсилає користувачам саме ту рекламу, яку вона вважає для них привабливою, а ступінь привабливості реклами обчислюється компанією, спираючись на аналіз таких даних щодо користувачів, як, скажімо, тематика сайтів, які вони відвідують. Наприклад, компанія відстежила тих, хто цікавиться автомобільними web-сайтами, невдовзі їм надсилається реклама різних марок машин. За це Double-Click отримує від рекламодавців премію.

За цілеспрямоване збирання інформації про своїх користувачів взявся і такий софтверний гігант, як корпорація Microsoft, і він це спланував із притаманними йому цілеспрямованістю та розмахом. Впливовий американський журнал "*BusinessWeek*" у редакторській статті висловлює занепокоєння щодо планів цієї корпорації централізовано накопичувати такі дані про користувачів, як їх персональний розклад робочого дня, професійні контакти, номери кредитних карток, навіть смаки у музиці та книгах. Для цього запропонована новітня аплікація для створення такої бази даних під кодовою назвою "*Hail-Storm*". Віддаючи належне позитивним моментам цієї пропозиції корпорації, у статті зазначаються і негативні моменти: така централізована база даних матиме "безпрецедентну кількість даних про користувачів...Компанія навряд чи встоїть перед спокусою продавати дані про споживачів маркетологам. Більш того, ця база даних стане спокусою і для хакерів – а історії відомо, що програми Microsoft, як і більшість інших, регулярно потерпають від того, що їх безпека порушується хакерами" [96]. Висновок, що його містить редакторська стаття, досить суворий. Відзначаючи, що ніхто не збирається відмовляти корпорацію від інновацій, в ній наполягається, що абсолютно недостатнім є добровільне прийняття гігантом софтверу зобов'язань щодо нерозповсюдження даних про клієнтів та користувачів Microsoft: "*Конче необхідними є суворі правила захисту privacy*" [96]. Коли вже захист персональних даних в контексті діяльності однієї з наймогутніших корпорацій світу стає темою редакторській статті американського економічного часопису першого ряду, це є індикатором великого занепокоєння ділових кіл корпоративної Америки щодо цієї проблеми.

З питанням захисту персональних даних та конфіденційної інформації в інформаційних супермагістралях та телекомунікаційному секторі нерозривно

пов'язане інше питання інформаційної безпеки в інформаційному суспільстві, — це мінімізація ризиків для кожного громадянина в тому аспекті, що всі форми спілкування користувача (а це може бути факс, телекс, телефонна розмова, електронна пошта, пошук і чат в Інтернеті і т. ін.) не перевіряються проти його волі, що комунікаційні акти, які він здійснює в мережі, є не ушкодженими. Тобто інформація і дані, якими він обмінюється з іншими приватними або бізнесовими адресатами, не використовуються іншими. Проте існують свідчення, що різні країни Заходу і Сходу, Півдня і Півночі, в тій чи іншій мірі, більш чи менш відкрито, або утаємничено, здійснюють такий контроль [97; 98].

Для успішного розвитку електронних бізнесу (e-business), торгівлі (e-commerce) та фінансів (e-finance) користувач онлайнових послуг має бути певним, що його фінансові і комерційні розрахунки, які здійснюються завдяки використанню Інтернету, отримуються в очікуваних місцях, що його комп'ютер, захищений надійними паролями, непідвладний вторгненню хакерів і т. ін. Ризики в таких сферах діяльності величезні. Провідні фірми несуть мільйонні збитки, індивідуальні користувачі потерпають від різних видів інформаційних шахрайств: зламаних паролів на їх комп'ютерах, що призводить до викрадення або ушкодження інформації, внесення різноманітних комп'ютерних вірусів тощо [99].

В інформаційно-розвинених країнах своєрідним показником нагальності вирішенні цих проблем є швидке збільшення фірм, що здійснюють розвідку в сфері електронного бізнесу для своїх клієнтів, як наприклад, міжнародна фірма "*Cyveillance*" із штаб-кватрирами у Вашингтоні та Лондоні, девізом якої є: "*Дбаючи про твій бізнес у Павутинні*" ("*Minding your business on the Web*").

В інформаційному суспільстві експонентно зростатиме відсоток працюючих на фірми і організації вдома на своїх персональних комп'ютерах. Завдяки загальній інформатизації збільшуватиметься також питома вага інтелектуального продукту, створеного на комп'ютерах. У зв'язку з цим поглиблюється така проблема інформаційної безпеки, як захист інтелектуальної власності. Людина в інформаційному суспільстві повинна бути захищена від крадіжки з комп'ютера або в мережі результатів її інтелектуальної праці, або використання її без дозволу власника. В аспекті держави це питання набуває ваги як таке, що зачіпає всі інші види національної безпеки (бо однаковою мірою стосується як економічної, так і політичної, як технологічної, так воєнної і екологічної безпеки). Всі ці види інформаційних загроз базуються великою мірою на питанні володіння мереж, доступу до процесування інформації в них, до встановлення міжнародних "правил гри", відповідних до революційних перетворень в інформаційно-комунікаційній сфері на початку третього тисячоліття.

Кінець XX — початок XXI ст.ст. приніс визнання того, що інформаційно-комунікаційний сектор має стратегічний характер. Об'єктивними ознаками цього стали його бурхливе економічне зростання. Інформаційно-комунікаційний сектор стає не тільки важливим у соціально-політичному і куль-

турному аспектах, він стає стрижневим сектором за масштабами економічного росту і зайнятості.

Відповідно зростають і соціальні ризики в інформаційно-комунікаційному секторі. Інформаційна економіка, на думку американських експертів, може призвести до подальшої ізоляції та занепаду профспілок у ньому. Зростає чисельність працівників у галузях ІКТ, які не охоплені жодною з існуючих профспілок. Так, відсоток працівників однієї з провідних телекомунікаційних компаній США AT&T, які є членами профспілки "Комунікаційні працівники Америки", після її злиття з низкою кабельних компаній впав до 25%. Керівники AT&T проводять жорстку лінію щодо запобігання юніонізації працівників тих відділень компанії, які не є ще членами профспілки, погрожуючи останній арбітражним судом. Як зазначає американський дослідник Р.Каттнер, "Різниця між старою економікою і новою економікою була щось на зразок міфу. В телекомунікаційній індустрії профспілками охоплені різні категорії працівників (від тих, хто встановлює обладнання до обслуговуючого персоналу), які виконують в цілому таку ж саму роботу, що і працівники галузі, які не є членами профспілок. Тільки перші більш захищені від ризиків втратити роботу та мають більший контроль щодо свого робочого середовища, а також у багатьох випадках вони мають кращу зарплатню і більше пільг. Натомість менеджери вважають, що профспілки стоять на заваді зростанню гнучкості, маневреності їхніх компаній" [100]. Таким чином, зростання соціальних ризиків працівників сфери високих технологій, породжуються глобалізаційними процесами, - концентрації і конгломерації, що відбуваються в інформаційному суспільстві. Це ще одна із загроз, яку не змогли спрогнозувати адепти безхмарного погляду на його становлення.

Кіберпростір активно почали "освоювати" політики і політичні партії. Тому питання інформаційної безпеки тісно пов'язані з питаннями політичної боротьби і маніпулятивними технологіями, особливо у передвиборні кампанії [101]. Це — тема окремого дослідження, але принагідно відзначимо, що таке нове інформаційне середовище, як кіберпростір, відкриває для маніпулювання свідомістю виборців нові, досі мало вивчені, а, отже, небезпечні технології, які поєднують у собі і технічні переваги, і нові можливості в охопленні аудиторії, і використання того моменту, що в Інтернеті важко застосувати законодавство про авторські права як на національному, так і на міжнародному рівні, тому що для цього середовища вони ще не вироблені. А це в свою чергу спонукає розвиток цілого спектру прийомів впливу на масову аудиторію. Йдеться не тільки про користувачів Інтернету, яких можна охарактеризувати як своєрідну еліту будь-якого суспільства, якщо не нині, то у найближчому майбутньому, але й про набагато ширшу аудиторію, яка включає в себе читачів періодики і глядачів телебачення, до яких політичні повідомлення з Інтернету надходять через вищеозначені традиційні ЗМК.

Розвиток Інтернету, його доступність не тільки для дорослих, але й для дітей і підлітків, містить безліч не тільки соціальних, але й соціально-психо-

логічних, моральних і, навіть, медичних проблем і ризиків для його користувачів різного віку і статі. Лікарі визнають, що існує "*комп'ютерний алкоголізм*", так само небезпечний, як побутовий алкоголізм, або вживання наркотиків. "*Комп'ютерний алкоголізм*", призводить до залежності від перебування у віртуальному просторі, не відпускає користувачів з віртуального життя в реальне. Ця соціально-психологічна хвороба небезпечна і для дітей, які, скажімо, не можуть відірватися від комп'ютерних ігор, і для дорослих, які нишпорять по "Павутинню". Особливо небезпечними є наслідки цієї залежності для дітей та підлітків. Проблема "*геймерів*" – так себе називають фанати комп'ютерних ігор — непокоїть вже не тільки їхніх батьків, але й педагогів, медиків, міліцію. Оскільки в багатьох випадках виникає стійка комп'ютерна залежність і непереборне бажання грати цілодобово, підлітки йдуть навіть на кримінальні злочини, аби дістати грошей на відвідання комп'ютерних салонів та ігротек [102]. Зафіксовані випадки скоєння серійних злочинів, у підґрунті яких, — переглядання порнографічних файлів [103]. Уже існують прецеденти, коли комп'ютерні ігри заборонені в країні на державному рівні. Так вчинив уряд Греції. Він прийняв закон № 3037, який набрав чинності з кінця липня 2002 р. Закон забороняє всі електронні ігри, навіть на мобільному телефоні. У випадку його порушення – великий штраф: від 5 тисяч до 75 тисяч євро або тюремне ув'язнення строком від одного до 12 місяців. Те саме очікує й іноземців, які привезуть у Грецію будь-які електронні ігри. Причиною такого суворого законодавства є бажання грецького уряду покласти кінець нелегальним азартним іграм [104]. Все це дає підстави говорити про те, що соціально-психологічні ризики, спричинені залежністю від різних типів електронних ігор, надто комп'ютерних, часто-густо розміщених і Інтернеті, загрожують і дітям, і підліткам, і дорослим чоловікам і жінкам. Від Інтернет-залежності, як сповіщає французький телевізійний канал ***TF 1***, розпочали лікування у США, де вже відкрито низку клінік відповідного профілю (Наприклад, такі клініки, де працюють висококваліфіковані лікарі-психіатри, існують у Гарварді, штат Массачусетс, у Бредфорді, штат Пенсильванія тощо). У Німеччині функціонує спеціальна організація, мета якої, - надання допомоги людям, котрі страждають на комп'ютерну залежність.

Жінки більш підпадають під вплив Інтернету: "Їх релігія Інтернет, їх молитви звернені до телефонів, факсів, модемів і провайдерів. Вони - жінки у тенетах Інтернету" [105]. Хоча й чоловіки часто шукають в ньому те, що неспроможні знайти в реальному житті. Наприклад, подругу життя. Соціологи і соціальні психологи піддають це сумнівам, підкреслюючи, що "в саму систему сватання "в режимі "on-line" закладені механізми, які роблять кожний віртуальний роман приреченим на невдачу при першій-ліпшій спробі перевести його в площину реальних відносин". В результаті цього виникають ризики психологічних травм, що може призвести до зміни особистості. Такі ризики і загрози мають багато причин, але основною, на думку американського профе-

сора Дж.Вальтера, спеціаліста з комунікації, соціальної психології та інформаційним технологіям, можна вважати "здатність "світового павутиння" створювати у користувачів ілюзію можливості виконання усіх можливих бажань" [106].

Ще більшою загрозою для користувачів Інтернету є, як їх називають соціологи і психологи, "*Інтернет-сайти з високим ступенем ризику*". До них, наприклад, відносять порносайти, особливо ті з них, в яких об'єктами насильства, збоченості і розбещеності дорослих виступають діти. Ступінь такої загрози для морального здоров'я людей стане вочевидь жахливою, якщо відзначити, що за даними дослідників десь половина сайтів в Інтернеті можна кваліфікувати як порносайти.

Окреслені і проаналізовані вище глобалізаційні загрози і ризики, які притаманні інформаційній ері, ставлять людство перед проблемою вироблення ефективних заходів щодо поліпшення інформаційної безпеки й тим самим запобігання руйнації соціальних, моральних і психологічних підвалин життєдіяльності людини.

Створення міжнародних регулятивних механізмів, вироблення нової глобальної комунікаційної політики — питання, яке неминуче буде внесено в порядок денний світового співтовариства XXI ст., що, сподіваємося великою мірою слугуватиме вирішенню питань інформаційної безпеки держави в умовах нового цивілізаційного періоду, в яке вступає людство.

Погляд другий. Зростання значимості інформації є важливою рисою світового суспільного прогресу. Україна вступає в нову еру інформаційного суспільства. На цьому шляху відкриваються широкі можливості розвитку країни, водночас — виникають нові загрози та виклики.

Існує цілий комплекс інформаційних загроз, серед яких — відсутність яскравої ідентифікації України у світовому інформаційному просторі та чіткої стратегії входження в Глобальне інформаційне суспільство.

Нині вперше в історії з'явилися технічні можливості суверенного розвитку для більшості людства. Всі країни світу так чи інакше здійснюють процес інформатизації. Об'єднати вільний розвиток з використанням новітніх досягнень науки і техніки — це не тільки магістральний напрям руху людства, але й найактуальніша проблема молодої української держави.

Неправильно обрана стратегія інформатизації або її недостатній динамізм і мобільність можуть призвести до суттєвих, подекуди драматичних змін в усіх сферах життєдіяльності країни.

Ті, хто вчасно не підготувався для інтеграції в світовий інформаційний простір ризикують залишитися на периферії історичного розвитку. У світі утворилася загроза нового поділу країн за ознакою рівня розвитку інформаційної сфери — на "*інформаційно багаті*" та "*інформаційно бідні*". В Україні рівень інформаційної безпеки наближається до критичної межі. Негативні тенденції розвитку її інформаційного простору пов'язані зі складнос-

тями реформ, кризовим станом економіки, неефективністю державної інформаційної політики. Шлях реформ Україна розпочала як одна з найрозвиненіших індустріальних держав, а нині за рівнем розвитку вона знаходиться у другій сотні країн світу.

У більшості країн світу розуміють, що без надзвичайних зусиль відставання в галузі інформаційних та комунікаційних технологій може призвести до руйнівних наслідків. Лідери країн "третього світу" з тривогою констатують своє відставання від розвинутих країн світу, що здійснюють інформатизацію. Це у повній мірі стосується і України. В будь-якій країні незалежно від рівня розвитку розуміють необхідність та невідворотність перетворення в життя ідей інформатизації суспільства. Багато країн мають національні програми інформатизації з урахуванням місцевих особливостей та умов. При створенні та реалізації таких програм слід спиратися на досвід передових країн світу, враховуючи їх успіхи та недоліки, відобразити в них існуючі та перспективні тенденції інформатизації.

Метою процесу інформатизації є створення інформаційного суспільства, в якому особливу роль відіграють не матеріальні об'єкти, а символи, ідеї, образи, інтелект, знання.

Ці зміни вже відбуваються в світі в історично короткий строк, за життя одного покоління. Впродовж 40 років повністю сформувалися передумови для переходу до інформаційного суспільства. Глобалізація всіх сфер людського буття, прискорений технологічний процес "*згортають*" час, відведений державам для формування політики, що дозволить безконфліктно підвестися на нову ступінь розвитку – в інформаційне суспільство.

Інформаційне суспільство виникає в рамках існуючих індустріального та постіндустріального суспільств з різним рівнем інтенсивності, але за загальними закономірностями. Їх аналіз дозволяє вченим виробити рекомендації, що прискорюють процес його формування в інтересах особистості та суспільства.

У 60-ті роки, коли в західній літературі почали вивчати теоретичні засади інформаційного суспільства, зазначалося, що основою його формування є розвиток обчислювальної та інформаційної техніки [107]. Визначалися й інші ознаки, серед яких : інформація набуває глобального характеру; державні кордони нездатні зупинити вільний рух інформаційних потоків; обмеження вільного обігу інформації шкодить країні, яка створює їй перепони; зростають можливості збору, обробки, зберігання та передачі інформації; збільшується вплив інформації на розвиток всіх сфер людського життя; поглиблюється процес децентралізації суспільства; відбувається перехід до нових форм зайнятості, передусім в інформаційній індустрії.

На початку 90-х років до теми інформаційного суспільства залучилися також вітчизняні вчені [86]. У політологічних, соціологічних словниках, виданих в Україні, розкриваються поняття "***інформаційне суспільство***", "***інформатизація***". Вчені вбачають сутність інформаційного суспільства в

забезпеченні комп'ютерного доступу громадян до надійних джерел інформації та перехід від рутинної до творчої праці на базі новітніх технологій. Вказується на наявність єдиного інформаційного простору для держав-учасниць, масове використання інформаційних технологій, створення і розвиток ринку інформаційних послуг і продуктів.

Учені виділять три базові характеристики інформаційного суспільства.

- По-перше, інформація використовується як економічний ресурс.
- По-друге, інформація стає предметом масового споживання у населення.
- По-третє, швидкими темпами формується та зростає інформаційний сектор економіки.

Новітні інформаційні технології значно збільшили можливості людини обробляти інформацію. Водночас відзначається затримка в розвитку законодавчого забезпечення прав людини на інформацію, недоторканість особистого життя, збереження персональних даних. Відсутність обмежень на концентрацію засобів масової інформації і комунікації може реально призвести та призводить до маніпуляції масовою свідомістю, контролю за особистістю з боку державних або кримінальних структур. Отже, в інформаційному просторі існують чинники негативного впливу на суспільну свідомість.

Автори книги "*Глобалізація та безпека розвитку*" зазначають, що по мірі зростання масштабів комп'ютеризації головним стає не технічний елемент, а соціальний і гуманітарний [108]. На їх думку, сам підхід до феномену інформації подекуди спрощується, а її глибинна сутність та фундаментальна соціальна функція залишається неусвідомленими. Нині ще відсутня методологічна основа інформатизації. В глобальному вимірі по планеті крокує практична інформатика. Йдеться про "перехідні містки" в інформаційне суспільство. Це – телеробота, дистанційна освіта, телепатичні послуги для бізнесу(електронна пошта, передача файлів, відео конференції та інше), комп'ютерне управління транспортними послугами, комп'ютерний контроль за повітряним сполученням, комп'ютерні мережі в галузі охорони здоров'я, електронна торгівля та інше.

Комп'ютеризація сьогодні не дає належного соціально-економічного ефекту. Попри позитивні можливості для сфери зайнятості, організації праці аналітики акцентують увагу на проблемі "*виключення*" з активного соціального життя певних соціальних груп, що становить загрозу стабільному розвитку. Серед них люди з низьким рівнем доходів, пенсіонери, безробітні, батьки-одинаки, жінки. Вони не можуть дозволити собі придбати нову цифрову інтерактивну техніку, працювати в комп'ютерних мережах, мати мультимедійні продукти.

Є ще одна причина "*соціального виключення*" з інформаційного середовища. Нові медіа вимагають від людей нових якостей – високого рівня абстрактного мислення, швидкої реакції, готовності до постійного підвищення освітнього рівня. Традиційна культура засобів комунікації в аграрному та індустріальному суспільствах була заснована на прямих людських контактах,

літературній освіченості та "паперовій інформатиці", на базі старих методів збереження, пошуку та поширення інформації (бібліотек, ручних методів пошуку та аналізу, пошти, телеграфу). Сучасна віртуальна комунікація змінює як поведінку користувачів, так і засоби репрезентації інформації (бази даних, інформаційно-пошукові системи, комп'ютерні мережі, супутниковий зв'язок, волоконно-оптичні кабелі, системи обробки текстів, локальні обчислювальні мережі, автоматизовані робочі місця).

Для подолання нерівності потрібна продумана політика, що допоможе запобігти виникненню дворівневого інформаційного суспільства. Інформатизація повинна вміщувати в собі не тільки комп'ютеризацію, але й моделювання інформаційних процесів, перебудову організаційних структур, юридичних норм, а також підготовку і перепідготовку кадрів. Це – свідома перебудова соціального інформаційного середовища, створення знань, ефективних методів інтелектуальної діяльності. Вона передбачає радикальний крок людства у вирішенні надзвичайно важливої проблеми ефективного використання людського потенціалу та новітніх інформаційних технологій.

Зміст інформатизації – забезпечення соціальних, економічних, правових , культурних і технологічних умов зберігання та активізації нових ідей та створення умов для людської творчості, доступності інформації кожній людині для її використання.

Світовий досвід свідчить про різноманітні шляхи вирішення проблем інформатизації. США вже 40 років створює інформаційну індустрію. Країни Західної Європи понад 30 років будують сучасну інформаційну структуру. Японія за рахунок державної науково-технічної політики ліцензування вирішила цю проблему менше, ніж за 20 років. Країни Південно-Східної Азії (Південна Корея, Бірма, Таїланд, Сінгапур), широко використали досвід розвинутих країн світу та в умовах регулюючої ролі держави 10 років успішно реалізовують національні програми інформатизації.

Деякі держави (США, Японія, Північна Корея) мають на меті втілення в життя ідеї створення інформаційного суспільства самостійно. Розвинуті європейські країни в своїх національних програмах передбачають об'єднати ресурси та спільно координувати програми інформатизації. Водночас з національними програмами існують програми та концепції, прийняті міжнародними організаціями та спільнотам [109].

Досвід Європейського Союзу привертає особливу увагу в контексті глобальної орієнтації національної стратегії України на співробітництво з ЄС та подальшу інтеграцію в Європу. Проте за даними експертів Ради Міністрів ЄС в Європі повільно використовуються новітні інформаційні технології порівняно зі США та Японією. Персональні комп'ютери в Європі мають лише 20% сімей, що в два рази менше, ніж в США. В США в чотири рази більше, ніж в Європі сімей отримують послуги в режимі реального часу. Європейці менше користуються послугами електронної пошти.

США є визнаним лідером сучасного етапу інформаційної революції. Тут активно експлуатуються мультимедійні технології, користуються інформаційними послугами і відповідно створюють нові корпорації – мультимедійні гіганти. Починаючи з 1990 р. в структурі американського бізнесу відбулися зрушення на користь компаній, які спеціалізуються в інформаційній галузі. Сьогодні вони посідають домінуюче місце в американській економіці і вважаються символом могутності Америки.

У відповідності до стратегії розвитку "***Європейського інформаційного суспільства***", прийнятої наприкінці 1999 р., Європейський Союз робить енергійні зусилля для подолання відстані від США в інформаційній сфері. Серед пріоритетних напрямів досліджень, що активно фінансуються Комісіями ЄС, важливе місце відводиться розвитку індустрії інформації, передусім електронних засобів для її передачі, нагромадження і обробки, а також програмного забезпечення. Значення розвитку інформатики стимулюється також тим, що 55% промислової продукції та 62% робочих місць в країнах ЄС залежать від новітніх інформаційних технологій.

Надаючи пріоритетну роль розвитку інформаційної сфери економіки, стратегія Євросоюзу відзначається своєю відвертою соціальною спрямованістю. На відміну від США, де перевага надається технологічним аспектам інформаційної супермережі, в Європі робиться акцент на соціальному вимірі. Так, саме соціальні складові розвитку стоять на першому плані в праці, підготовленій Європейською Комісією "***Робота та життя в інформаційному суспільстві***". В цій "Зеленій книзі" підкреслюється, що сучасні технологічні трансформації створюють складні соціальні проблеми, що пов'язані зі сферою зайнятості: чи зможуть люди адаптуватися до змін в умовах, коли інформаційні та телекомунікаційні технології руйнують робочі місця? Інша проблема – інформаційний розрив між індустріальними та менше розвинутими країнами, молодим та старим поколінням. В "Зеленій книзі" зазначається, що втрата соціальної орієнтації технологічного розвитку загрожує також посиленням контролю над особистістю, маніпуляцією масовою та індивідуальної свідомістю з боку тих, хто володіє знаннями , має доступ до інформації.

З позиції визначення знань своєю головною цінністю та маючи на меті інтеграцію всіх прошарків населення в інформаційне суспільство, Європейська Комісія розпочала широке обговорення ідей інформаційного суспільства. Форуми ЄС з інформаційного суспільства проводяться з весни 1995 р. по два рази на рік. В них беруть участь представники влади, промисловості та культури [110].

Діяльність форумів відбувається, головним чином, по підгрупам, де обговорюються проблеми економіки та зайнятості, людських цінностей та демократії. Зокрема, робота підгрупи "*майбутнє культури та ЗМІ*" сконцентрована навколо питань нейтралізації негативного впливу ЗМІ на суспільну свідомість і психіку громадян. З метою збереження європейської ідентичності вони пропонують: вдосконалити відповідне законодавство; зберегти систему

державного мовлення в практиці інформаційного суспільства; ввести обмеження на свободу поширення негативної інформацій, зокрема насильства та порнографії на рівні національних рішень, враховуючи загально гуманістичні та спільно європейські ідеали; підвищити роль медіа-освіти в суспільстві.

Європейська Комісія підкреслює значення дискусії про інформаційне суспільство для подальшого розвитку демократії, освіти, суспільної злагоди. Дискусія спрямована і на залучення до участі в ній представників бізнесу. Саме на їх фінансову підтримку розраховано основні програми створення нових інформаційних структур.

З 1 січня 1998 р. телекомунікаційний простір Європейського Союзу відкрито для вільної конкуренції. Перехід до політики лібералізації здійснюється з метою створення майже мільйона нових робочих місць упродовж найближчого десятиріччя та підвищення конкурентоспроможності європейського бізнесу. Через лібералізацію забезпечується залучення приватного сектора економіки до фінансування конкретних проектів побудови інформаційного суспільства. Так, чисельні оператори телефонних та комп'ютерних мереж мають право пропонувати нові інформаційні та комунікаційні послуги (передача даних, кабельне телебачення) та створювати конкуренцію колишнім монополістам — національним Телекомам. Ще до формального початку лібералізації в Європі вже розпочався цей процес. На європейському та світовому ринках лідерами стали два транснаціональних об'єднання — "Глобал уан", до якого увійшли "Франс телеком", "Дойче телеком" І корпорація "СПРИНТ"(США) та "Юнисос", в якому здійснюють співпрацю американська "Ей-ті енд ті" та телекомунікаційні компанії Швеції, Швейцарії, Нідерландів, Італії.

Оскільки реалізація великих інформаційних та телекомунікаційних проектів — досить ризикований бізнес, держава не має права вкладати в цю сферу гроші . Тому всі ризики покладаються на акціонерів, а держава тільки створює умови для діяльності приватного бізнесу. Бажання бути лідером на ринку, перемагати конкурентів — природне прагнення бізнесменів. Якщо держава не контролює цей процес, то відбувається монополізація ринку. Підтримка конкуренції та боротьба з монополізмом окремих виробників є наріжним каменем державного регулювання. В європейських країнах в галузі телекомунікацій об'єднання різних компаній на національному та міждержавному рівнях відбувається обов'язково з дозволу відповідних органів. Вони визначають чи не призведе це об'єднання до монополії, яка не тільки зведе нанівець конкуренцію, але й знизить якість послуг, приведе до зростання цін.

Європейська політика лібералізації телекомунікацій сьогодні є складовою частиною глобальної стратегії, ухваленої Всесвітньою торговою організацією. В лютому 1997 р. під егідою СОТ 69 країн світу, що становлять 90% ринку телекомунікацій, підписали договір про його лібералізацію. Таким чином, європейська позиція наближується до американської. Але в довгостроковій перспективі підхід Європейського Союзу засновується на суспільних

пріоритетах — демократичних цінностях та правах людини, освіті, підвищенні зайнятості.

Використання новітніх інформаційних технологій в Європі зорієнтовано на досягнення соціальних цілей. Вивільнюючи шлях приватним ініціативам, Європейський Союз залишає за собою право визначати суспільні пріоритети та основні напрямки спільної політики переходу до інформаційного суспільства. Так, у 1995 р. "*Велика сімка*" провела в Брюсселі нараду присвячену проблемам інформаційного суспільства. На ній було висунуто ідею "*глобальної інформаційної інфраструктури*", в створенні якої країни "сімки" покликані відігравати провідну роль [109].

Високого ступеня інтегрованості у світовий інформаційний простір можуть досягти лише країни з високим науково-технічним потенціалом і культурно-освітнім рівнем населення. Про це свідчить факт, що на розвинуті країни світу припадає майже 90% всіх наукових кадрів і приблизно 94% сумарних витрат на науку, що і забезпечило стрімку інформатизацію цього регіону. Перспективи інтеграції до глобальної інформаційної інфраструктури у значній мірі залежать від ставлення суспільства до специфічного інформаційного ресурсу. Саме така залежність зумовлює дисбаланс, нерівномірність соціально-економічного розвитку країн світу та створює в геополітичному плані напругу та протистояння.

Усвідомлення вирішальної ролі інформаційного ресурсу державами, що прагнуть інтегруватися у світове інформаційне співтовариство у найближчому майбутньому, стає важливою передумовою здійснення інтеграційних процесів. Становлення інформаційного суспільства супроводжується потужним соціальним замовленням на ринку інформаційних послуг. Створюються всі умови для придбання засобів інформатизації та користування послугами по доступним цінам. Кінцевою метою такої політики повинен стати такий же попит на засоби інформатизації, який існує на телефонний зв'язок. Нове інформаційне середовище стає природним середовищем для людей.

Державна підтримка процесу інформатизації має бути забезпечена відповідною національною політикою. Держава повинна чітко визначити своє ставлення до проблеми і конкретизувати дії і наміри уряду по досягненню поставлених цілей. Аналіз закордонної практики регулювання інформаційної сфери суспільства дозволяє виділити низку основних напрямків діяльності державних органів. А саме:

- заохочення до конкуренції: боротьба з монополізмом, контроль за концентрацією власності в одних руках;
- юридичне та технологічне забезпечення права та технічних можливостей на доступ до інформації й інформаційних ресурсів для всього населення;
- реалізація концепції універсального доступу, що передбачає гарантію держави на інформаційні та телекомунікаційні послуги своїм громадянам (телефон, електронна пошта, мультимедійна освіта);

- дотримання свободи слова незалежно від технологічного середовища розповсюдження інформації;
- захист інтересів національних меншин, молодого покоління в інформаційній сфері, особливо в сфері моральності;
- зміцнення національної культури, мови, протистояння експансії інших держав;
- переорієнтація системи освіти з урахуванням вимог інформаційного суспільства, поширення дистанційної освіти;
- широке використання телемедицини для надання послуг населенню віддалених регіонів;
- забезпечення інформаційної безпеки особи і суспільства, зокрема боротьба з комп'ютерною та високотехнологічною злочинністю;
- охорона інтелектуальної власності;
- цілеспрямоване використання новітніх інформаційних технологій для формування відкритої, демократичної держави, поширення діалогу з громадянами [111].

В Україні стан і темпи впровадження новітніх інформаційних технологій не відповідають світовим тенденціям розвитку, національна інформаційна інфраструктура знаходиться на початковому рівні. Наявні лише розрізнені мережі, що не складають загальну систему. Створення технологічної бази інформаційного суспільства в Україні затяглося: рівень інформатизації українського суспільства порівняно з розвинутими країнами Заходу становить лише 2-2,5%. Паростки інформаційного суспільства виявляються у вигляді базової інформаційної та телекомунікаційної інфраструктури. Проте у відриві від перетворень у соціальній та економічній галузі вони так і залишаться паростками.

З іншого боку, відбувається процес уніфікації масової свідомості, оскільки в Україні через канали телебачення "споживають" практично ті самі новини та серіали, йде масована пропаганда способу життя західної, техногенної цивілізації. Особливо сильно цей механізм діє на молодь. Відповідно через років десять виросте покоління людей, що повністю поділятиме стереотипи західного суспільства. В цьому плані йдеться не про технічний бік інформатизації, а про соціальні, правові аспекти інформаційної безпеки країни. В Україні існує гостра необхідність у введенні національних пріоритетів в інформаційній сфері, які потрібно контролювати.

Вирішити ці питання в країні може лише держава. На державному рівні необхідно захистити інформаційний ринок України, надати державну підтримку підприємствам, що впроваджують новітні технології в галузі інформаційного обслуговування, діяльність яких направлена на розвиток інформаційних мереж на рівні стандартів високорозвинених країн світу [112].

Після здобуття незалежності Україна прагне відродитися як могутня європейська держава. Маючи багатий людський потенціал, Україна стоїть пе-

ред завданням розробки інноваційної політики та стратегії, що сприятимуть ефективному зростанню цього історичного потенціалу. Держава координує всі процеси, які перетворюють основи суспільства. Здебільш це стосується зовнішнього напряму її діяльності. Тут український уряд працює дуже активно. Сьогодні Україна представлена в таких впливових міжнародних організаціях, як Міжнародна Спілка електрозв'язку, Європейська конференція Адміністрацій зв'язку, Європейський інститут телекомунікаційних стандартів та Регіональне співтовариство в галузі зв'язку. Успіхом є також підписання Паризького меморандуму взаєморозуміння стосовно розвитку інформаційного суспільства. За ним високих пріоритет у взаємовідносинах між Європейською Комісією і Україною належить побудові в Україні інформаційного суспільства.

Інформаційні та комунікаційні технології визнаються на державному рівні відповідно до Національної Програми Інформатизації як головні чинники і рушії майбутнього процвітання України.

1.5. Спеціальні інформаційні операції: теорія і практика

Спеціальні інформаційні операції здійснювалися з найдавніших часів, принаймні з перших часів появи писемності. Ще давніша історія спеціальних психологічних операцій: початок їхнього використання можна віднести до появи *homo sapiens*.

Спеціальні інформаційні та спеціальні психологічні операції належать до різних типів спецоперацій. Незважаючи на це, після закінчення *«холодної війни»* дедалі частіше відбувається змішування цих понять. Термінологічна плутанина пов'язана зі спробами позбутися історичного синдрому, викликаного понад 40-річним протистояння двох наддержав. За свідченнями сучасних дослідників, *«холодна війна»* була насамперед війною психологічною".

Як зазначалося, основна різниця між спеціальними інформаційними та спеціальними психологічними операціями полягає у їхньому підґрунті. Спеціальні психологічні операції використовують особливості масової та індивідуальної психології з акцентом на підсвідоме та діють за умов сталої структури суспільної комунікації. Інформаційні операції адресуються насамперед до суспільної свідомості, працюють з характерними рисами суспільної комунікації, мають на меті модифікацію її структури. Попри відмінності межу між цими типами операцій іноді провести дуже важко.

Про успішне використання спеціальних психологічних операцій свідчить ще Старий Завіт (алегоричне сприйняття епізоду з Єрихонськими трубами). Багато їхніх прикладів можна знайти у давній та середньовічній історії. Так, наказ перського царя Ксеркса висікти море, що знищило переправу, - це і відчутна магічна складова (вплив на богів моря) і психологічна складова (вплив на військо – злочин проти великого царя не може бути не-

покараний). У даному разі можна говорити про зв'язок психологічних та інформаційних операцій з магією, тобто вони беруть свій початок саме у магічних ритуалах давнини.

«Записки про Галльську війну», «Записки про громадянську війну», «Записки про африканську війну» Гая Юлія Цезаря містять цікавий матеріал стосовно психологічних операцій. Великий полководець давнини приділяв надзвичайну увагу підтримці бойового духу своїх військ та впливу на військо противника. Не менш відомі й піраміди з черепів ворогів, що складав на місцях битв Великий Кульгавий (Тамерлан).

Класичними спеціальними психологічними операціями можна вважати і будь-які публічні страти (надмірне покарання за символічне посягання на тіло суверена). Вбивство Лжедмитра Першого, коли його попелом було заряджено гармату, з якої вистрілили у бік Польщі — найяскравіший приклад психологічної операції середньовіччя, що має відчутний магічний відтінок.

В Україні спеціальні психологічні та інформаційні операції здійснювалися з найдавніших часів, бо її теперішня територія завжди була ареною протиборства наймогутніших імперій (*Візантійської, Хазарської, Османської, Священної Римської, Австрійської, Російської тощо*). Певною мірою однією з перших інформаційних операцій, що була здійснена візантійцями та визначила майбутнє переважної більшості слов'янського світу на тисячоріччя вперед, було створення кирилиці та переклад народною мовою священних книг. Надзвичайно вдало у художній формі проілюстрував цей процес М. Павич її романі «Хазарський словник» у статті "Кирило» («...и пока славяне в 860 году осаждали Царьград, Константин в том же Олимпе в Малой Азии, в тишине монашеской кельи мастерил для них ловушку, вычеркивая первые письмена славянской азбуки...»).

Резонанс від публікації документа, образливого для честі Французького імператора Наполеона III, змусив Францію розпочати воєнні дії у вигідний для Пруссії час. А фабрикація французами «Заповіту Петра Великого» наприкінці XVIII ст., створення керівником закордонної агентури охранки М. Ратаєвим та публіцистом С. Нілусом «Протоколів сіонських мудреців» наприкінці XIX ст. — були вже інформаційними операціями. Вони формували певні структури комунікації.

Методи спеціальних психологічних операцій широко використовувалися під час першої світової війни. Як приклад може слугувати телеграма Цимермана (перехоплена телеграма німецькому послу в Мексиці, в якій пропонувалося підбурювати цю країну до нападу па США), публікація якої остаточно вирішила питання виступу США на боці Антанти. Такою самою операцією, щоправда зі значною інформаційною складовою, можна вважати дії Німеччини та Австро-Угорщини стосовно підтримки більшовиків на чолі з Володимиром Леніним.

Як приклад спеціальної психологічної операції у межах спеціальної інформаційної можна розглядати діяльність німецької розвідки задля форму-

вання пацифістських та «пораженческих» настроїв у Росії, зокрема, через підтримку більшовиків.

У липні 1916 р. у Стокгольмі відбулися переговори між агентом МЗС Німеччини Боккельманом та колишнім приватним секретарем графа С. Вітте Колишком й князем Бебетовим про створення видавництва у Москві для про німецької пропаганди. 12 серпня 1916 р. німецький промисловець Стіннес надав Боккельману позику для фінансування цього видавництва. Існують припущення, що частина цих коштів потрапила через Колишка до газети М. Горького *«Новая жизнь»*.

Міжвоєнний період (1918—1939 рр.) надає багато матеріалу для вивчення проблематики спеціальних інформаційних операцій. У ті часи методи спеціальних інформаційних операцій активно використовувалися у внутрішньополітичній боротьбі, зокрема, в недемократичних країнах. Досить навести відомі приклади Московських процесів 1936—1938 років і «війни, що виграв Гітлер» (нацистської пропаганди). За даними опитувань, що проводили серед військовополонених підрозділи психологічної війни ЗС США у листопаді 1944 року, понад 52 % німецьких солдат довіряли Гітлеру та вважали, що він приведе Німеччину до перемоги.

Друга світова війна не тільки довела дієвість спеціальних психологічних та інформаційних операцій, а й визначила межі ефективності їхнього застосування. Набагато пізніше один американський офіцер писав, що найкращим типом психологічних операцій проти приморської країни є поява авіаносного з'єднання на рейді головного порту цієї країни. А корифей нацистської пропаганди Й. Геббельс зауважував, що пропаганда ефективна тільки тоді, коли за спиною пропагандиста стоїть вояк з гостро заточеним мечем.

Відповідні операції здійснювалися і з боку союзників, зокрема, під час війни в Лондоні активно діяв Міжсоюзницький комітет з психологічної війни. У ході «Битви за Англію» (липень 1940 — березень 1941 рр.) німцями було здійснено одну з найжорстокіших і варварських спеціальних психологічних операцій в історії людства: тотальне бомбардування англійського міста Ковентрі. Місто не мало жодного стратегічного значення, на його території не було розміщено важливих підприємств воєнно-промислового комплексу. Не важко зрозуміти, що тотальні бомбардування Німеччини, які, починаючи з 1943 р., здійснювала союзницька авіація, значною мірою мали справити саме психологічний ефект на населення Рейху.

Як пише видатний французький історик, фундатор школи «Анналів» М. Блок: «Розповідали, що Гітлер, перед тим як виробляти план битви, користувався порадами експертів у галузі психології. Я не знаю, чи дійсно це було так. Але це дуже схоже на правду. Одне можу сказати точно: блискучі повітряні атаки, здійснені німцями, демонстрували їхню спроможність впливати па нервові центри людини й можливість її пригнічення. Той, хто хоч раз у житті чув пронизливий свист літаків, що готуються кинути на землю бомбу, навряд чи коли-небудь забуде його. Цей довгий різкий звук не тільки навіював думки

про смерть і знищені міста. Насмілюсь сказати, що від його акустичних особливостей тужавіє душа і виникає загальна паніка. Мені здається, що німці навмисно посилювали звук за допомогою спеціальних пристроїв. Річ у тім, що повітряні удари були задумані німцями не тільки як засіб руйнування міст і знищення людей. Оскільки радіус дії бомб доволі малий, то в результаті повітряних атак страждає не дуже велика кількість населення. А от коли доторкується до нервової системи, то паніка охоплює величезну кількість людей і зводить нанівець усі оборонні можливості наших загонів. Цього і домагалося вороже командування, щодня здійснюючи повітряні нальоти на територію Франції. Можна впевнено стверджувати, що в цьому вони були успішні, та результати перебільшили всі очікування» [113].

У наш час, за наявними матеріалами відкритих джерел та інформаційними документами, методи спеціальних інформаційних операцій активно застосовуються практично усіма спецслужбами світу. Розглянемо досвід найпотужніших з них.

США. Управління стратегічних служб (УСС), попередник ЦРУ, створене у 1943 р. і очолюване У. Доннованом, мало у своєму штаті відділ психологічної війни, головним завданням якого було здійснення інформаційних операцій. Діяльність цього підрозділу спрямовувалася насамперед проти гітлерівської Німеччини та виявилася ефективною на останньому етапі другої світової війни [114].

Основні напрями діяльності УСС були такі:

- *Радіопропаганда.* Діяли кілька підпільних радіостанцій, зокрема таких, що виходили в ефір від імені певних груп опору в Німеччині.
- *Безпосередня пропаганда.* За допомогою осередків Руху опору, що були створені в європейських країнах за безпосередньої участі співробітників УСС та розвідки Великобританії, союзники намагалися донести свої пропагандистські матеріали до мешканців окупованих територій.

Найактивнішими дії відділу психологічної війни були на Тихоокеанському театрі воєнних дій в останній період другої світової війни. Окремі операції, наприклад, проти японських військ на о. Окінава, можуть вважатися найдосконалішими їхніми зразками. У певному сенсі навіть використання ядерної зброї проти Японії у серпні 1945 р. (м. Хіросіма та м. Нагасакі) можна вважати інформаційними операціями.

«Холодна війна» та пов'язане з нею жорстке ідеологічне протистояння створили умови для широкого застосування методів спеціальних інформаційних операцій. В середині 40-х років XX ст. дії, спрямовані на зміну масової чи індивідуальної свідомості, отримали в англомовній літературі назву спеціальних психологічних операцій (PSYOP, ПсО).

Слід зазначити, що США створили найпотужнішу у світі систему зовнішньополітичної пропаганди. До речі, саме американці вперше в історії розділили напрями впливу на закордоння та на власну країну. До найваж-

ливіших організацій зовнішньополітичної пропаганди США необхідно віднести:

• *USIS*, раніше USIA (протягом 2000 р. здійснювалася чергова реорганізація цієї установи з метою підвищення ефективності інформаційно-пропагандистського забезпечення зовнішньої політики США за умов кардинальних змін у технологічній основі інформаційної діяльності);

• «*Корпус Миру*»;

• радіостанцію «*Голос Америки*»;

• радіостанції «*Свобода / Вільна Європа*»;

• радіостанцію «*Вільна Азія*»;

• радіостанцію «*Радіо Марті*» тощо.

Наймасштабніший в історії комплекс ІО та ПсО був здійснений за часів «холодної війни». Як писав 1946 р. один з архітекторів американської зовнішньої політики, директор ЦРУ (1953—1961 рр.) А. Ф. Даллес, «людський мозок, свідомість людей здатні змінюватися. Посіявши хаос, ми непомітно підмінимо їхні цінності на облудні та змусимо їх вірити у фальшиві цінності. Як? Ми знайдемо своїх однодумців, союзників у самій Росії, Україні, Білорусії, Прибалтиці, Закавказзі, Середній Азії і далі — скрізь» [115].

Далі він визначає сценарій перебігу подій. «Епізод за епізодом розігруватиметься грандіозна за своїми масштабами трагедія загибелі найнепокірніших народів, остаточного, незворотного згасання їхньої самосвідомості. З літератури та мистецтва, наприклад, ми поступово вичавимо їхню соціальну сутність, відучимо митців, знеохотимо їх зображати <...> досліджувати ті процеси, що відбуваються в глибинах народних мас. Література та кіно — усе відображатиме та прославлятиме найбрутальніші людські почуття. Ми всіляко підтримуватимемо і возвеличуватимемо так званих митців, які насаджуватимуть і втокмачуватимуть людську свідомість культ сексу, насильства, садизму, зрадництва — одним словом, усілякої аморальності.

У керівництві держави ми насадимо хаос та ворожнечу.

Ми непомітно, але активно і постійно, потуратимемо самодурству чиновників, хабарництву й безпринципності. Бюрократизм і, тяганина видаватимуться за благодійність. Чесність і порядність висміюватимуться, стануть нікому непотрібними, перетворяться на пережиток минулого. Нахабство, брехня, пияцтво і наркоманія, тваринний жах один перед одним, безчесність, зрадництво, націоналізм і ворожнеча народів, передусім ворожнеча та ненависть до російського, українського, сербського, білоруського та інших слов'янських народів — усе це ми спритно й непомітно культивуватимемо, все розквітне махровим цвітом.

І лише дехто, дуже нечисленні люди, здогадуватимуться і розумітимуть, що відбувається. Але таких людей ми загонимо у глухий кут, перетворимо на посміховисько, знайдемо засіб; оббрехати їх та оголосити відщепенцями суспільства.

Вириватимемо духовне коріння, опошлюватимемо і знищуватимемо основи народної духовності.

Ми розхитуватимемо таким чином покоління за поколінням. Братимемося за людей з дитячих, юнацьких років, головну ставку робитимемо завжди на молодь, розкладатимемо, розбещуватимемо, розтліватимемо її. Ми зробимо з них паскудників.

Ось так ми й зробимо» [115].

Ця розлога цитата найяскравіше характеризує основний напрям, за яким здійснювалися спеціальні інформаційні операції протягом *«холодної війни»*.

Доволі ефективними виявилися дії американських спецслужб під час виборчих кампаній кінця 1940- х років у Західній Європі, коли вдалося запобігти майже неминучій перемозі комуністів у Італії та значно послабити їхні позиції у Франції.

Першою масштабною СІО, що мала цю назву, була здійснена ЗС США. Операція була спрямована па підтримку військ ООН у Корейській війні (1950—1953 рр.). Перед її початком у США було ухвалено військовий Статут FM 33-5 *«Ведення операцій психологічної війни»*. Переглянути підходи у психологічному протиборстві керівництво ЗС США змусила велика кількість дезертирів (близько 40 тис. щорічно протягом усієї війни). Усвідомлення американськими фахівцями ідеологічного характеру сучасних воєн підвищило їхній інтерес до проблем психологічного протиборства, а також і до спеціальних інформаційних операцій.

Вперше після другої світової війни до діючої армії було передано тактичний інформаційний загін, що базувався у Форт — Райлі (США). З 1952 року у Форт - Брезі (Північна Каролiна) на його основі було створено Центр психологічних операцій. У 1951 р. у Міністерстві армії було створено Управління психологічних операцій, яке у 1955 році перетворили на Управління спеціальних методів війни. Розпочалася масова підготовка спеціальних кадрів [116].

Фахівці цього Управління брали активну участь у «холодній війні». Зокрема, за їхніми порадами було здійснено операцію з постачання продуктовими наборами громадян НДР (літо - осінь 1953 р.). За оцінками експертів, ця операція значно ускладнила діяльність прорадянської влади у Східній Німеччині щодо стабілізації ситуації після дня «Х» (17 червня 1953 р.) [117].

Другим конфліктом, де широко застосовувалися ПсО, стала війна у В'єтнамі. Тут уперше випробовувалася батальйонна організація військ ПсО. Ефективність дій нової системи довів перехід понад 250 тис. північних в'єтнамців та в'єтконговців на бік Південного В'єтнаму (за даними незалежних спостерігачів). У цій війні використовувався практично весь арсенал засобів інформаційних операцій, починаючи від тотального знищення м. Фулі у Північному В'єтнамі і закінчуючи першим в історії створенням пропаган-

дистської телевізійної мережі. Усього в конфлікті з американського боку було використано понад 1000 спеціалістів із СІО.

Необхідно зазначити, що спеціальні інформаційні та психологічні операції під час в'єтнамської війни були спрямовані як на безпосередніх противників (в'єтконговців та Північного В'єтнаму), так і на союзників (Південний В'єтнам) та населення США.

Наступною широкомасштабною ПсО стала інформаційна підтримка американського вторгнення в Гренаду. В операції було задіяно 1-й батальйон ПсО. Штатних сил і засобів батальйону цілком вистачило для створення радіостанції з передавачем потужністю 50 кВт і 11 годинами ефіру щодоби, видання газети «*Голос Гренади*», розповсюдження листівок тощо. Як наслідок — більшість особового складу армії Гренади добровільно здалася у полон.

Першою ПсО, що здійснювалася за ретельно розробленим планом, стала інформаційна підтримка висадки американців у Панамі. Незважаючи на ґрунтовну цілеспрямовану підготовку панамських збройних сил, очолюваних генералом Норьєгою, до оборони проти ЗС США і проти методів їхньої психологічної війни, відповідні американські військові та цивільні спеціалісти з ЦРУ, Держдепартаменту тощо загальною кількістю до 3,5 тис. осіб під час цієї операції мали чималі здобутки. Під час панамської кампанії вперше було широко вжито доктрину «дій, що турбують». Її сутність полягає у впливі на аудиторію, який не переривається на жодну секунду, не дає зосередитися, відпочити, відновити сили.

Масштабно застосовувалися війська ПсО й у війні у Перській затоці, коли вперше перед її початком були оприлюднені дві основні мети «Бурі у пустелі»: створення сприятливої суспільної думки в США та інших країнах світу стосовно подій; безпосереднє інформаційно - пропагандистське забезпечення воєнних дій. До участі в операції було залучено 8-й батальйон 4-ої групи ПсО американських ЗС, а також штатні підрозділи спеціального призначення. Крім того, відповідні функції виконували спеціалісти розвідувальних відомств США.

Після перемоги у війні у Перській затоці американські фахівці також здійснювали інформаційні операції проти режиму Саддама Хусейна. Формально ці операції спрямовувалися на захист курдського та шиїтського населення Іраку [118].

Масштабні ПсО та ІО було проведено й у межах операцій «*Морський ангел*» та «*Підтримка демократії*» (Гаїті, 1991, 1994рр.), «*Відродження надії*» та «*Спільний щит*» (Сомалі, 1992 - 1995 рр.) [119], «*Спільні зусилля*» (Боснія, 1996 р.) [120]. Практично всі миротворчі кампанії, що в них беруть участь США, супроводжуються психологічними операціями.

Не досягла бажаного успіху лише операція «*Відродження надії*» у Сомалі [121], що пов'язувалося американськими дослідниками з механічним перенесенням досвіду операцій у Перській затоці на Сомалі, поганим знанням місцевих традицій, відсутністю досвіду роботи у подібних умовах та необхідної

кількості фахівців зі знанням місцевих мов [116]. Аналіз причин поразки вказує на необхідність максимально враховувати конкретні умови під час здійснення операцій.

Зараз починають з'являтися матеріали стосовно ролі американських спецслужб у розпаді СРСР. Як зазначає у своєму надзвичайно відвертому та цікавому інтерв'ю «Независимой газете» перший міністр оборони незалежної Литви А. Буткявичюс, стратегія протистояння радянській армії під час січневої кризи 1991 р. спиралася саме на методи психологічної війни: «Насамперед ми мали не допустити фізичного та збройного зіткнення й перенести центр конфлікту в інформаційну та психологічну сфери. Інформація стосовно методів психологічної війни була отримана з Інституту Ейнштейна в США, який очолювала професор Джинна Шарп. Цей інститут займався такими розробками» [122]. Багато відповідних матеріалів можна знайти у мемуарах колишніх співробітників КДБ СРСР [123]. Одна з книг Дж. Шарп представлена нині на одному з українських сайтів [124].

З 1991 р. на Балканах США послідовно здійснюють низку спеціальних інформаційних операцій. Для цього у 1996 р. було сформовано оперативну групу «*Орел*», до якої входить 8-й батальйон ПсО, видається сербською мовою газета «*Гласник мира*». У цих операціях активно використовується символічний вплив на свідомість, наприклад, багаторазово підкреслюється приналежність американської військової форми [125]. У грудні 1996 р. різко зростає мовлення радіостанції «*Голос Америки*» на Балкани, причому інтенсивно наголошується, що це зроблено для заміни забороненої сербської радіостанції «Б - 52» [126]. Запит у пошукову службу Інтернет - порталу Alta Vista «*The Balkan Conflict and psyops*», зроблений о 14.18 06.03.99, дав такий результат: «Alta Vista found 238532 Web pages for you».

Однією з головних форм впливу на свідомість американські фахівці вважають здійснення «чорної» пропаганди. Конкретним її прикладом є діяльність мережі Prolink International inc., що складається з 47 «незалежних» ТВ - станцій з 60 - мільйонною аудиторією [127]. Ця телевізійна мережа вважається незалежною попри приховане фінансування спецслужбами США.

Досвід американських підрозділів зі здійснення спеціальних психологічних та інформаційних операцій найретельніше досліджений. Певні матеріали щодо використання Вашингтоном цих методів, хоча в апологетичному дусі, репрезентують матеріали Американської Асоціації психологічних операцій [128].

Роль інформаційно - психологічного забезпечення політики США найліпше ілюструє така цитата: «Показово, що найвищий військовий чин американської армії, Голова комітету начальників штабів генерал Джон Шалікашвілі у період гаїтянської кризи 1994 р. цілком відверто заявив: *«Ми не перемагаємо поки CNN не говорить, що ми перемагаємо»*. За шістдесят років - з 1916 р. до 1978 р. - співвідношення числа репортерів до числа воюючих «джи-ай» у США зросло у **1000 (!)** разів. За даними журналу

«*Military review*», якщо у першій світовій війні один журналіст припадав на 20 тисяч військових, то під час операції у Боснії - на 500 військовослужбовців» [129].

Активну інформаційно - пропагандистську діяльність здійснюють американські урядові структури і на пострадянському просторі. Так, державний секретар США М. Олбрайт під час зустрічі з лідерами опозиційних партій Казахстану у травні 2000 року заявила, що уряд США готується відкрити в Казахстані нову друкарню, яка буде безперешкодно друкувати незалежні газети. З відповідним проханням до уряду США і конгресу неодноразово звертався Акежан Кажегельдин (лідер опозиції, колишній прем'єр - міністр Казахстану) та інші лідери Форуму демократичних сил, що регулярно відвідують Вашингтон з робочими візитами. Офіційна версія створення цієї друкарні така: «У правлячих колах США чудово розуміють, що тотальний контроль держави над поліграфічними потужностями в Казахстані й інших державах Центральної Азії дозволяє «душити» опозиційні видання, не звертаючись до відкритого насильства. А друкарня, що знаходиться у власності уряду США, буде захищена від тиску спецслужб й адміністрації Казахстану» [130]. Фактично йдеться про пряме втручання у внутрішні справи республіки Казахстан під приводом захисту демократичних прав і свобод.

Нині у США створені та діють системи здійснення спеціальних психологічних операцій у межах ЦРУ та Міністерства оборони (підрозділи Об'єднаного командування спеціальних операцій). Поряд з ними у військових та спеціальних службах створено стрункy систему роботи зі ЗМІ та з громадськістю. Загальна проблематика цієї сфери визначена директивою міністра оборони 5122.5 та настановами Об'єднаного комітету начальників штабів ЗС США.

Систему зв'язків з громадськістю та пресою очолює помічник міністра оборони зі зв'язків з громадськістю. У складі об'єднаних командувань ЗС США у зонах для роботи зі ЗМІ під час бойових дій передбачено розгортання оперативних центрів зі зв'язків з громадськістю. Система служб зі зв'язків з громадськістю сягає рівня дивізія - окрема бригада [131]. Для підтримки системи інформаційно - пропагандистського забезпечення зовнішньої політики у США створено чітку систему підготовки кадрів для психологічної війни та здійснення спеціальних інформаційних операцій.

У межах системи проходження військової служби офіцерським складом (Officer Personnel Management System, OPMS) передбачено існування функціональної області (FA) «психологічні операції та робота з цивільним населенням» (FA 39). На 1998 р. у цій функціональній області налічувалося понад 1000 офіцерів у званнях від капітана до підполковника. Діють системи перепідготовки та підвищення кваліфікації, заохочується навчання офіцерів у магістратурі (докторантурі) [132].

Основним підрозділом психологічних операцій у ЗС США є батальйон, що налічує від 200 до 400 чоловік і складається з груп: радіо, телемовлення,

розповсюдження листівок, гучномовців, спецефектів, створювачів пропагандистських текстів, планування, розвідки, допоміжних служб тощо. Структуру батальйону побудовано таким чином, щоб він міг здійснювати спеціальні психологічні операції оперативно - стратегічного рівня. Проведення спеціальних інформаційних операцій здійснюється із залученням сил і засобів Розвідувального управління МО (РУМО), ЦРУ та інших спецслужб США.

Прикладом підрозділу з психологічних операцій є 193-тє спеціальне оперативне крило Національної гвардії штату Пенсільванія [133]. Основним завданням цієї одиниці є здійснення своїх задач із застосуванням спеціальних літаків, радіо- й телетрансляторів на базі С - 130 (С - 130Е/RR). Крило має базу в США і в Європі (Гамбург, ФРН), особовий склад налічує близько 1000 осіб, серед яких близько 200 - кадрові військовослужбовці. Річний бюджет підрозділу становить понад 35 млн. дол. (за курсом НБУ на січень 2003 р. - близько 190 млн. грн. Для порівняння: бюджет СБ України у 2001 р. складав 484720,4 тис. грн, тобто близько 90 млн. доларів).

Німеччина (ФРН). Єдина серед європейських країн, що за мирних часів має розгорнуті частини психологічної війни. За часів Боннської республіки було створено потужну систему зовнішньополітичної пропаганди, у складі якої: німецьке інформаційне агентство, спеціальне управління інформацією канцелярії канцлера ФРН, радіостанція «Німецька хвиля», спеціальні підрозділи БНД, система Гете - інституту, квазідержавні фонди Ф. Еберта та К. Аденауера [134].

Величезного досвіду німецька система зовнішньої пропаганди та спеціальних інформаційних/психологічних операцій набула за часів існування двох німецьких держав та їхнього протиборства, що точилося насамперед в інформаційній сфері.

У 2000 р. в м. Пулаху (ФРН) у штаб-квартирі БНД відбулася науково - практична конференція *«Інформаційні методи ведення війни»*, на якій було підбито підсумки щодо використання інформаційних операцій в локальних конфліктах, зокрема, у Косово у 1999 р. На думку генерала В. Ерца, колишнього речника НАТО, інформаційні служби Альянсу припустилися певних помилок, зокрема, в окремих відеоповідомленнях про воєнні дії відеоряд не відповідав коментарю [135].

Індія. У 1990 р. при Міністерстві оборони Індії було створено спеціальну службу інформаційних операцій. Структура складається з департаменту організації воєнних психологічних операцій і двох відділів (закордонних і внутрішніх операцій). Свою роботу служба координує з Комітетом начальників штабів ЗС Індії, військовою розвідкою, МЗС тощо [136]. Результативність цієї діяльності засвідчили події у Каргилі (травень - червень 1999 р.) [137], коли світ дивився на перебіг збройного конфлікту крізь призму індійських інтересів.

Ізраїль. У спецслужбах цієї країни працюють найліпші фахівці у сфері спеціальних психологічних та інформаційних операцій. *«Богообраний на-*

род» за свою тисячолітну історію здійснив та витримав не один найжорстокіший вплив, зокрема, в інформаційній сфері. Успішне використання найнесприятливіших зовнішніх умов, вміння перетворювати нищівну поразку на найвидатнішу перемогу — це все стосується і спецслужб Ізраїлю.

Прикладом однієї з найвдаліших спеціальних психологічних операцій, що за багатьма своїми характеристиками наближається до операції інформаційної, можуть слугувати події 1957- 1958 рр. У той час провідну спецслужбу Ізраїлю, що працювала проти СРСР — Російський відділ (РВ) МЗС (штат центрального апарату до 40 осіб, резидентура у посольствах Ізраїлю в Росії (Москва) та інших соціалістичних країнах) очолював Нехімія Леванон (колишній перекладач Головного управління військової контррозвідки РСЧА *«Смерш»* у 1943—1944 рр.). Співробітники РВ скористалися ефектом від критики сталінізму, ініційованої М. Хрущовим, для роздмухування кампанії навколо антисемітизму в СРСР. За авторитетною думкою І. Лейблера, одного з керівників Всесвітнього єврейського конгресу, у майбутньому ця операція спричинила розколи у Французькій, Італійській, Ізраїльській та кількох інших компартіях [138].

Китай (КНР). Як зазначалося, стратегія непрямих дій, зокрема психологічних впливів, активно використовувалася Піднебесною з найдавніших часів. З відносно сучасних операцій можна назвати вдале використання китайцями дезінформації стосовно своїх економічних відносин із Заходом на початку 70-х років [139].

Важливим чинником здійснення інформаційних операцій з боку Китаю є широке використання спецслужбами цієї країни, а також (що показово) кримінальними організаціями мережевих принципів організації. З іншого боку, відсутність християнського підґрунтя у китайській культурі значно спрощує здійснення ІО, фактично знімаючи проблеми моральності.

Росія (СРСР). Російський уряд активно використовував засоби спеціальних психологічних та інформаційних операцій з найдавніших часів. На початку XX ст. надзвичайно активна пропаганда здійснювалася на території Буковини та Галичини. Як зазначав один з депутатів австрійського парламенту, «майже в кожному селі Східної Галичини сидить платний російський агент і ціла низка повітів краю охоплена небувалою російською агітацією. У маленьких селищах створюються російські бурси - школи, де дітей навчають російській мові. Кожний хлоп, що віддає дітей у ці бурси, отримує рублі на руки. Агітація здійснюється так беззастережно, що агітатори не встигають навіть розміняти рублі на кропи й надають цю можливість самим селянам на міських ярмарках» [140]. На російські гроші були створені й діяли «москвофільські товариства у Львові та інших містах Галичини. Субсидії, що сягали 200 тис. рублів на рік передавалися через Галицьке — Російське благодійне товариство, утворене 15.12.02 р. у Санкт-Петербурзі.

Початок використання радянською розвідкою так званих «активних заходів» офіційно датується 11 січня 1923 р., коли Іза поданням заступника Го-

лови ДПУ І.С. Уншліхта було ухвалено рішення Політбюро ЦК РКП(б) щодо створення спеціального міжвідомчого Бюро з дезінформації [141]. У цьому рішенні окреслено завдання Бюро.

1. Концентрація відомостей про ступінь обізнаності іноземних розвідок щодо ситуації в Росії, що надходять до ДПУ, Розвідувального управління Червоної Армії, інших відомств.
2. Облік і характеристика відомостей, що цікавлять противника.
3. З'ясування ступеня обізнаності противника про нас.
4. Складання і технічне виготовлення неправдивих відомостей і документів, що створюють у противника хибне уявлення про внутрішній стан Росії, організацію й стан Червоної Армії, політичну роботу керівних партійних і радянських органів, роботу НКЗС тощо.
5. Доставка вказаних вище матеріалів і документів противнику (через відповідні органи ДПУ та Розвідувального управління).
6. Розробка статей для преси; формування ситуації для поширення різного роду фіктивних матеріалів з представленням їх на розгляд одному із секретарів ЦК РКП(б).

Одним з непрямих свідчень ефективності дій цього підрозділу є той факт, що діяльність Бюро «не тільки практично не залишила в архівах розвідки жодних слідів з описами заходів, а й навіть опосередкованих посилань про тих, хто тією чи іншою мірою мав відношення до їхньої розробки» [142].

Вирішальним етапом діяльності радянських спецслужб у напрямі психологічної та інформаційної воєн стала друга світова війна.

Психологічні та інформаційні операції у 1941 - 1945 рр. здійснювалися у кількох напрямах.

1. На власне населення (у межах цих операцій доцільно розглядати виступи голови РНК СРСР В. Молотова на сесії ВР СРСР 31.10.1939 р. «...Про зовнішню політику Уряду» («Нечего доказывать, что в момент полного распада Польского государства наше правительство обязано было протянуть руку помощи... братьям украинцам и братьям белорусам») та 22.06.41 («...Братья и сестры. К Вам обращаюсь я, друзья мои... Враг будет разбит. Победа будет за нами»), проходження колони німецьких військовополонених через Червону площу у серпні 1944 р., парад Перемоги тощо).
2. На армію та населення Німеччини (створення та діяльність Комітету «Вільна Німеччина» на чолі з фельдмаршалом Паулюсом).
3. На союзників по антигітлерівській коаліції.

Після першого періоду війни акцепт в інформаційно-пропагандистській діяльності посунувся з класових аспектів на «загальнолюдські». Робота велася у позаідеологічній сфері, не «***проти***», а «***за***». За даними львівської дослідниці Л. Леонтьєвої, у 1941 р. класові принципи використовувалися у понад *60 %* радянських пропагандистських матеріалів, а у 1943 р. вже у 35 %

[143]. Як свідчить К. Крайніков, у другому періоді війни (1943 - 1945 рр.) ефективність спеціальних операцій була доволі висока [144]. Досвід, накопичений протягом війни, активно використовувався у подальшому. Цікавий огляд діяльності радянських спецслужб у цій сфері можна знайти в роботі Л. Бітмана, колишнього керівника відповідного підрозділу чехословацької розвідки, який після подій 1968 року переїхав на Захід [145].

Важливий етап історії використання спеціальних інформаційних операцій репрезентує боротьба спецслужб СРСР з націоналістичним підпіллям в Західній Україні протягом 1944 - 1956 рр. Як свідчать матеріали Служби безпеки ОУН, однією з найнебезпечніших для закордонної частини ОУН була операція щодо утворення групи Української революційної демократичної партії (лівиця). Використовуючи введених агентів, МДБ СРСР захопило провідні позиції у цій групі. За їхньою допомогою було розпочато цілеспрямовану кампанію щодо формування іміджу ОУН як сили, що дотримується титоїстських позицій. Інакше кажучи, закордонним ЗМІ та представникам розвідок країн західного блоку надавалася інформація щодо «просоціалістичних, проте фрондерських позицій» ОУН, що значно ускладнювало діяльність цієї організації [146].

Активно здійснювали ПсО та ІО й особливі відділи радянських окупаційних військ у Німеччині та Австрії. Об'єктом їхньої зацікавленості були переміщені особи, багато з яких мешкали на теренах переможених країн у західних зонах. Інструкцію Верховного комісара державної безпеки СРСР в окупаційних зонах, опубліковану в матеріалах СБ ОУН, можна розглядати як вдалий приклад керівного документа щодо стратегії оперативної ІО [147].

Вдалим винаходом радянських спецслужб щодо репатріантів було створення так званого комітету генерала Михайлова. Основним завданням цієї організації стало забезпечення повернення емігрантів до СРСР та сприяння агентурній роботі в їхньому середовищі. До комітету залучалися провідні діячі культури (наприклад, Ю. Смолич). Слід зазначити, що залучення відомих літераторів до своєї діяльності здійснювало й ОУН. Наявні відомості про звернення до М.Рильського, який відмовився від цієї пропозиції.

Ефективність цих заходів, що мали наслідком значне послаблення позицій ОУН в емігрантському середовищі, визнається й СБ ОУН [148].

У ПГУ КДБ СРСР (зовнішня розвідка) існувало Управління «А» [149], що відповідало за «активні заходи» (одним з його напрямів були спеціальні інформаційні операції).

У СРСР існувала потужна система зовнішньополітичної пропаганди, до якої відносилися такі установи.

1. ***Агентство преси «Новини» (АПН)***. Створене у 1947 р., агентство виконувало роль неофіційного рупора СРСР (на внутрішньополітичній арені цю роль відігравала «Литературная газета» [149]).

2. ***Мережа «товариств дружби*** з ...», що діяли практично в усіх важливих, з точки зору зовнішньої політики СРСР, країнах.

3. Закордонне радіомовлення СРСР та інші ЗМІ, спрямовані назовні (журнал «Советский Союз» та інші).

Цікаву розвідку щодо ефективності цієї системи у післявоєнні роки підготував російський вчений А. С. Стикалін [150]. Він пише, що радянською стороною активно використовувався керований витік інформації у пресу під час переговорів. Російський дипломат Ю. Квіцинський відзначає постійне використання «недисциплінованості» західнонімецького та східнонімецького МЗС (це спричиняло надання пресі відповідних матеріалів) на переговорах чотирьох союзних держав щодо статуту Західного Берліну у 1971 р.[151].

Прикладом спеціальної психологічної операції, здійсненої КДБ, може слугувати публікація 1982 р. в індійській газеті «Patriot» щодо вірусу СНІДу, який начебто було створено в таємних лабораторіях Пентагону [152]. До речі, ця газета неодноразово використовувалася радянськими спецслужбами для вкидання інформації. Розкручування здійснювалося, зокрема, через «Литературную газету». Особлива роль останньої в радянській післявоєнній структурі ЗМІ висвітлена у мемуарах К. Симонова [149]. Останнє робить операцію щодо висунення американської версії походження вірусу СНІДу модельною.

Довідка *«Засоби й методи радянської пропаганди»* підготовлена підкомісією юридичного комітету сенату США з метою збільшення асигнувань па психологічну війну [153]. Можна стверджувати про причетність КДБ СРСР до руху за недопущення розміщення ракет «Pershing - 2» у Західній Європі на початку 80-х років.

Залишаються ще недослідженими такі цікаві постаті радянських фахівців з інформаційної боротьби, як І. Еренбург, В. Луї, які жили на Заході та репрезентували неофіційну позицію СРСР. Також чекає на свого дослідника історія взаємозв'язків і взаємовпливів радянських спецслужб і лівих кіл Заходу, певних національних діаспор, насамперед вірменської та єврейської.

Слід зупинитися і на системі захисту радянського суспільства від спеціальних інформаційних операцій, що була репрезентована насамперед 5-м управлінням КДБ СРСР та його підрозділами у місцевих органах державної безпеки.

Акцент у боротьбі з *«ідеологічною диверсією»* робився на заборонювальні заходи, що, зрештою, не могло дати належного ефекту. Наслідки цього відбилися на суспільних процесах, що призвели до колапсу СРСР.

Разом з тим слід відзначити дуже вміле, у певному сенсі класичне, використання радянським режимом наявних засобів для досягнення внутрішньополітичних цілей. Йдеться насамперед про «найважливіше з мистецтв» - кінематограф. Як приклад розберемо один з найпопулярніших радянських фільмів - комедію Л. Гайдая ***«Кавказька полонянка»***. Сучасне сприйняття його характеризує оглядова стаття *«Леонид Гайдай и эпоха беззаботного смеха»* [154]. Час виходу фільму — середина 1960-х років (1967 р.) — супроводжувався значним посиленням напруженості у відносинах Москви з місцевими владними елітами Кавказу і Середньої Азії. Силу ос-

танніх репрезентує відома історія щодо висновків Комісії Міністерства держконтролю СРСР на чолі з міністром В. Меркуловим. Її матеріали стосовно корупції в Азербайджані, зокрема у ЦК КП Азербайджану, першим секретарем якого був Багіров, були заховані під сукно особисто Сталіним з формулюванням: «Не треба загострювати, хай живуть як бажають».

Кожен з образів та епізодів зазначеної комедії допускає кілька трактувань: від виключно гумористичного до суто політичного. Наприклад, Шурик — збирач народного фольклору у — певній іпостасі може розглядатися як агент КДБ, що відслідковує громадську думку. Сюжет про санепідемстанцію та фіктивну епідемію ящура викликає стійкі алюзії до методів боротьби радянської влади з басмацтвом, а перебування Шурика в психіатричній лікарні взагалі не вимагає пояснень. Дуже важливий момент фільму — механізм розв'язання суперечності, в якому зло (відкрите нехтування радянським законом) з боку т. Саахова (типовий представник місцевої еліти) покарано за місцевим законом (законом гір), а рішення радянського суду лише легітимізує останній. Останнє наголошує на визнанні Москвою умов «контракту» з місцевими елітами. За цими умовами, азіатські та кавказькі місцеві еліти демонструють свою лояльність до Центру, а Центр значно обмежує своє втручання у місцеві справи. Варто зазначити, що розрив цього контракту з боку Москви, проголошений відомою *«узбецькою»* справою слідчих Г. Гдляна і М. Іванова був одним з важливих чинників розпаду СРСР.

Як свідчать матеріали російської та західної преси і розробки аналітиків [154], підрозділи спеціальних інформаційних та психологічних операцій активно діють у російських спецслужбах, зокрема, СВР РФ і ФСБ РФ, і після розпаду СРСР.

Як пише фахівець Центру досліджень конфліктів міністерства оборони Великобританії Г. Беннет, у складі СВР РФ діє підрозділ спеціальних інформаційних та психологічних операцій — прямий спадкоємець традицій Управління «А» [155]. Зокрема, значного розголосу набуло малоефективне використання федеральними силами методів спеціальних інформаційних операцій у Чечні протягом 1994 - 1996 рр. У 1999—2002 рр., навпаки, можна відзначити доволі високий рівень інформаційно - пропагандистської діяльності російської держави, особливо у власному суспільстві.

Види та структурні характеристики інформаційних операцій

Як вважає російський науковець Расторгуєв, переваги спеціальних інформаційних операцій полягають у наступному.

1. Латентність (скритність) агресивних дій.
2. Практична відсутність людських втрат.
3. Можливість вести бойові дії на кілька фронтів.
4. Відсутність реваншистського ефекту.
5. Необізнаність опонента з точним арсеналом інформаційної війни.

6. Можливість поетапного охоплення населення (спочатку роблять-ся акценти на лідерів думок, молодь, що може призвести до виникнення ефекту ланцюгової реакції).

7. Неможливість ідентифікації ворога.

8. Неможливість протидії впливу, якого не відчуваєш.

9. Відсутність видимих руйнувань, в результаті чого суспільство не може включити захисні механізми.

На думку автора, цей список дещо перебільшений. Наведемо найва-гоміші переваги подібних операцій:

- практична відсутність людських втрат;
- відносно невеликі витрати на проведення операції;
- відсутність реваншистського ефекту, оскільки переможені не відчува-ють свого програшу.

Таким чином, можна констатувати, що сучасна розвинена держава ли-ше за допомогою інформаційних засобів боротьби може повністю розгромити супротивника.

Найактуальнішими типами інформаційних операцій для розв'язання завдань дослідження є ті, здійснення яких передбачається за мирних часів.

Виходячи з наведеної у попередніх розділах монографії класифікації та аналізу перебігу сучасних подій, на думку автора, доцільно окремо розглянути певні види інформаційних операцій.

- Операції, спрямовані проти суб'єктів, які ухвалюють рішення (СУР).
- Операції, спрямовані на компрометацію, завдання шкоди опонентам.
- Операції, спрямовані на політичну (економічну) дестабілізацію.

Операції, спрямовані проти СУР, репрезентують перехідний тип опе-рацій між спеціальними психологічними та інформаційними. Незважаючи на використання психологічних особливостей людини під час такої операції, фактично здійснюється зміна структури комунікації. Це дозволяє вважати операції проти СУР як інформаційними, так і психологічними, навіть перши-ми більшою мірою.

Інформаційні операції різних типів здійснюються за приблизно однако-вою схемою. Виходячи із загальних положень системного аналізу та ма-теріалів, наведених у попередньому розділі, ця схема виглядає як поєднання кількох етапів.

- Попередній етап, або етап планування І0. Метою діяльності на цьому етапі є планування операції, зокрема, визначення доцільності її здійснення, цілей, завдань, сил і засобів, цільової аудиторії впливу, прийомів і методів впливу на систему, соціально - політичної комунікації тощо. Найважливішим завданням цього етапу є пошук або формування у складі об'єкта впливу «груп підтримки» («п'ятої колони»), на які мож-на було б спертися під час проведення інформаційної операції.
- Інформаційний привід. Під інформаційним приводом розуміють подію (можливо, й псевдоподію), що її можна використати як привід для про-

пагандистської кампанії або інформаційної операції (впливу на суспільно-політичну комунікацію). Вибір інформаційного приводу становить окрему проблему, яку докладніше розглянуто нижче. Тут зазначимо лише, що повідомлення про інформаційний привід має переслідувати кумулятивний ефект.

- «Розкрутка» інформаційного приводу. Цей етап є основною частиною будь-якої інформаційної операції. Його сутність полягає у використанні інформаційного приводу задля досягнення цілей операції, тобто для посилення, формування або руйнування певних структур суспільне-політичної комунікації, або гегемонії.
- «Вихід з інформаційної операції, або етап закріплення». Найважливіше завдання цього етапу завершення пропагандистської кампанії або інформаційної операції після досягнення поставлених цілей або внаслідок форсмажорних обставин [156].

Етап планування інформаційної операції. Порядок діяльності на цьому етапі може варіюватися (порядок, визначений автором, побудовано з позицій загальноприйнятого механізму планування в силовій галузі) [157].

1. Визначення мети.
2. Визначення об'єкта.
3. Зважения сил і засобів, ресурсів, визначення виконавців.
4. Визначення методів і прийомів.
5. Розробка приблизного сценарію.
6. Визначення критеріїв оцінки успіху.

Подібний загальний план пропонують й автори Інтернет - сторінки, присвяченої реалізації впливів на свідомість (школа американського психолога Р. Чалдіні) [158]. Кожний з перерахованих вище пунктів можна деталізувати і далі, проте досягнутий рівень деталізації виявляється для цілей даного дослідження оптимальним.

Етап створення інформаційного приводу. Як інформаційний привід можна використовувати практично будь-яку подію, про що свідчить відомий історичний анекдот стосовно гулі алжирського бея. Суть цього анекдоту полягає в наступному: французький журналіст, перебуваючи в Алжирі, побачив на обличчі тамтешнього бея гулю та передав в Європу, що під час збройної сутички бея побили вороги. Бей був союзником Франції, тому газета надрукувала повідомлення про антифранцузьку змову в Алжирі, під час якої постраждав бей. Німецька газета передрукувала це повідомлення з коментарем про французькі загарбницькі плани у Північній Африці й закликала підтримати волелюбних арабів. МЗС Франції після одержання німецької газети викликало посла Німеччини для пояснень підтримки антифранцузької змови.

Втім, набагато краще, коли інформаційний привід дійсно є важливою подією сам по собі. Такими є події, що якось співвідносяться (чітко супере-

чать) наявним актуальним стереотипам аудиторії, порушують певні заповіти, акти святотатства, надзвичайне насильство тощо. Варто зазначити, що дослідження стереотипів - сама по собі цікава проблема, яка потребує чіткого наукового підходу.

Другий варіант інформаційного приводу — події, що здійснюють безпосередній вплив на осіб, які складають переважну більшість цільової аудиторії. Дієвим прикладом подібного приводу для масової аудиторії є ті події, що впливають на її базові потреби (за А. Маслоу). Це, передусім, негаразди в економічному житті, особливо у сфері постачання продовольства (відомі «хлібні бунти»: Лютнева революція в Росії, події у Болгарії зими 1997 р. тощо). Варто також назвати непередбачувану різку девальвацію національної валюти, стрибок цін [159].

Як доводить С. Кара-Мурза, базові потреби дуже активно використовувалися у повсякденній символічній комунікації. Загроза голоду, донині базова у нашій свідомості, активно експлуатувалася в рекламі холодильників, а загрози безпеці та недоторканості житла — в рекламі кондиціонерів [160].

У більшості випадків як інформаційний привід використовують певні негативні події як такі, що набагато чіткіше відбиваються у свідомості аудиторії. Саме негативні повідомлення найшвидше продукуються та можуть впливати на структуру системи соціально - політичної комунікації.

На привід мають впливати характеристики цільової аудиторії, зокрема, її національні, соціальні та інші стереотипи і настанови, взагалі характеристики системи соціально - політичної комунікації.

«Розкрутка» інформаційного приводу. Цей етап фактично є пропагандистською кампанією. Проте врахування вимог зворотного зв'язку, важливе й під час звичайних пропагандистських кампаній, в інформаційних операціях набуває ключового значення.

Аналіз досвіду використання інформаційних операцій, дозволяє дійти певних висновків щодо «розкрутки» інформаційного приводу за сучасних умов.

Наприклад, для успіху інформаційного впливу необов'язково мати тотальний контроль над усіма ЗМІ країни. Цілком достатньо контролювати кілька видань (наприклад, 5-7) та 1-2 канали телебачення, кілька «розкручених» Інтернет - видань. Звичайно, тотальний контроль над ЗМІ, з одного боку, є бажаним, але в умовах ворожого середовища досить контролювати тільки найвідоміші розважальні, тобто ті, що дивляться, але не політичні ЗМІ. Цей висновок, що отримав назву ідеї керівних висот, на думку автора, не завжди може бути поширений на інші, недестабілізуючі напрями інформаційного впливу. Як відомо з теорії систем [161], тривкість будь- якої системи визначиться її найслабкішою ланкою. Тому, знайшовши цю ланку і спрямувавши саме на неї зусилля, можна добитися необхідного ефекту з мінімумом витрат.

Закріплення, або вихід з інформаційної операції. Будь-яка інформаційна операція використовує маніпулювання свідомістю (суспільно-політичною комунікацією). Як вважає Є.Доценко, однією з основних ознак маніпулювання є його незрозумілість, прихованість для об'єкта [162]. Інакше кажучи, розгадане маніпулювання за визначенням є невдалим: якщо об'єкт впливу зафіксує здійснення інформаційної операції, він зможе протидіяти їй. Саме тому необхідно здійснювати «м'який» вихід з інформаційної операції. Часто цією вимогою нехтують, що призводить до значного, а подекуди й катастрофічного послаблення ефекту операції. На цьому етапі необхідно закріплювати досягнуті результати. Це особливо важливо в операціях, спрямованих проти суб'єктів ухвалення рішень.

Важливість цього етапу визначається також тим, що інформаційні операції належать до царини соціальних технологій. Соціальна тканина сучасного суспільства і дуже консервативна, і дуже чутлива система. Зберігаючи основний напрям розвитку, вона може значно змінювати траєкторію відповідно до характеру впливів. Певним чином наслідки тонких, зокрема інформаційних, впливів на майбутнє соціально-політичної системи можна порівняти з розповсюдженням хвиль у середовищі з надзвичайно ускладненою внутрішньою структурою. За образним порівнянням українського дослідника О. Хамрая (при особистому спілкуванні з автором), наслідки інформаційної операції можуть відчуватися, а отже, вона може тривати й через століття після того, як зітліли кістки тих, хто її розпочинав.

У багатьох випадках ці далекі наслідки конкретних дій жодним чином не піддаються прогнозуванню і можуть обернутися проти організаторів. Досить нагадати історію з підтримкою Генеральними штабами Німецької та Австро-Угорської імперій групи Володимира Леніна задля дестабілізації політичної ситуації в Росії [163]. Операція дістала успіху, проте згодом діяльність Леніна та його соратників сприяла падінню імперій-донорів. Понад те, прогноз віддаленіших наслідків інформаційних операцій позбавлений практичного сенсу. Фактично це неможливо, виходячи зі складності процесів самоорганізації у комунікативній структурі сучасного суспільства.

Розглянувши загальну схему здійснення інформаційних операцій, докладніше проаналізуємо характерні особливості різних типів інформаційних операцій.

Операції, що реалізують вплив на суб'єктів, що ухвалюють рішення (СУР).

Розглянемо визначення поняття «суб'єкт, який ухвалює рішення». Традиційно це поняття охоплює сукупність трьох доволі різних частин:

а) особи, які ухвалюють рішення;

б) компактні структури, що ухвалюють рішення (адміністрації, штаби, комісії тощо);

в) розподілені, або мережеві, структури, що ухвалюють рішення [164]. Зауважимо, що в реальному житті чітко відокремити типи операцій за суб'єктами впливу неможливо, проте наведена класифікація доречна. Ретельно розглянемо перший пункт зазначеної класифікації. Незважаючи на певні зміни, що відбулися останніми десятиріччями у процесі ухвалення рішень, роль політичного лідера, державного діяча залишається надзвичайно важливою, а у багатьох випадках — вирішальною. Саме на цьому припущенні ґрунтується ідея впливу на свідомість осіб, які схвалюють рішення (ОУР).

Операції, спрямовані проти ОУР, можна розділити на два типи: контактні та позаконтактні, або дистантні.

Контактні операції відомі з давніх часів, їхнє підґрунтя — ідея підведення агентів до ОУР і реалізація через них впливу на рішення. Екзотичним прикладом подібних дій є операції венеціанської розвідки XVI століття [165; 166]. За тих часів основним суперником Венеції у боротьбі за вплив та панування у Середземномор'ї була Османська імперія. Використовуючи звичаї турків, венеціанська розвідка неодноразово розробляла та здійснювала багатокрокові операції щодо цілеспрямованого введення вихованих дочок своїх правлячих сімейств у гарем турецького султана, щоб ті досягали в ньому стану «улюбленої дружини» і спрямовували політичні прагнення султана у сприятливому для Венеції напрямі.

Цей приклад цікавий також тим, що фактично йшлося про здійснення непрямого впливу. Софія Бофоні (ймовірно, венеціанський агент) працювала не безпосередньо із султаном (який навіть теоретично не міг прислухатися до порад жінки у політичних питаннях), а з валіде, вплив якої на рішення сина був, за давньою традицією, визначальним.

Для порівняльної характеристики стереотипів мусульманської та європейської свідомості показовим є такий факт. В момент небезпеки європеєць намагається передусім врятувати дітей, потім дружину і тільки потім мати, мусульманин же намагається врятувати матір; аргументація тут приблизно така: дітей можна ще народити, ніхто не заборонить одружитися з іншою жінкою, але матір вже не повернеш.

Наведений приклад доводить надзвичайну залежність інформаційних операцій від структури суспільства, особливо його панівних кіл.

Можна навести безліч інших, ближчих до сучасності, прикладів [167].

Проте подібні операції відносяться швидше до стандартних методів спецслужб. Згадаємо широко популярних після виступів колишнього Голови КДБ СРСР В. Крючкова «агентів впливу» [168]. Ця проблематика ретельно досліджена у спеціальній, зокрема науковій, літературі.

Суттю інформаційних операцій проти ОУР є використання особливостей їхніх психотипів. За конкретних соціальних умов ОУР стають люди певного психологічного типу, знаючи який можна здійснювати вплив па структуру їхньої комунікації, а через це — забезпечувати успішне маніпулювання ними.

Канали передачі інформації ОУР можуть бути найрізноманітнішими. Можна ефективно використовувати засоби масової інформації, настінний живопис (графіті), чутки, навіть офіційні документи. Головною вимогою до каналу є максимальна ймовірність доведення інформації до відома ОУР. Американський науковець Р. Чалдіні фахівець у сфері психології впливу, після ретельного аналізу емпіричного матеріалу виокремлює сім основних механізмів психологічного впливу. Вони побудовані за схемою «посилка» — «відповідь» [169]. На підґрунті кожного механізму може бути побудовано сценарій, схему реалізації дистантного впливу на ОУР. Їхній аналіз є, на погляд автора, дуже складним науковим завданням.

Операції, спрямовані на інших суб'єктів ухвалення рішень, типологічне близькі до операцій проти ОУР. При їхньому плануванні та здійсненні необхідно враховувати, що навіть суб'єкти ухвалення рішень другого типу, не кажучи вже про третій, мають певну структуру і «живуть своїм внутрішнім життям», тобто є соціальним організмом. Тому необхідно досліджувати внутрішні взаємозв'язки, стосунки в організації. Зокрема, дуже важливо з'ясувати неформальну структуру, порядок та процедуру ухвалення рішень, наявність ворогуючих партій (фракцій) тощо. Одним з методів врахування подібних характеристик є розробка структурно—інформаційних карт організації. Йдеться насамперед про необхідність врахування структур внутрішньої комунікації у СУР.

Важливішим підтипом операцій, спрямованих проти СУР, можна вважати підготовку та сприяння просуванню майбутніх політичних лідерів.

Операції, спрямовані на компрометацію, завдання шкоди опонентам. Подібні операції найчастіше здійснюються з метою послаблення позицій і/або, якщо це можливо, «усунення» опонентів на першому етапі операцій з дестабілізації, «виключення» їх з процесів соціально—політичної комунікації або дослідження їхнього впливу на неї. Зміст поняття «матеріал, що компрометує» суттєво залежить від національних, історичних та інших умов. Те, що є компроматом для одного часу, необов'язково є таким за інших часів. Необхідно зазначити, що поняття компромату жорстко пов'язане з чинною ідейно - політичною гегемонією.

Можна розрізняти два основні типи компрометувальних операцій.

1. Спрямовані на підрив гегемонії.
2. Спрямовані на витіснення певної особи (групи осіб) з панівного прошарку.

Операції першого типу детальніше описані у наступному розділі. Найпоширенішими є операції другого типу, їхнім прикладом є хакерські дії в Інтернеті. Невідомі знищують або спотворюють веб - сторінки політичних ворогів. Дуже поширена заміна правильних посилань (ліпків) на неправильні, що виводять, наприклад, на порнографічні сайти. У 1997—1999 рр. зазнали подібних впливів веб - сторінки президентів Польщі, Білорусії та Іраку.

Одним з найактуальніших прикладів подібних масованих компаній можна вважати дії, спрямовані на формування психологічного іміджу країни у світовому інформаційно-символічному просторі. Розглянемо цю проблему на прикладі України.

Проблема міжнародного іміджу України — одна з найпопулярніших тем дискусій перших років незалежності. У 1992 р. вона розглядалася переважно в контексті боротьби за самостійність, утвердження державного суверенітету. Основна причина необхідного сприйняття України світовим суспільством вбачалася в тім, що світ дивився на неї крізь «московські окуляри».

На грунті здійсненого українськими науковцям аналізу масиву впливової західної (американської та англійської) преси можна стверджувати, що у цих ситуаціях чітко простежується наявність єдиного координаційного центру, діяльність якого має прихований характер та здійснюється насамперед із застосуванням синергетичних механізмів [170]. Найвідомішим прикладом, на думку автора, є масована кампанія щодо ядерного роззброєння України [171]. Найпомітнішим моментом цієї кампанії була публікація таємної доповіді ЦРУ щодо кризового становища в Україні у грудні 1993 р. Інформаційна операція досягла мети у січні 1994 р., коли у Москві було підписано спільну Заяву США, РФ та України щодо ліквідації української ядерної зброї.

Напередодні практично кожної важливої зовнішньополітичної акції США стосовно України в американській пресі здійснюється кампанія, що має на меті «натиснути» на українську дипломатію. Українські високопосадовці починають виправдовуватися, переговорні позиції відразу погіршуються, що призводить до якісних змін у характері та обсязі поступок. Найпоказовішим можна вважати скандал навколо поводження НБ України з кредитами МВФ, застрільником якого виступала найвпливовіша англійська бізнес - газета *«The Financial Times»* (зима— весна 2000 р.).

Показовою з цього боку є також інформаційна кампанія навколо продажу станцій радіотехнічної розвідки «Кольчуга» до Іраку, яка продемонструвала як велику ефективність цього засобу зовнішньої політики США, так і майже повну неготовність України до обстоювання своїх національних інтересів у сучасних умовах.

Операції, спрямовані на дестабілізацію політичного (економічного) стану. Подібні операції є важливим видом інформаційних операцій. Основною їхньою метою є дестабілізація політичної ситуації в регіоні, країні, створення умов для досягнення певної мети, наприклад, приведення до влади дружньо налаштованих урядів (або зміна політичного курсу).

Необхідно чітко усвідомлювати, що дестабілізація ніде, ніколи та за жодних обставин не може бути самостійною. Для з'ясування мети операції, її дослідження чи з метою захисту від неї вкрай необхідно розглядати події відповідно до ситуації. Нині існує широкий набір методик і сценаріїв подібних операцій. Практично всі вони побудовані за трикомпонентною схемою.

1. Дискредитація влади з метою її подальшої де легітимації (підрив чинної гегемонії або її певних складових).

2. Створення та подальша підтримка опозиції (формування ядра майбутньої гегемонії).

3. Приведення опозиції до влади та закріплення позитивних результатів операції.

Необхідно ще раз підкреслити умовність цієї та інших подібних схем. Можна розглядати операції, метою яких є «*керована нестабільність*». Ретельніше один зі сценаріїв інформаційних операцій буде розглянуто нижче.

Неабиякою є важливість останнього типу операцій, бо, як відомо, існують три основні форми іноземного панування [172]:

- *пряме, безпосереднє;*
- *у формі гегемонії;*
- *змішане.*

Описані нижче сценарії дозволяють забезпечити панування у гегемонії, а перехід від неї до першої або історично найпізнішої третьої форми — питання часу та тактичної доцільності.

Сценарії спеціальних інформаційних операцій

Проблема планування спеціальних інформаційних операцій полягає передусім у визначенні впливів на індивідуальну та масову свідомість, а також систему суспільно-політичної комунікації і прогнозуванні їхніх наслідків для суспільства. Прогностична функція є однією з основних функцій сучасної, зокрема політичної, науки.

Методи прогнозування змінювалися протягом часу залежно від панівних парадигм світосприйняття, картин світу. Своєю чергою, вони значно впливали на розвиток світогляду, зокрема наукового, прискорюючи чи, навпаки, гальмуючи розвиток науки за умов панування певної наукової парадигми [173].

Ця теза стосується насамперед наук про суспільство та людину. Наприклад, швидкий розвиток американської політичної науки з середини XX ст. був значною мірою викликаний потребами «*холодної війни*» - першого в історії глобального протистояння. Попередник ЦРУ — Управління стратегічних служб, заснований Д. Рузвельтом, робило ставку на щонайширше залучення науковців до розвідувальної діяльності. Цю організацію інколи називали одночасно «клубом панів» та «науковим зібранням», величезні асигнування значно прискорили розвиток соціальних та політичних наук. Відомо, що саме Управління аналізу і оцінок ЦРУ, відповідні підрозділи Держдепартаменту, Пентагону й адміністрації президента стали поряд з академічним середовищем колискою сучасної американської політичної науки.

Наближеність подібних структур до центрів ухвалення рішень фактично робить прогнозування їхнім основним завданням. Саме прогностика є для загалу найзрозумілішою функцією науки. Як вважає, наприклад, С. Кримський, «область передбаченого не охоплює всі шари історії, наприклад, непе-

редбачуваним є все особистісне» [174]. Проте перебрання функцій оракула (думки Д. Белла та А. Грамші, науковців, що належать до марксистського напряму політичної науки, проте доволі різних його відгалужень, ще раз засвідчують вдалість цього порівняння) значною мірою визначило рівень суспільного авторитету політології.

З іншого боку, передбачення майбутнього тісно пов'язане з проблемами містики. В історії можна знайти багато прикладів, коли ця сфера людської діяльності негативно впливала на розвиток науки. Особливо це відбилося на суспільствознавчих науках, передусім на політичній науці. Разом з тим важко переоцінити і позитивний аспект взаємодії та взаємопроникнення наукового та містичного, особливо у політичній практиці.

Відомо, що відносини науковця та об'єкта дослідження становлять одну з найвизначніших проблем гуманітарних наук. Ще більшого значення вона набуває у сфері політичного прогнозування, що є невід'ємною функцією влади з усіма відповідними наслідками. «*Передбачення не може бути актом пізнання, бо каже про те, чого немає*». Водночас «передбачення — абстрактно виражене зусилля, що докладається як практичний спосіб створити колективну волю» [175].

З іншого боку, прогнозист, як і будь-який суспільно-політичний аналітик, виступає певним чином в якості драматурга. Він фактично формує дійсність, інтерпретуючи соціальні феномени і процеси. Саме у цьому знаходять пояснення прогнози, що самосправдовуються. Насамперед це стосується такого прогнозного методу, як написання сценаріїв.

Звертаючись до технології прогнозування, зауважимо, що управління має п'ять основних функцій [176].

1. ***Визначення цілей.***
2. ***Планування.***
3. ***Координація.***
4. ***Заохочування.***
5. ***Контроль.***

Виходячи з відомих кібернетичних положень, третя, четверта та п'ята функції відносяться до механізму зворотного зв'язку [177]. Проблема прогнозування постає на етапі визначення цілей та на етапі планування.

Визначення цілей, або визначення ідеалу, потребує узагальненої прогностики. Необхідно визначитися з кількома основними цільовими параметрами. Надмірна конкретизація може лише заважати моделі майбутнього. Зовсім інші вимоги висуває етап планування: від прогнозування вимагаються найконкретніші відповіді на порушені питання.

Спробуємо сформулювати кілька загальних вимог до процесу прогнозування. У викладі спиратимемося, зокрема, на праці українського аналітика А. Гуцала.

По-перше, принцип холізму, прогнозист має виходити з розуміння цілісності світу та його нерозривності, єдності. Навіть такі історичні злами як

революції не повністю змінюють перебіг процесів у системі. Як вже зазначалося, все нове завжди є результатом певного чудернацького поєднання елементів старого та радикально нового.

По-друге, треба зважати на існування принципу історичних аналогій. Він є одним з найпродуктивніших, але й найнебезпечніших для прогнозування. Хибні історичні аналогії дуже поширені.

По-третє, прогнозист має враховувати принцип нестабільності, або постійної зони біфуркації. Будь-який політичний процес є принципово нелінійним та, відповідно, нестабільним. Надзвичайно велика кількість ступенів свободи у поведінці людини, з одного боку, здається, унеможливлює жодне реальне прогнозування, а з іншого — за законом великих чисел багато флуктуацій компенсуються. Проте ця компенсація відбувається тільки на певному, досить високому, рівні розгляду. Політичний прогнозист завжди має виходити з усвідомлення реальної непередбачуваності поведінки людини (хоча б на одному з можливих рівнів її поведінки) та можливості прогнозувати діяльність тієї самої людини зі значною ймовірністю (на інших рівнях). Це зауваження, на думку автора, є принциповим, бо змушує постійно пам'ятати про ймовірнісність будь-яких реальних прогнозів.

Будь-яка конструкція, підґрунтям якої є певне твердження стосовно *людської природи, наприклад, що людей спонукають до дії їхні усвідомлені* інтереси (так вважає і марксизм, і лібералізм), являє собою комфортну для дослідника модель. Але не більше. Часто прогнозисти забувають про ті припущення, що є підґрунтям їхніх побудов. Подібна помилка призводить іноді до катастрофічних наслідків.

Найважливішою проблемою політичного прогнозування, на погляд автора, є проблема передбачення за нерегулярних умов, у транзитивних перехідних станах. Транзитивним перехідним станом суспільства вважатимемо такий стан, коли старі правила політичної поведінки вже недійсні для всього чи переважної більшості суспільства, а нові ще не сформувалися. Основною характеристикою такого стану є процеси кристалізації, вироблення правил гри. Такий підхід до визначення перехідного стану дозволяє викреслити зі списку подібних суспільств такі сталі системи, як, наприклад, радянська, незважаючи на її самовизначення як проміжної, перехідної (від капіталізму до комунізму).

Як вже зазначалося, прогнозування, зокрема політичне, вже досить давно стало об'єктом наукового дослідження. Розглянемо один з можливих підходів до технології прогнозування.

Політичне прогнозування тільки певною мірою є науковою діяльністю. Найчастіше прогнозист працює на замовлення. Це із самого початку позбавляє дослідника цілковитої об'єктивності з досліджуваного питання. Вказану тезу необхідно враховувати задля розуміння сутності процесу прогнозування, який здійснюється переважно з точки зору однієї зі сторін, залучених до конфлікту. Саме тому надзвичайної важливості набувають спроби формалізувати процес прогнозування.

Д. Мангейм і Р. Річ виділяють два основні типи політологічного аналізу: нормативний та емпіричний [178]. Якщо емпіричний аналіз апелює до фактів життя і є наслідком наукової революції XVII—XVIII ст., то нормативний, найперший тип гуманітарного наукового знання, ґрунтується на описах життя, рукописних текстах. Похідними з цих типів аналізу є відповідні типи прогнозів.

Кожен з типів прогнозів потребує для своєї реалізації застосування окремих методів, яких існує значна кількість. Е. Янч виділяє їх 150. З них найпоширенішими, на його думку, є такі: мозкова атака, метод Дельфи, екстраполяція, контекстуальне картографування, морфологічне дослідження, сценарний підхід, синоптична ітерація, економічний аналіз, використання теорії ігор, кількісні моделі, вертикальні й горизонтальні прийняття рішень, дослідження операції, дослідження рішень, мережеві методи, системний аналіз [179].

Серед цих методів для наших цілей найадекватнішими є методи моделювання. Під моделлю розуміємо чітко сформульоване та описане спрощене уявлення процесів, що відбуваються у реальності. Моделювання застосовується для вибору серед найважливіших, з точки зору дослідника, характеристик об'єкта дослідження та відкидання другорядних. Саме в сутності методу і полягає його основна вада — можливість нехтування певними чинниками перебігу подій. До методів цієї групи можна віднести: екстраполяцію — метод, що базується на теорії ігор; побудову кількісних моделей; сценарний підхід; синоптичну інтерацію; певні різновиди економічного аналізу. Окрему підгрупу становлять методи, пов'язані з математичним моделюванням. До переваг цієї групи методів можна віднести їхню формалізованість, певну можливість автоматизації тощо. Необхідно зауважити, що сфера наук про людину й суспільство вміщує спеціальні модельні методи, наприклад, метод історичних аналогій.

Проблема застосування методів моделювання, особливо математичного, в областях біфуркацій є надзвичайно складною. Сьогодні остаточно не розв'язано проблему розробки адекватного математичного та понятійного апарату. Звичайні моделі принципово лінійні, що обумовлює їхню непридатність застосування в областях нестабільності. Проте використання ідеї модельного підходу є, на погляд автора, плідним...

Необхідно звернути увагу на те, що сценарний підхід є, перефразуючи відомий вираз, певною мірою «сучасністю, продовженою у майбутнє». Значною мірою сценарій є засобом описання стабільних процесів. Проте неформальні можливості, що відкриває цей метод, дозволяють описувати й нестабільні ситуації. На думку дослідників, саме це робить побудову сценаріїв адекватним методом прогнозування за умов застосування синергетичної парадигми у політичній науці.

Як вважає фундатор дослідження нерівновісних систем І. Пригожин, «минуле не входить як складова у майбутнє [180]. Навіть у фізиці (як і в соціології) можна передбачити лише можливі сценарії», варіанти розвитку.

Сценарний підхід є надзвичайно цікавим ще й тому, що його функції не вичерпуються лише прогнозуванням подій. Як вважає Е. Янч, «сценарій не передбачає майбутнє, а формує його варіант» [179]. У цьому вислові міститься важлива передумова для ідеї прогнозів, що самосправдовуються. У термінах синергетики оприлюднений сценарій формує атрактор, а отже, жорстко впливає на майбутнє.

Відомий вислів «попереджений, отже, озброєний» є точним формулюванням цієї ідеї. Оголошення результатів прогнозу у формі політологічного прогнозу, часто формує віртуальну версію подій та змушує їх відбуватися в інший спосіб: цікаво порівняти з ідеями І. Пригожина та І. Стенгерс щодо штучної побудови атракторів. — Прим. О. Л.). З іншого боку сценарії є такими, що самореалізуються (порівняно з одним з фундаментальних принципів квантової механіки: спостерігач є рівноправним учасником подій, від самого факту наявності якого залежить їхній перебіг). Важливі матеріали з даного питання вміщені у статті Л. Гуцала та М. Ожевана [181].

Тут і далі розумітимемо під сценарієм систему передумов та нарис плану перебігу подій. У такому розумінні сценарій належить не до сфери прогнозування, а до політичного планування, де побудова у разі застосування певних методів впливу за наявності відповідних передумов дозволяє охопити політичну ситуацію загалом. З певними припущеннями сценарій можна розглядати варіантом політичного плану, а кажучи про кожний політичний план, «треба нагадати висловлювання Мольтке, який казав, що при складанні військових планів попередньо можуть бути вироблені тільки основна схема, загальний план, і не деталі, тому що їхнє здійснення залежить значною мірою від переміщень противника» [182]. З іншого боку, будь— який план може бути втілений у життя, реалізований лише за умов дотримання вимог принципу Б. Трентовського («не пливти наперекір стихії, а вміти використовувати її для своїх цілей») [183].

Загальні умови щодо розробки сценаріїв здійснення інформаційних впливів були такі.

1. Критерії вибору об'єкта здійснення впливу

Середньорозвинена постсоціалістична країна з великим прошарком інтелектуалів, перевиробництвом кваліфікованих кадрів, нині вже непотрібних для функціонування економіки, з відносно низьким рівнем життя, наявністю ефекту «культурного шоку» (див. далі).

Більш-менш чітке дотримання владою у країні загальноєвропейських стандартів прав людини (йдеться виключно про відсутність стороннього «заморожування» процесів, можливість існування непідконтрольних державі преси, політичних партій та об'єднань, свободу слова та зібрань). Слабка влада не є обов'язковою вимогою, швидше потрібна влада безпорадна, соціально інерційна, неспроможна належним чином відповісти на виклики майбутнього (детальніше остання вимога визначена у підручнику із сучасної політології та

геополітики, складеному під керівництвом Д. Корчинського. — Прим. О. Л.).

Відповідність обраним критеріям дозволяє характеризувати ситуацію у країні—об'єкті нападу як принципово нестабільну, траєкторії розвитку якої лише окреслені та припускають значну варіативність.

Перед викладенням сценарію спеціальної інформаційної операції проти нестабільних суспільств автор вважає за необхідне визначитися з дефініцією «політична стабільність» як такою.

Стабільність розглядається як несамостійний, похідний стан. Згідно з іншими, політична стабільність визначається як певне заперечення.

1. Стабільність як стан відсутності загрози нелегітимного суспільства (Ф. Білі, К. Даудинг, Р. Кімблер, Д. Яворські).
2. Стабільність як відсутність змін уряду (І. Циммерман).
3. Стабільність як відсутність змін у конституційному ладі (С. Хантингтон).
4. Стабільність як відсутність структурних змін (Д. Сіаринг).
5. Стабільність як стан балансу політичних сил (Дж. Лівелі).

Отже, нестабільність є результатом слабкості або неефективності певних компенсувальних механізмів.

Можна доповнити це визначення: нестабільність — зміна правил політичної гри, до якої політична система неспроможна адаптуватися.

Згідно з іншими підходами, нестабільність — це стан невизначеності траєкторії розвитку, можливість вибору напряму з кількох можливих. Інакше кажучи, нестабільність — суттєва характеристика зони біфуркації (!), фактична її сутність.

Вимоги до країни, яка здійснює інформаційну операцію. Високорозвинена в інформаційному плані держава, яка має у своєму розпорядженні сучасні спецслужби та інші відповідні інститути та ресурси, значний вплив у світових мас—медіа, фінансові ресурси в обсягах десятків—сотень мільйонів доларів. Спеціальні умови для запуску спеціальних інформаційних операцій за наведеними нижче сценаріями описано на початку кожного з конкретних їхніх описів.

1. *Сценарій впливу* на особу, яка ухвалює рішення. Об'єктом сценарію, що описується, має бути особа, бажано авторитарного складу, яка є не ритуальним, а справжнім лідером. Ця особа може особисто ухвалювати рішення та за кризових ситуацій звикла спиратися передусім на власні відчуття, а не на поради експертів.

Можна виділити чотири етапи операції за цим сценарієм: підготовчий, дестабілізувальний, формувальний, вихід з операції.

На першому, підготовчому, етапі необхідно створити політичний та психологічний портрет об'єкта, на якого спрямовуватиметься операція [184;185]. Виконати це завдання можна кількома способами, що докладно описано у відповідній літературі. На думку автора, на особливу увагу заслуговують методи дистанційного дослідження особистості, особливо метод створення психологічного портрета лідера на основі його промов [186]. Незважаючи на

зовнішню простоту технології, остання широко застосовувалася під час *«холодної війни»* та давала, за певними оцінками, непогані результати [187].

У колишньому Радянському Союзі на базі Інституту світової економіки і міжнародних відносин АН СРСР під проводом доктора політичних наук Є. Єгорової склалася школа створення психологічних портретів політичних лідерів. За розробками цієї школи, при створенні психологічного портрета лідера слід аналізувати інформацію за такими напрямами: Я-концепція, потрібнісно-мотиваційна сфера, система політичних переконань, стиль ухвалення політичних рішень, стиль міжособистісних стосунків, стійкість до стресу [188].

Другий етап мусить вивести об'єкта операції зі стану психологічної рівноваги, тобто викликати в об'єкта будь-які сильні емоції. Залежно від цілей кампанії та психологічних характеристик об'єкта впливу ними можуть бути гнів, роздратування, самозаспокоєність, неспокій тощо. Класичними методами на цьому етапі є використання дратівливих карикатур, наклепницьких статей та інших подібних матеріалів, їхньою особливістю має бути постійне звернення до однієї «больової точки», використання певної прихованої або відкритої вади, магії. Часто такого «точкою» є «царський комплекс», жага влади, відданість певним ідеалам, гіперболізована підозрілість, манія переслідування, сексуальні комплекси тощо.

Послабивши (а в ідеалі пригнітивши, вимкнувши) раціональну складову свідомості об'єкта впливу, на третьому етапі у свідомість реципієнта намагаються вкласти вже готові рішення, за допомогою витонченіших підходів — бачення, оцінки ситуації.

Завдання четвертого етапу — закріплення досягнутих результатів, поступовий вихід з операції. Залежно від психологічних характеристик об'єкта для закріплення можна використовувати великий спектр дій, починаючи з підхвалювання.

Зрозуміло, що наведена схема є ідеальною. Черговість та чіткі межі етапів можуть змінюватися, можливе також раціональне вирішення завдань різних етапів. Наприклад, другий і третій етапи здебільшого поєднуються: на етапі *«роздратування»* пропонуються способи виходу, подолання криз.

2. *Сценарії впливу* на великі маси людей за умов дестабілізаційної обстановки. Ці сценарії можуть використовуватися, наприклад, під час страйків, кампаній непокори тощо. Автор вважає: за доцільне класифікувати їх як «провокувальні». Умови для здійснення подібних сценаріїв такі:

- дестабілізована ситуація, наявність значних груп людей, які висувають будь-які вимоги до центральної влади, від суто економічних до політичних (група «протестуючі»);
- Вжиття режимом жорстких заходів, аж до пролиття крові. Якщо влада наважується на це — перша кров «руйнує» спеціальну операцію. Людська кров і карнавал несумісні. Або те, або інше. У цьому разі дося-

гається тактична перемога, проте стратегічно «гра» поступово програється. Ще М. Некрасов писав: «*Умрешь недаром — дело прочно, когда под ним струится кровь*».

- Влада не помічає мітинги. Ігнорує виступи опозиції, бере участь у карнавалі не в ролі страховиська, а як рівноправний учасник. Це найкраща стратегія, проте, практично нездійсненна. За сучасних умов влада має бути обов'язково міжнародно визнаною. Фактично вона виступає не як самостійна й самодостатня структура, а як місцевий представник вищої інстанції.

Зауважимо, що це цілком логічно випливає з описаного у попередньому розділі процесу формування глобальної системи гегемонії.

Технічно операція складається з чотирьох обов'язкових й одного додаткового етапів.

Перший (підготовчий) етап операції є, точніше, може бути латентним (прихованим). На ньому виявляється чи створюється сервільна («кишенькова») опозиція («п'ята колона»). Бажано, але зовсім необов'язково, залучення до її лав одного—двох діячів загальнонаціонального масштабу. Необхідний час — близько 2—3 місяців.

Зрозуміло, що за наявності певних коштів та за умов дії системи стратегічного планування на основі стабільних національних інтересів діяльність щодо формування «п'ятої колони» у різних країнах світу не переривається жодної миті. Одним з найпоширеніших методів є відбір представників національної еліти, що нестандартно мислять, вибір з них відповідним чином налаштованих та штучну роботу з кожним за допомогою різноманітних фондів розвитку, освітніх програм, інформаційних центрів, систем зовнішньополітичної пропаганди. Відомо, що подібні потужні системи існують та існували у багатьох розвинених країнах світу, таких, як США (...), Німеччина (Гете—інститут), Великобританія (British Council), колишній СРСР (АПН, спілки дружби з СРСР тощо). Дослідження та регулювання цієї діяльності є одним з найважливіших завдань держави у сфері забезпечення безпеки, провідним напрямом діяльності спецслужб.

Наведене вище жодним чином не може розцінюватися як заклики до боротьби з іноземним впливом за радянськими зразками.

Навпаки, необхідно всіляко сприяти щонайширшому культурному, науковому тощо співробітництву. Відмова від нього призводить, окрім зрозумілих наслідків ізольованості країни, до втрати імунітету до впливів, але знати про наявність потенційної загрози необхідно. Необхідно зауважити, що проблеми інфільтрації, молекулярного впливу, змішування в умовах сучасного нестабільного постсоціалістичного суспільства потребують окремого ретельного дослідження. Зрозуміло, що створення «п'ятої колони», яке відбувається за мирних часів, не потребує жодних важливих рішень на рівні політичного керівництва країни і є звичайною діяльністю розвідувальних служб.

Перехід до другого етапу спеціальної інформаційної операції вже передбачає ухвалення відповідального рішення на рівні вищого політичного керівництва країни.

Другий етап: нагнітання та «розкручування». Він характеризується напів'явними діями, спрямованими на інформаційне «розкручування» опозиції під гаслами на кшталт «режим веде державу до катастрофи». Необхідно використовувати мінімум два—три загальнонаціональних видання та одну—дві популярні радіостанції 1-М—діапазону, що діють у столиці. Бажано використовувати ще й телеканал. Створення безпосередньо під вирішення цього завдання подібних видань та радіостанцій можливо, але оптимальним є використання вже «розкручених», відомих. Важливою умовою діяльності на цьому етапі є поява кількох повідомлень в авторитетних світових ЗМІ. Пропаганда опозиції орієнтується саме на столицю, конкретно — на столичну молодь, зокрема, студентів.

Важливим завданням, якщо воно не повністю вирішено на першому, латентному, етапі, є створення у столиці політичної інфраструктури, здатної організувати демонстрації молоді, студентів. У разі наявності цієї інфраструктури необхідно її удосконалити, пристосувати до дій у кризових ситуаціях, режимі воєнного часу. Одним з важливих напрямів формування інфраструктури є створення, а точніше — активізація вже існуючих осередків в університетах та інших найбільших вищих навчальних закладах. Підґрунтям цих осередків можуть бути як політичні групи (осередки опозиційних політичних партій, їхні молодіжні організації), так і різні неполітичні організації на кшталт профспілок, клубів за інтересами, навіть релігійних спільнот певного спрямування. Мінімальний термін реалізації завдань цього стану — близько 2—3 місяців.

Третій етап передбачає дестабілізацію суспільно— економічного життя в столиці. Можливий спосіб: організація несанкціонованої емісії великих обсягів національної валюти з виведенням їх на валютну біржу (ефект від падіння національної валюти на десятки відсотків за один день), масові крадіжки грошей (зокрема, це можливо зробити, практично не втрачаючи коштів, через проникнення крізь захист системи електронних розрахунків; технічні подробиці залежать від конкретних характеристик системи). Досягнення дестабілізації можливо і традиційнішими засобами.

Наприклад: терористичний акт проти популярного діяча; терористичний акт зі значною кількістю жертв; штучне створення перебоїв з постачанням продовольства найширшого вжитку (хліб, молоко тощо).

Як відомо, *«революції здійснюють не хронічно голодні а ті, кому два дні не дали хліба»* [189]. Масована інформаційна операція, що розглядається, в жодному разі не є соціальною революцією, проте вона має з останньою багато спільних рис.

Термін: дестабілізація за 1—2 дні, причому підготовчий період (час, потрібний на знешкодження систем захисту, створення умов для здійснення

теракту, підготовку блокування транспортних, телекомунікаційних мереж) триває близько 6 місяців.

Четвертий етап: «оксамитова революція». Характеризується організацією в столиці масових демонстрацій опозиції. Необхідним є виведення на ці демонстрації великих мас молоді. Демонстранти мають певний час контролювати центр столиці. Характер мітингів має бути не страшний, грізний, а м'який, неначе карнавальний. Ворог не хтось конкретний, а абстрактна Страшна Влада. Влада, виводячи війська й поліцію на вулиці, тільки підігрує демонстрантам: «Проти кого спрямовані війська — проти наших дітей?»

Цим подіям необхідно надати потужного пропагандистського звучання у міжнародній та місцевій, підконтрольній опозиції, пресі. Акцепт у пропаганді слід робити на принципово ненасильницький підхід опозиції. Доцільним є використання таких гасел, як «боротьба свободи проти рабства», «прогрес проти відсталості» тощо. Цілком виправдане масоване використання відповідної символіки. Важливим завданням міжнародної пропагандистської кампанії є створення образу влади як збіговиська ретроградів, корупціонерів, злочинців (злочином має стати сама служба ворогам прогресу, демократії, свободи, нації, тобто старій владі). Реалізація цього завдання дозволяє нейтралізувати раціональні міркування під час аналізу ситуації і перевести обговорення в речище боротьби Абсолютів (Добра зі Злом).

На певному етапі перебігу подій за допомогою ЗМІ слід довести необхідність інтернаціоналізації конфлікту. Сприйнятливим сценарієм є забезпечення посередництва міжнародних організацій. Обов'язковою умовою посередництва має стати обіцянка проведення вільних дострокових виборів під міжнародним контролем. Досягненням відповідних поступок з боку влади четвертий етап закінчується.

Можна говорити про певні варіації у перебігу подій. У разі повного успіху операції й деморалізації владних структур завершенням четвертого етапу може стати передача влади до рук опозиції та формування з її лав тимчасового уряду. Тоді результат досягнено вже на цьому етапі. В іншому разі слід додати ще певних зусиль для досягнення необхідного результату на виборах.

Розгляд проблеми застосування сучасних комунікаційних технологій для здобуття опозицією перемоги не є метою роботи. Проте перемога керованої опозиції при правильному застосуванні наявних інформаційних потужностей практично гарантована. Результатом здійснення подібного сценарію має стати повна чи часткова зміна урядового курсу. Інакше кажучи, досягнення певних цілей.

Реальність та застосовуваність наведеного вище сценарію зайвий раз довели жовтневі, 2000 р., події у Югославії. Результатом чіткої роботи американських спецслужб стало повалення режиму С. Мілошевича та приведення до влади В. Коштуніци — політика з проамериканськими поглядами. Окрім великої кількості непрямих ознак (значна скоординованість дій до того воро-

гуючої опозиції, значні фінансові та інтелектуальні ресурси, задіяні у конфлікті, високий професіоналізм здійснення пропагандистських кампаній тощо), про організований характер «народної югославської революції» свідчать матеріали світової, зокрема американської, преси. Дуже показовим є матеріал М. Добса «Американські поради та управління опозицією Мілошевичу» [190]. У цій статті відверто і до найменших подробиць розкриваються механізми американського втручання у перебіг соціально—політичних процесів у Союзній Республіці Югославія протягом 2000 р.

Останні події свідчать про удосконалення й розробку нових сценаріїв. Зокрема, можна говорити про значну увагу до проблем «палацових переворотів», потрясінь виключно верхів елітного характеру. Проте ця тема є надзвичайно складною і потребує на окреме ретельне дослідження.

Цілком зрозуміло, можна казати про певну умовність та обмеженість наведеного сценарію, тим більше, що це дослідження не може вичерпати усі аспекти проблем спеціальних інформаційних операцій, але тут розглянуто один з можливих підходів до ведення масованих інформаційних операцій стратегічного характеру.

Отже, можна дійти таких висновків.

1. Будь-які спеціальні інформаційні операції можна розділити на два типи: ті, що спрямовані на підрив діючої гегемонії та ті, що спрямовані на витіснення певної особи (групи осіб) панівного прошарку.
2. За мирних часів застосовуються спеціальні інформаційні операції, серед яких можна виділити операції, спрямовані на здійснення впливу на суб'єктів ухвалення рішень, на дестабілізацію соціально—політичної ситуації та на компрометацію політичних чи суспільних діячів.

Доцільно розглядати єдину схему здійснення спеціальних інформаційних операцій, що складається з чотирьох етапів: підготовчого, створення інформаційного приводу, «розкрутки», закріплення результатів та виходу зі спеціальної інформаційної операції.

Одним з нових підходів до здійснення спеціальних інформаційних операцій стратегічного характеру є спроба моделювання значних історичних подій. Зокрема, задля дестабілізації певної суспільно-політичної ситуації та зміни влади можна використовувати відому модель карнавальної комунікації за М. Бахтіним

1.6. "Pax Americana" чи "Pax Sinica": глобальний інформаційний виклик Пекіна й відповідь Вашингтона

У сучасній міжнародній системі Китайська Народна Республіка (КНР) перетворилася в настільки потужний центр сили, що з ним не можна не рахуватися. В державах, які нині визначають магістральні напрямки світової політики, жоден діяч, що розробляє чи реалізує проекти у сфері безпеки регіонального й глобального значення, не може ігнорувати китайський фак-

тор. Не випадково у „*Стратегії національної безпеки США*" від 17 вересня 2002 р. КНР віднесена до потенційно великої держави – „недемократичної", але з ринковою економікою, за котрою визнається безперечне право володіти й удосконалювати ракетно-ядерні військові технології [191].

Контури світу, в котрому Китай відіграватиме роль геополітичного й геостратегічного полюса, поки що складно окреслити, але він поступово формується, незалежно від бажання тих чи інших міжнародних акторів. Боротьба Пекіна за планетарне лідерство почалася не вчора, хоча самі китайські лідери про це відкрито не говорять, натомість пропагуючи тезу про багатополярність світу як більш продуктивний і стабільний устрій. Її офіційно підтримує Росія, що як держава-продовжувач СРСР (з міжнародно-правового погляду) ще в недавньому минулому мала статус наддержави, а тому досить незатишно почуває себе нині на другорядних ролях у світовій політиці. Чимало прихильників багатополярності (з присмаком антиамериканізму чи під привабливою вивіскою „багатовекторності") є і в нашій країні.

Але якщо виходити з реалій сьогодення, то слід визнати, що нині є лише одна наддержава – США, котра збереже цей статус, щонайменше, до середини століття, коли КНР досягне з ними паритету не лише за економічним потенціалом, а й наблизиться до жаданого балансу у військовій сфері. Цю тезу можна було б аргументувати низкою фактів із будь-якого поля міжнародної політики, на неї „працює" й теорія довгих циклів, запропонована американськими економістами Дж.Модельським і В.Томпсоном.

Згідно з нею, кожні півтисячі років відбувається періодична зміна історичного глобального процесу, у рамках цього відрізку часу так само періодично кожні 120 років змінюються фази політичного циклу. Окремі теоретики, наприклад, Т.Босуелл, додають до них ще „*хвилі*" М.Кондратьєва (60-річні великі цикли кон'юнктури), щоб урахувати динаміку зміни економічних процесів. На підставі аналізу всіх зазначених фаз та циклів і прогнозуються держави-гегемони на той чи інший період.

Відповідно до теорії довгих циклів, із завершенням Другої світової війни на статус глобального політичного лідера стали претендувати США, котрим кинув виклик СРСР. Унаслідок багатьох причин (вашингтонські теоретики головним чином вказують на „морську державність" США) Кремль програв боротьбу за світову гегемонію, тому США в якості одноосібного лідера чи гегемона доживуть якраз до середини XXI ст. У той же час, згідно зазначеної теорії, на початку нинішнього віку має з'явитися новий суб'єкт світової політики, котрий через півстоліття поставить під сумнів гегемонію США. Подібна перспектива, звісно, не радує американських футурологів, і значна їх частина переконує, що замість нового гегемона з'явиться щось на кшталт „світового уряду", який і буде вирішувати глобальні проблеми на засадах справедливості.

Але вся зафіксована в писемних джерелах історія людства просякнута гострою боротьбою за світову гегемонію, досить згадати драматичну історію виникнення, розвитку й краху Ассирії, Давнього Риму, імперій Ахеменідів,

Александра Македонського, Чингіз-хана, Тамерлана, Османів, Габсбургів, Романових і Наполеона Бонапарта. Навряд чи XXI століття виявиться мудрішим від попередніх століть, незважаючи на всілякі революції в області знань, інформації й технологій, боротьба за світове домінування продовжуватиметься й надалі, але вона не призведе до формування багатополярної структури у вигляді державних центрів, приміром, США, КНР, Японії, Індії, Німеччини (Євросоюзу) й Росії.

Причина проста: для того, щоб посісти місце „світового полюса" потрібно володіти потенціалом наддержави, тобто такими економічними можливостями, військовою силою й політико-дипломатичним впливом, щоб усі ці складові одночасно відчувалися міжнародним середовищем у будь-якому куточку земної кулі. Потенційно в середньостроковій перспективі зазначених якостей може набути і, з огляду на чимало факторів, стати такою наддержавою найбільші шанси має саме Китай, географічно розташований посередині Східної Азії.

Як відомо, у вересні 1982 р. на XII з'їзді Компартії Китаю була спланована стратегія модернізації країни до 2049 р. (столітнього ювілею КПК), коли КНР має перетворитися на сучасну високорозвинену державу з життєвим рівнем населення вище від середньозаможного (ідеальне суспільство *„сяокан"*), що за часовими рамками відповідає ***„хвилям"*** М.Кондратьєва. Для подібних прогнозів є солідні підстави, передусім, динаміка економічного розвитку КНР. Незважаючи на спричинений боротьбою із SARS спад у сфері авіаперевезень, туризму і готельного бізнесу, промисловість Китаю отримала потужний стимул для розвитку: за підсумками 2005 р. ВВП КНР (за паритетом купівельної спроможності) склав $ 8,883 трлн. і збільшився, порівняно з попереднім роком, на 10,2 %, в тому числі промислове виробництво виросло на 29,5 %, експорт сягнув $ 752,2 млрд., що дало змогу накопичити $ 825,6 млрд. золотовалютного резерву [192].

Починаючи з 3-го пленуму ЦК КПК 11-го скликання в грудні 1978 р., коли з ініціативи Ден Сяопіна було ухвалено офіційне рішення щодо проведення широкомасштабної економічної реформи, протягом майже трьох десятиліть щорічні темпи приросту ВВП в КНР не опускалися нижче 8 %. За прогнозами фахівця з порівняльної економіки А.Меддісона, навіть при зменшенні цього показника до 5,5 % ВВП КНР сягне рівня США у 2015 р. Це означає, що коли на зорі реформ, у 1978 р., ВВП Китаю становив 5 % від світового ВВП, у 1998 р. – 10 %, у 2005 р. – більше 13 %, то до 2015 р. він сягне 17 % світового ВВП.

Якщо ж до цього додати сукупний економічний потенціал китайської діаспори (хуацяо) у Південно-Східній Азії, що налаштована виключно патріотично й активно допомагає історичній батьківщині не словом, а ділом, можна передбачити, що загальна сукупна китайська частка у світовому ВВП дорівнюватиме 23-25 % (сучасний показник США). На думку американських аналітиків Р.Бернстайна і Р.Манро, у 2020 р. (саме тоді, за визначенням Цзян

Цземіня на XVI з'їзді КПК у листопаді 2002 р., в країні має бути побудоване суспільство середнього достатку) ВНП Китаю становитиме $ 20 трлн. і залишить на другому місці США із $ 13,5 трлн. [193].

У будь-якому випадку КНР на наших очах перетворюється на повноправного учасника геостратегічної гри в масштабах, адекватних значимості США, а геополітичне протистояння Пекіна й Вашингтона перетворюється у визначальний фактор світової політики. Початок йому, сам того не бажаючи, поклав на початку 70-х рр. минулого століття президент США Р.Ніксон. Скориставшись різким погіршенням відносин між Москвою й Пекіном, він спробував приручити комуністичний Китай і зробити його спільником США у протидії радянському впливові в Азії й *„третьому світі"* загалом. Кремлівська пропаганда влучно назвала це *„розіграти китайську карту"*.

Але Пекін, прикриваючись жвавою антирадянською риторикою, використав нормалізацію відносин із багатою Америкою для подолання успадкованої від часів *„культурної революції"* дипломатичної ізоляції, зміцнення свого міжнародного впливу і підйому економіки. Коли ж у приморських провінціях КНР почалося створення спеціальних економічних зон, до котрих потекли багатомільярдні іноземні інвестиції, автор ідеї антирадянського американо-китайського союзу, тогочасний державний секретар Г.Кіссінджер, прозрів і виступив із запізнілим попередженням: *„Як тільки Китай стане достатньо сильним, він може виступити проти нас"*.

Патріарх американської дипломатії як у воду дивився, хоча у відносинах із сусідніми азійськими державами протягом останніх десятиліть КНР не давала приводу для звинувачень у прагненні до регіональної гегемонії, вирішуючи всі спірні територіальні питання за столом переговорів. Інша справа — США, котрі у стратегічному союзі з Японією, Південною Кореєю й Тайванем поки що мають абсолютну військову перевагу в АТР, ця ж обставина зумовлює застосування Пекіном у наступі на Вашингтон виключно інформаційних і економічних засобів.

Ще у середині 80-х рр. минулого століття у надрах китайських спецслужб була розроблена стратегічна концепція добування фінансових ресурсів і передових технологій за допомогою методів інформаційної війни. Власне, сам термін *„інформаційна війна"* в сучасному сенсі — як дії, спрямовані на досягнення інформаційної переваги в інтересах національної стратегії шляхом впливу на інформаційні системи супротивника за одночасного захисту власних, чи не вперше був впроваджений у 1985 р. саме китайським теоретиком-політологом Шень Вейгуаном.

Творчо опрацювавши *„інформаційну концепцію"* начальника Генерального штабу Збройних сил СРСР у 1977-1984 рр. Миколи Огаркова, китайці спробували вирішити одночасно два завдання — спланувати заходи щодо захоплення глобального інформаційного простору і створити захисний інформаційний кордон держави — своєрідну *„Велику китайську стіну"* в п'ятому вимірі. Структурно китайський підхід полягав у:

- мирному залякуванні супротивника;
- протистоянні інформаційних потенціалів;
- конкуренції інформаційних стратегій;
- підвищенні інформатизації військ (штучний інтелект);
- економічній інформаційній агресії;
- *культурній інформаційній агресії*;
- інформаційній війні мізків.

Ця програма сподобалася архітекторові модернізаційних реформ Ден Сяопіну, котрий виявився стратегічним аналітиком глобального рівня й прийняв рішення щодо пріоритетного фінансування спецслужб і активного використання методів інформаційної війни для досягнення економічного процвітання. З того часу в КНР була створена могутня державна система ведення інформаційного протиборства зі США, що дозволяє здійснювати масоване застосування сил і засобів у потрібний час. Її осередком є Дослідне бюро при Держраді КНР і Системно-аналітичний центр міністерства держбезпеки.

Найефективніше китайська система інформаційного протиборства діє у фінансовій сфері, а необхідними матеріалами її забезпечують азійсько-тихоокеанська діаспора (хуацяо) й розвідка. З Пекіна здійснюється тотальний контроль над ЗМІ країн АТР, значна кількість газет, теле- і радіоканалів придбана агентами і офіцерами розвідки КНР, через підконтрольні ЗМІ проводяться активні комплексні інформаційно-психологічні операції. Феноменальним успіхом китайських спе́цслужб є встановлення контролю над найбільшими банками Східної Азії, передусім у Малайзії й Сінгапурі. Лише в Індонезії трохи більше 4 млн. хуацяо й досі контролюють 3/4 приватного бізнесу країни.

Розвідка КНР має настільки сильні позиції серед майже 20-мільйонної китайської діаспори США (основна її частина зосереджена на Тихоокеанському узбережжі), що американські спецслужби не в змозі повністю контролювати її активність у таких містах як Сіетл, Лос-Анджелес, Сан-Франциско, Х'юстон. Своєрідним попередженням Білому Дому стало обрання у 1996 і 2000 рр. етнічного китайця Ло Цзяхуея (Гарі Лока) губернатором штату Вашингтон (столиця штату - Сіетл є головними воротями китайської еміграції в Америку). Не виключено, що масові безпорядки в цьому місті під час проведення форуму Світової торговельної організації наприкінці 1999 р. були інспіровані китайськими спецслужбами.

Першу велику перемогу в інформаційній війні проти США Пекін одержав у червні 1989 після кривавого придушення опозиційних виступів на площі Тяньаньмень, коли через ЗМІ до пересічного громадянина була доведена інформація, що у Пекіні, Шанхаї й деяких інших великих містах діяли невеликі групи екстремістів та кримінальних злочинців. Більш того, китайські лідери переконали народ у тому, що безпорядки були інспіровані США, тому сучасна молодь, яка пізнала смак плодів економічного процвітання КНР 90-х рр. XX ст., погодилася, зрештою, підтримати гасло правлячого режиму: *„Не потрібно більше ніяких політичних реформ"*.

Через численні ЗМІ (щороку в КНР видається більше 2 млрд. журналів, 20 млрд. газет, функціонує 3240 теле- і 1,5 тис. радіостанцій) всіляко стимулюється ріст патріотизму, спрямованого проти стратегічного супротивника — США, який іменується головною перешкодою на шляху втілення історичної мрії китайців стати світової наддержавою. Населенню нагадується про всі приниження, яких зазнав Китай від Заходу за останні півтора століття, і закликається безумовно підтримати владу. Будь-яка стурбованість США дотриманням прав людини подається як *„імперіалістична інтервенція"* й спроба не дозволити Китаю стати ще сильнішим.

Для покарання представників ліберальної інтелігенції, що критикують, приміром, корупцію у владних ешелонах, все частіше використовується звинувачення у шпигунстві на користь США. Під час Косовської кризи 1998-1999 рр. китайським ЗМІ було наказано захищати репресивну політику С.Мілошевича і не повідомляти про нього жодного негативу, гуманітарна ж інтервенція НАТО була названа *„військовим вторгненням"*.

Пекіну вдалося повністю „переграти" американців у ході інформаційного протиборства під час азійської фінансово-економічної кризи 1997-1998 рр., представивши КНР в якості стабілізуючого фактора в АТР. А у травні 1999 р. міністри оборони КНР і Куби підписали угоду про створення на „Острові Свободи" китайського центру радіоперехоплення і стеження за супутниками США, аналогічного тому, що мала Росія в м. Лурдес до січня 2002 р.

1 квітня 2001 р. розпочався другий етап американо-китайської інформаційної війни за владу в фінансовому світі, коли досить несподівано для американців банальна авіаційна пригода над Південно-Китайським морем перетворилася у гострий інформаційний геополітичний конфлікт. Тоді внаслідок спроби китайських винищувачів витиснути розвідувальний літак ВМС США ЕР-3В за межі виняткової економічної зони КНР сталося зіткнення, внаслідок якого один винищувач упав у море, а американський літак змушений був здійснити посадку на о. Хайнань, що належить КНР.

В Інтернеті спалахнула справжня битва між американськими й китайськими хакерами, причому почали її американці, які ламали китайські сайти, залишаючи в них образи на адресу КНР і, зокрема, пілота Ван Вея, що загинув. У відповідь китайське неформальне об'єднання Honker Union оголосило про початок відплатних дій — стався масовий злам американських сайтів, у тому числі й урядових, так, сайт уряду США зазнавав безперервної атаки протягом 6 годин. Після того як у Honker Union нарахували тисячу зіпсованих американських веб-вузлів, його члени поширили повідомлення, що вважають свою мету досягнутою.

За даними ВВС, за 11 днів активного протистояння між КНР і США китайські *„кібернаціоналісти"* *„наїхали"* як мінімум на 9 американських урядових і комерційних сайтів. Зокрема, протягом тижня відвідувачі сайту пенсільванської компанії *„Intelligent Direct"* замість реклами карт, які нею виготовляються, змушені були милуватися червоним китайським державним

прапором і заявами на кшталт: *„У Китаю також є атомна бомба"*. Американські експерти наголошували, що китайські хакери поралися у віртуальному світі з 1998 р., руйнуючи мережні сайти й запускаючи віруси в комп'ютерні системи. Причому, на відміну від російських чи філіппінських хакерів, вони керуються не меркантильними міркуваннями, а політичними.

Дж. Буш-молодший відрядив до о.Хайнань три есмінці оперативного флоту США й у різкій формі засудив китайців за те, що вони зволікають із дозволом американським представникам зустрітися з 24-ма членами екіпажу, оскільки це, на його думку, суперечило дипломатичній практиці. Щоб розрядити обстановку, офіційний Пекін дозволив зустріч (після чого есмінці були відкликані), але відпустив американських льотчиків на батьківщину лише після того, як 11 квітня 2001 р. отримав офіційного листа уряду США, в котрому висловлювався жаль з приводу інциденту.

Та оскільки жодна зі сторін не визнала себе відповідальною, конфлікт залишався неврегульованим іще півтора місяця, на консультаціях щодо подальшої долі літака-розвідника, оголошеного Пекіном військовим трофеєм, китайська сторона висунула вимогу до США взагалі відмовитися від польотів розвідувальних літаків уздовж узбережжя КНР. Лише 24 травня, задовольнившись вибаченнями американських урядовців, китайський уряд погодився з пропозицією Вашингтона розрізати літак і переправити його у США на вантажному судні.

Таким чином, принаймні частково, Пекіну вдалося примусити Вашингтон до того, чого не зміг добитися М.Хрущов від Д.Ейзенхауера сорока роками раніше, - до офіційного вибачення за порушення повітряного простору іншої держави, і то навіть не в глибині її території, як це було 1 травня 1960 р. з У-2, а над водами виключної економічної зони.

Тверезо враховуючи гіркий досвід СРСР 70-80-х рр. минулого століття, китайське керівництво добре усвідомлює, що попри вражаючі економічні успіхи, КНР не зможе витримати тривалу гонку озброєнь із США. Проте було б помилкою вважати, що Пекін зоставатиметься глухим до розгортання протиракетної парасольки над США після їхнього виходу в 2002 р. із радянсько-американського Договору про обмеження систем ПРО 1972 р. Беручи до уваги наявні ресурси, китайське керівництво прагне діяти вибірково, щоб зайняти якомога вигідніші позиції у нових політичних умовах. Ця вибірковість має два очевидні напрямки:

- консолідація всього того, що дозволяє країні утримувати домінуюче континентальне становище;
- підготовка до асиметричного ведення війни.

Пекін зупинився на пріоритетному розвиткові технологій, пов'язаних із ракетно-космічною технікою. Вони дозволять КНР, незважаючи на його помітне відставання від США в галузі звичайних і стратегічних озброєнь, створити потенціал, за допомогою котрого Китай буде в змозі завдавати удари по больовим точкам супротивника — системам інформації й комунікацій,

супутникам, платформам для „Стелсів" і авіаносцям. Така стратегія означає кардинальну зміну в китайській геополітичній думці – перенесення уваги з потенційного материкового ворога (Росія, Індія) на морського (США, Японія).

Згідно з повідомленнями гонконгської преси, у Пекіні вже розроблена система озброєння під назвою "Зірка-паразит", яка здатна стикуватися із ворожими супутниками, перешкоджати їхній роботі або знищувати. А за оцінками Інституту дослідження національної стратегії США, на замовлення Народно-визвольної армії Китаю (НВАК) ведеться розроблення супутникової системи, призначеної для передачі інформації про супротивника всім формуванням Збройних сил включно до підрозділу, що виконує те чи інше бойове завдання, одночасно і у реальному масштабі часу [194].

Пекін успішно реалізує концепцію Мережних сил – військових підрозділів до батальйону включно в складі висококваліфікованих комп'ютерних експертів, навчених у державних вузах. Головний акцент робиться на залученні активної молоді, передусім із числа користувачів Інтернету, за кількістю яких (123 млн.) КНР міцно утримує друге місце у світі після США. Вже проведено кілька масштабних навчань Мережних сил з відпрацювання концепції інформаційної війни.

За іронією долі, у грудні 2000 р. серйозного поштовху розвиткові китайської ракетно-космічної промисловості надало рішення Вашингтона про припинення санкцій, запроваджених у зв'язку з підозрами щодо передачі Пекіном ракетних технологій Ірану та Пакистану. Відразу ж після цього американські компанії стали активно співпрацювати з КНР у галузі комерційних космічних програм, унаслідок чого китайський Інститут космічної техніки запланував на 2001-2005 рр. вивести на орбіту не менше 30-ти власних супутників [195]. Навіть в умовах чинності санкцій США, у листопаді 1999 – січні 2001 рр. Пекіну вдалося запустити в космос два безпілотних космічних апарати „Корабель богів", а невдовзі після їхнього скасування - в жовтні 2003 і жовтні 2005 рр. – пілотовані космічні кораблі „Шеньчжоу („*Небесний човен*") – 5" і „Шеньчжоу – 6".

Місцем розгортання нової космічної програми КНР ще навесні 1999 р. був обраний о.Хайнань, котрий не випадково так „уподобали" американські літаки-розвідники. Він розташований неподалік екватора, що полегшує запуск ракетносіїв, із очікуваним завершенням будівництва основного космодрому біля м. Венчанг значно зменшиться ризик падіння ракет на густонаселену територію країни, оскільки вони пролітатимуть над океаном. Крім того, на острові знаходяться два великі центри радіо- та радіотехнічної розвідки НВАК, що відстежують усі радіосигнали над Південно-Китайським морем, а також перехоплюють повідомлення з американських і російських супутників зв'язку.

Незважаючи на урядову пацифістсько-ізоляціоністську риторику Пекіна („не претендувати на гегемонію", „виступати проти політики сили", „не втручатися у внутрішні справи інших країн"), що лунала під час офіційних

візитів Дж. Буша-молодшого до Пекіна 21-22 лютого 2002 р. і Ху Цзіньтао (тоді ще віце-президента КНР) до США 1-2 травня того ж року, в реальності КНР виявилася втягнутою в глобальну *„шахову гру"* від Перської затоки до Корейського півострова.

Виступаючи перед слухачами Національного військового коледжу США, начальник пекінської Академії військових наук генерал Лі Цзицзюнь наголосив, що сучасна концепція *„активної оборони"* КНР „включає стратегію обмеженої, високотехнічної війни із слабкими сусідами на китайській периферії, особливо на узбережній периферії. Інтегральною частиною цієї стратегії є встановлення оборонної зони навколо серця Китаю — ланцюга островів і периметра, що тягнеться від островів Спратлі, через Тайвань і острови Сенкаку й закінчується на півночі Кореї" [196]. Зрозуміло, що така постановка питання означає неминуче зіткнення (хоча і необов'язково військове) зі США.

Тайвань — поки що єдина точка на карті світу, де китайські й американські геополітичні та національні інтереси прямо суперечать одні одним. Безперечно, острів стане для континентального Китаю тією *„Малою землею"*, відстоявши котру він зможе розраховувати на своє відродження. Приєднавши Тайвань, Пекін, окрім капіталів, отримає розумні мізки (у КНР їх не вистачає, даються взнаки наслідки *„культурної революції"*) і передові технології, які йому ніколи не надасть Захід, це дозволить кардинально скоротити військово-технологічне відставання від США. По-друге, возз'єднання Тайваню з КНР спричинить стрімке зростання національної самосвідомості всіх китайців, у тому числі хуацяо, що суттєво наблизить реалізацію мрії всіх чотирьох поколінь керівників КНР про створення „Великого Китаю". До того ж встановлення контролю над Тайванем є необхідною умовою для перетворення КНР у велику морську державу, її військово-морський флот отримає вихід у Тихий океан і стане менш вразливим для американців.

„Взяття Тайваню, до яких би руйнувань на острові воно не призвело, краще, ніж його втрата", - стверджує китайський письменник Цзуо Ган, але його оптимізм не поділяють пекінські військові. За їхніми оцінками, для окупації Тайваню КНР доведеться задіяти 400-тисячну армію, а після війни витратити мільярди доларів для відновлення зруйнованої економіки острова і південних приморських (найрозвиненіших) районів материкового Китаю. В економічному відношенні це відкине КНР на десятиліття назад, але найбільш небезпечним є велика ймовірність втягування у конфлікт США і Японії.

Тому в Пекіні сподіваються, що возз'єднання Тайваню з материком відбудеться мирним шляхом, якщо, звичайно, тайваньці самі не спровокують конфлікт, наприклад, негайним проголошенням незалежності. У цьому випадку КНР не залишиться іншого вибору, крім як почати війну, оскільки дотримання ідеї національної єдності стало в країні непорушним принципом. Пекін недвозначно дав зрозуміти, що він готовий застосувати відносно Тайваню, котрий не бажає визнати КНР, військову силу, незалежно від того, якою великою буде ціна такого кроку. Голова Народної Політичної Консультативної

Ради КНР Лі Жуйхуань якось навіть заявив: "*Краще втратити 1000 солдат, ніж позбутися хоча б однієї п'яді своєї землі*" [196].

Треба віддати належне прагматизму керівництва Демократичної прогресивної партії Тайваню (виражає інтереси корінного населення острова, що в основній масі не вважає себе етнічними китайцями), яке під час передвиборних кампаній взимку-навесні 2000 і 2004 рр. активно експлуатувало самостійницькі гасла, але після обрання його кандидата Чень Шуйбяня президентом висловлювало готовність вилучити з партійної програми вимогу проголошення незалежності острова. Чень Шуйбянь вийшов із ДПП і запропонував Пекіну почати переговори про мирне об'єднання країни, а депутати парламенту від Гоміндану, що разом із союзниками (*„Панблакитна коаліція"*) зберіг там більшість і після виборів 11 грудня 2004 р., відмінили заборону на пряму торгівлю між Тайванем та провінцією Фуцзянь на узбережжі Тайванської протоки.

Але нарощування Вашингтоном поставок Тайваню найсучасніших систем озброєнь, відсутніх у НВАК, викликає украй гостре роздратування у Пекіні й живить грунт для антиамериканських настроїв у китайському суспільстві, як це мало місце у квітні 2001 р., коли „бунтівний" острів очікував партію підводних човнів, протичовнових винищувачів і надводних суден, у тому числі есмінців, споряджених радарною системою Aegis (після її невеликого удосконалення Тайвань можна приєднати до системи ПРО США).

Дж. Буш-молодший тоді навіть у ранковому виступі на каналі „Ей-бі-сі" заявив, що використання Збройних сил США „є одним із варіантів" у разі вторгнення КНР на Тайвань. Щоправда, дещо пізніше в інтерв'ю „Сі-ен-ен" він уточнив, що ці слова не слід сприймати як виступ за незалежність Тайваню, а американський уряд „повністю підтримує політику єдності Китаю" й очікує, що „всі суперечки будуть вирішуватися мирним шляхом". Продаж Тайбею есмінців із системою Aegis був відкладений.

Щоправда, самі тайваньці скептично ставляться до відомої формули Ден Сяопіна „одна держава – два лади", за котрою відбулося возз'єднання із КНР Гонконгу і Макао у 1997-1999 рр., і воліють почекати лібералізації політичного устрою КНР. „Результати виборів на Тайвані засвідчили, що вирішення тайванської проблеми безпосередньо залежить від політичних реформ у КНР. Це дзвінок до пробудження. КПК має наслідувати приклад Гоміндану і, ще перебуваючи при владі, рушити до демократії", - такі анонімні заклики все частіше з'являються на сторінках Інтернету.

На протилежному боці Тихого океану з середини 90-х рр. минулого століття тема американо-китайського зіткнення поступово витіснила міркування про американо-китайську дружбу початку 80-х рр. Газети знову заговорили про „жовту небезпеку", а доповіді ЦРУ почали малювати апокаліптичні картини війни в Азії за участі КНР, яка насмілилася утвердитися в АТР в якості гравця № 1, витуривши звідти США. Розвідникам наслідували політологи на кшталт С.Хантінгтона, що лякали світ *„зіткненням цивілізацій"*.

У 1997 р. бестселером у США стала книжка вже згаданих Р.Бернстайна і Р.Манро *„Майбутній конфлікт із Китаєм"*, де йшлося про результати його комп'ютерного моделювання військовими. Вони виявися приголомшуючими: США переможуть у ядерній війні з КНР лише в тому разі, якщо вона спалахне до 2015 р., після цього економічна і військова могутність Піднебесної зросте настільки, що війна з нею стане самогубством навіть для Америки. Щоправда, за оцінками незалежних від Пентагону експертів, військові надто перебільшили темпи росту китайської військової небезпеки — в області збройних технологій КНР відстає від США майже на 30 років.

Взагалі ж серед американських учених також немає однозначної позиції щодо майбутньої ролі КНР на міжнародній арені, оскільки чимало науковців і аналітиків припускають можливість перетворення КНР у наддержаву. Але не менше й тих, хто скептично, як З.Бжезінський, ставиться до піднесення *„дракона"* з огляду на його численні внутрішні проблеми, що не дозволять Китаю *„дотягнути"* до статусу наддержави [197]. Щоправда, американські вчені й політики тим і відрізняються від українських, що прораховують як „гірші" для США (набуття КНР наддержавності), так і „кращі" (колапс китайських реформ) сценарії, сподіваючись на „краще", але й готуючись до „гіршого".

„Оптимісти", сконцентровані переважно в Університеті національної оборони США та Інституті дослідження національної стратегії (П.Годвін, Н.Ларді, Дж.Ліллі, М.Нахт, К.Нілер, М.Піллсбері, Т.Робінзон, Р.Соломон, Р.Фішер та ін.), переконані у неминучому посиленні КНР, що, на їхню думку, може завдати шкоди національній безпеці США. Вони стверджують, що Китай прагне стати глобальною наддержавою й поширити свій вплив по всій земній кулі. Такі наміри Пекіна є викликом для США та їхніх союзників, оскільки в основу китайської стратегії покладено націоналізм.

Зазначені науковці виділяють три зони безпосереднього зіткнення інтересів між КНР і США. Перша пов'язана з неминучим проникненням Пекіна на Близький Схід унаслідок стрибкоподібного зростання енергоспоживання економікою Китаю, що призведе до конфронтації зі США, Японією та іншими постіндустріальними державами, які вже облаштувалися в цьому регіоні. До цього прогнозу можна додати ще одну зону потенційних американо-китайських суперечностей із-за нафти і газу — Прикаспій і Центральна Азія.

Наступну зону конфлікту, на переконання *„оптимістів"*, формує політика багатополярності Пекіна, яка полягає у стимулюванні появи нових і посиленні старих центрів сили, що загалом ніби-то зменшує наддержавне значення американського центра. Її проявами є спроби дискредитувати систему американо-японської безпеки, послабити військові зв'язки США з країнами АСЕАН, зміцнити „стратегічне партнерство" КНР з Росією, Іраном і Пакистаном, інтенсифікувати економічні зв'язки з Євросоюзом. Нарешті, третьою очевидною зоною зіткнення є Тайванська проблема.

„Оптимісти", визнаючи великі можливості КНР у справі економічного розвитку, разом із тим не бачать підстав для стурбованості з цього приводу

внаслідок скромного військово-стратегічного потенціалу КНР (282 ядерні боєголовки на стратегічних ракетах і 120 – на тактичних [198]), можливості котрого якісно не зміняться до 2010 р. Звідси робиться висновок про те, що між КНР і США навряд чи станеться збройний конфлікт до 2016 р., але далі однозначної ясності вже немає, тому потрібно зробити все можливе, щоб відвернути Пекін від військово-стратегічного суперництва з Вашингтоном. Це можливо шляхом залучення КНР до діалогів з усього спектру міжнародних проблем, як на двосторонній, так і багатосторонній основі, тобто пропонується та ж політика „залучення", що здійснювалася адміністрацією В.Клінтона.

Колишній посол США у КНР Дж.Ліллі наполягає на її модифікації у вигляді „балансування між залученням і стримуванням", що передбачає нарощування Збройних сил США у Східній Азії включно з розміщенням систем протиракетної оборони, проти чого активно виступає Пекін. Тому американський дипломат рекомендує Білому домові стимулювати переорієнтацію уваги КНР з Тихого океану на внутрішню континентальну Азію, щоб Пекін відмовився від морської стратегії й поновив китайсько-російську ворожнечу. Це дозволить ефективніше нейтралізувати негативні для США наслідки піднесення Китаю на світовій арені.

На противагу „голубам" з Інституту дослідження національної стратегії США фахівці з *„REND Corporation"* стверджують, що Тайванська проблема може привести до конфронтації й навіть військового конфлікту КНР із США та, можливо, з Японією. До такого висновку їх підштовхує китайська військова доктрина, що включає концепції локальних чи обмежених війн на основі високих технологій і активної периферійної оборони.

На переконання сінологів згаданого *„мозкового центру"*, після 2010 р. стратегічний баланс сил у Східній Азії зміниться на користь КНР, а збройний конфлікт можуть спровокувати тайванські лідери, якщо відважаться проголосити курс на незалежність, у цьому випадку Пекін неминуче використає військову силу проти бунтівного острова. Аналогічну провокаторську роль можуть відіграти і США в разі повернення до політики „двох Китаїв" та збільшення поставок наступальної та оборонної зброї, включно з системою ПРО. Тому США слід залучити КНР в орбіту американської стратегії, змусивши тим самим Пекін грати за правилами Вашингтона.

Концепції *„залучення і стримування"* КНР дотримуються також фахівці з консервативного „Фонду спадщини", що відзначаються високим рівнем професіоналізму і прямотою. Вони не вважають Пекін таким же ворогом Вашингтона, яким була комуністична Москва, але припускають, що дії КНР можуть становити загрозу для США, навіть якщо Китай і не буде сприйматися в якості ворога. Тому Вашингтон повинен зберігати свою військову перевагу в Азії, щоб попередити агресію й розташувати систему ПРО з метою захисту Америки та її союзників від загрози ракетних атак. До того ж США повинні зупинити передачу Китаєм військових технологій і

зброї Ірану, КНДР і Пакистану, оскільки це несе потенційну загрозу американським інтересам.

Водночас *„Фонд спадщини"* висуває вимогу налагодження взаємовигідного співробітництва між Пентагоном і НВАК, маючи на увазі відкриття Пекіном інформації про становище Збройних сил і військові доктрини КНР. Росію ж, Ізраїль і країни Євросоюзу слід попередити про небезпеку переозброєння КНР і відвадити їх від військового експорту в Піднебесну. В економічному блоці рекомендацій головною вимогою є інтеграція КНР у глобальну економіку й анулювання всіх обмежень на торгівлю з боку США в обмін на поступки Пекіна в області прав людини. Не останню роль, на думку вчених із „Фонду спадщини", повинно відігравати і сприяння експансії приватного сектора в КНР як засобу зменшення урядового контролю і реформування політичної системи країни.

Слід зазначити, що практично всі вищенаведені рекомендації наукових центрів США стосовно оцінки місця й ролі КНР у глобальній та азійсько-тихоокеанській міжнародних системах сучасності й на найближчу перспективу були враховані відповідальними діячами адміністрації Дж. Буша-молодшого. Відразу ж після його першої інаугурації радник президента з національної безпеки (нині – держсекретар) К.Райс наголосила, що ідея американо-китайського стратегічного партнерства, яка активно пропагувалася попередньою адміністрацією, повністю втратила своє значення. Одне лише прагнення Китаю змінити співвідношення сил в Азії на свою користь перетворює його у стратегічного конкурента США.

А заступник міністра оборони П.Вулфовіц (у минулому – посол США в Індонезії) в інтерв'ю „Washington Times" відверто пояснив, що Пентагон стурбований спрямованістю зовнішньої політики КНР у цілому. „Китай майже напевне стане наддержавою у найближче півстоліття, а можливо вже у найближчу чверть віку, — зі знанням справи повідомив американський урядовець. – Питання в тому, чи буде новий Китай жити в мирі зі своїми сусідами, чи ж він стане на шлях традиційної *„дипломатії сили"*... Не думаю, що Китай обов'язково стане загрозою, але вважаю, що, коли ми виявимо самозаспокоєність, то фактично сприятимемо тому, щоб ця загроза матеріалізувалася". Аналогічної позиції дотримувався й колишній шеф Пентагону Д.Рамсфельд, який зазначив: *"На мій погляд, майбутнє Китаю ще не написане й пишеться зараз"* [199].

Таким чином, США припускають імовірність перетворення КНР у наддержаву, що несе загрозу безпеці Америки не лише у Східній Азії, але й на Близькому Сході та в Центральній Азії. Політика залучення, що здійснювалася за президентства В.Клінтона, доповнилася політикою стримування, передусім у питаннях військової безпеки, перетворившись після трагічних подій 11 вересня 2001 р. у політику „м'якого стримування Китаю за допомогою його активнішого залучення". Усіма наявними засобами США будуть намагатися загальмувати процес перетворення КНР у наддержаву, чи іншими словами,

самостійний центр світової політики глобального масштабу з тим, щоб зберегти за собою статус одноосібного лідера-гегемона.

1.7. Зброя масової деконсолідації: медіа-тероризм у контексті "синдрому 911"

Міжнародні мас-медіа – інформування чи маніпулювання?

В усіх його формах та різновидах терор обов'язково має на меті встановлення особливого типу ненормативних (патологічних) суспільних комунікацій з активним використанням засобів масового комунікування та інформування. І справа терористів не така вже й безнадійна, як може видатися з першого погляду. Не слід забувати, що чимало історичних рухів розпочиналися саме із системного "*революційного терору*" (більшовизм, націонал-соціалізм), а вже потім між терористами та суспільством, що перетворювалося у їх придушену жертву, встановлювалися відносини патологічної солідарності ("*стокгольмський синдром*").

Отже, у нинішньому світі, що рухається до глобалізації, мас-медіа з їх потужними впливами на масову свідомість та архетипи колективного несвідомого – це саме та грізна двосічна зброя, що її можна повернути на користь антитерористичним операціям, але з таким самим успіхом використати на користь терористів. Адже, орієнтуючись на низькопробні смаки, мас-медіа зазвичай схильні не лише до всілякої «полуничкі», але й до демонстрації сцен ігрового терору з метою збільшення чисельності своєї аудиторії, від чого, відповідно, збільшуються доходи від реклами. А тут мета виправдовує засоби.

Один із західних фахівців з проблем медіа-тероризму, Тед Коппел із американської телекомпанії ABC свого часу слушно зауважив:

«Мас-медіа — особливо телебачення — й терористи, вступаючи у відносини спеціальної залежності, потребують одні одних, між ними виникають відносини симбіозу Без телебачення терорист уподібнився би до філософа, закинутого у лісові нетрі, до голосу якого ніхто не дослухається й докази якого ніким не почуті. Але й телебачення без показу актів терору...втратило б значною мірою інтерес аудиторії» .

Щодо медіа-тероризму ("*медіа-кілерства*") – то він є особливим різновидом психологічного терору, що відноситься до так званого "інфраструктурного". Його глибинна сутність полягає у спробах шляхом організації спеціальних медіа-кампаній зруйнувати знаково-символьну інфраструктуру суспільства та його держави. Йдеться, зокрема, про руйнацію символів влади (і не лише державної). Спектр таких руйнівних деконсолідуючих медіавпливів досить широкий: створення атмосфери громадянської недовіри до дій та намірів влади, непокори, обернення героїв на антигероїв, ідеалів на антиідеали. Особливою мішенню медіа-терору зі зрозумілих причин стають си-

лові структури, покликані захищати суспільний порядок. Укорінюються ксенофобні настрої й підозриливі настановлення щодо "чужинців, якими можуть виявитися представники будь-яких меншин (і навіть "*більшин*").

Політичний терор засобами мас-медіа став у XX ст. справою професіоналів від спецтехнологій, оскільки, згідно П.Бурдьє, "у політиці, як і в мистецтві, експропріація прав більшості співвідноситься і навіть є наслідком концентрації власне політичних засобів виробництва в руках професіоналів, що можуть розраховувати на успіх у власне політичній грі лише за умови, що мають специфічну компетентність" [200].

Політика, як і будь-яка інша сфера професійної діяльності, вимагає оволодіння специфічною мовою більш-менш однозначних у своєму тлумаченні термінів та словосполучень. Тут, як і в тісно спорідненій з політикою сфері права, вибір у дилетантів вельми обмежений. Їм залишається або вдаватися до послуг фахівців, або ж судити про те, що відбувається насправді, орієнтуючись на повідомлення таких малонадійних комунікаторів як мас-медіа Оскільки призначені вони переважно не скільки для інформування, скільки для маніпулювання, що є особливо відчутним у сфері безпосередньо "недотикальної" міжнародної політики.

Йдеться, зазвичай, про медіа-маніпулювання штучно створеними ситуаціями, що підмінюють природні і які визначають у термінах "*макіавеллізму*". З ним нерозривно пов'язана квазідемократія, яку кваліфікують як маніпулятивну. У внутрішній політиці така маніпулятивна демократія спирається на вузький прошарок квазіеліти, який вітчизняні політичні аналітики визначають химерним терміном "олігархізм". Але, якщо внутрішня квазіеліта маніпулює поведінкою людей в окремо взятих країнах, то міжнародна - поведінкою цілих регіонів світу.

У вітчизняній політичній практиці усе це досить умовно називається використанням "адмінресурсу". Неважко здогадатися, наскільки потужним є такий ресурс в міжнародній політиці. Особливо враховуючи, що за умов сучасної глобалізації відповідні міжнародні штаби, які спеціалізуються на глобальному урядуванні (Global Governance), починаючи від СОТ, МВФ й СБ і закінчуючи Давоським форумом та зібраннями "Великої Вісімки", діють дедалі успішніше, міжнародні мас-медіа дедалі успішніше виживають з інформаційних просторів національні, а глобальне (транснаціональне) громадянське суспільство перебуває, тим часом, лише у зародковому стані.

Оже, демократична зовнішня політика поки що залишається сферою благих намірів та побажань. Якщо, наприклад, перенести на міжнародну арену схему "один виборець - один голос", то незрозуміло, хто мав би виступати суб'єктом міжнародного "виборчого процесу". Якщо це мають бути окремі національні держави, то тоді Фолклендські острови матимуть той же статус, що й Китай. Якщо ж створити один глобальний виборчий округ, то виявиться, що кожен третій виборець у цьому окрузі буде китайцем або індусом. У кінцевому підсумку, проблема надання міжнародним інститутам

демократичної легітимності поки що принципово виглядає як "*квадратура кола*".

Проте, реально існують медіа-інформаційні ТНК й ці потужні міжнародні мас-медіа (МММ) створюють повну ілюзію існування глобальної громадської думки і навіть глобального громадянського суспільства. Іноді таке міжнародне медіа-маніпулювання уподібнюється до культурного неоколоніалізму, прибираючи демонстративно антидемократичних й антинаціональних форм. Але частіше воно здійснюється в завуальованих формах, коли "*вчителі демократії*" вдаються до популізму у "*світовій школі демократії*" (майже так само як це роблять пересічні шкільні вчителі) й позиціонують цілі країни та регіони за статусними ролями "двієчників" та "відмінників".

Тут відбувається щось подібне до телевізійних сюжетів на політичні теми, пов'язаних з апеляцією до інтересів масової аудиторії, думки якої подаються як *vox populi*. Хоча насправді мова йде про інтерактивну гру, покликану "легітимувати" або думку режисера телепередачі, або наміри його замовника. Жодна реальна аудиторія в таких телепередачах насправді участі не бере, а є лише уявний образ цієї аудиторії, — міф, що його придумав для себе і на потребу своєму замовнику журналіст. Майже те саме, по суті, відбувається у випадку з маніпулюванням міжнародними рейтингами і показниками, суб'єктами якого виступають чисельні західні аналітичні центри (*think tanks*).

Звичайно, йдеться про старе правило "*поділяй і владарюй*". Не випадково абревіатуру WMD, що означає "weapons of mass destruction" ("*зброя масового нищення*") на Заході дедалі частіше за співзвуччям розшифровують як "weapons of mass desruption" ("*зброя масової деконсолідації*").

Синдром 911: антитероризм і міфологема суспільства "всезагальної безпеки". Нині, у "постверсневій" ситуації дехто поспішає констатувати — "*The American Dream is Over*" ("Американська Мрія уже позаду").

У подібній констатації є чимала правда, бо ревізії зазнає не лише "Мрія", але й світовий "ялтинський" порядок безпеки, що сформувався після II Світової війни. Відповідно світовими мас-медіа активно руйнується під благим приводом антитероризму знаково-символьна інфраструктура, яка відповідала "*застарілому*" світоустрою.

Адже "башти-близнючки" (Twin Towers) Світового Торговельного Центру (СТЦ) символізували не лише геркулесові стовпи, що, у свою чергу, стали загальноусталеним символом "*Його Величності Долара*", — $. Вони символізували щось більше від поважної американської грошової одиниці й самої Америки, — спосіб життя, замішаний на всеосяжній утопії ринкового суспільства (маркетопії, - Market Society).

Такий квазіринок у координатах "The American Dream" був чимось на зразок "соціокультурної віагри". Нині ж, коли "*вірус*" тероризму цю

«Синдром 911» має на увазі сам цю, приурочену до терактів 11 вересня 2001 р., «постверсневу ситуацію», оскільки в усталеному на Заході написанні дат спочатку вказується місяць. а згодом число.,

соціокультурну програму з'їв, її доведеться переписувати, але у зовсім інших координатах.

Провідними цінностями тут напевно будуть, не Ринок і Демократія, а Безпека у всіх її вимірах та на усіх рівнях (*safety&security*). Тут знадобляться свої оруелловські "міністерства правди". Тут пануватимуть не "високі", а "низькі" медіа-інформаційні технології: маніпулятивна "мікровлада", утаємниченість, адаптивність, висока ступінь дублювання тощо.

Є також певна символіка в тому, що найпершим об'єктом "помсти" США вибрали наймаргінальнішу країну світу, яка у світових координатах знаходиться буквально на протилежному полюсі – Афганістан. Разом із іракською авантюрою усе це знадобилося лише для того, щоб "переписати" національну ідентичність та фундаментальні цінності "The American Empire". Відповідно, можна стверджувати, що "Empire" зазнає стрибкоподібного фазового переходу і вступає у третій після II Світової війни період свого ідеологічного розвитку, переосмислюючи відносини між минулим, теперішнім та майбутнім.

Перша "Мрія" сформувалася після Великої Депресії під впливом кейнсіанства. Це була віра у всемогутню регулятивну функцію держави та її фіскальної політики. Наслідком стало перетворення США після війни у найпотужнішу державу світу. Впродовж трьох десятиліть зростали стандарти життя й, відповідно, демографічні показники.

В'єтнам та Уотергейт зруйнували цю першу версію Мрії й призвели до "стагфляції", пік якої припав на 1973 р. Кінець 70-х рр. дискредитував Мрію про "державу всезагального благоденства" остаточно. Імпотентність такої держави особливо унаочнилася в історії з 52 американськими заручниками (працівниками посольства) в Тегерані, яких впродовж 444 днів і ночей не змогли визволити американські спецслужби.

Коли ж Америка початку 80-х рр. вибрала президентом Рональда Рейгана, то вона увійшла у другий період переосмислення своєї Мрії. Саме тоді з'явилася утопічна ідеологема "Market Society", яку США почали пропагувати й насаджувати у глобальних масштабах. Цьому посприяло й безпрецедентне економічне зростання 1983-1990 рр., що дало привід для виникнення теорії "дерегулювання" й масованої приватизації як всезагальної економічної панацеї. Падіння Берлінського муру та "*оксамитові революції*" кінця 80-х – початку 90-х рр. ще більше підсилили цю ринкову утопію, з позицій якої державне регулювання та планування розглядалося як безнадійний анахронізм. Зрештою, — таким самим анахронізмом проголошувалися національно-державні утворення як такі. Доктрина "*нового трайбалізму*" (Герберт Маршал Маклюен) пропонувала відміну державності національного типу й повернення на новому витку спіралі до родоплемінних утворень у "*глобальному селі*".

Проте, наприкінці 90-х США зустрілися з економічною рецесією та примарою Великої Депресії зразка 1929 р., про небезпеку якої, до речі, попе-

реджав у відомій промові про "ірраціональне збагачення" від 5 грудня 1996 р. глава Федеральної резервної системи Алан Грінспен. 8-річна "Клінтоніада" закінчилася й тому спадкоємець попереднього президента Ал Гор не мав жодних шансів стати новим президентом. Отже, "Market Society" було справжньою мішенню терактів, вчинених "чорного вівторка". Але ринкове суспільство не може врятувати американців і гарантувати їм порядок та безпеку. Радше навпаки, воно може лише підсилювати безладдя та небезпеки. Те, у чому уже встигли переконатися на своєму гіркому досвіді "ринкових перетворень" постадянські суспільства з українським включно стало нині самоочевидним і для Америки та усього "*вільного світу*".

Отже, на черзі нова версія Американської Мрії, яку Річард Еріксон свого часу проголосив "політикуванням у ризикованому суспільстві" ("policing [of] the risk society"). Провідною формою цієї нової політики стане кризовий менеджмент, а державі буде повернути її регулятивні функції. Значно посилиться роль військових та спецслужб. Неважко передбачити й новий виток мілітаризації економіки. Власне, вона уже розпочалася після проголошення Дж.Бушем масштабної програми створення НПРО (NMD). Виключна увага надаватиметься методам збору й обробки інформації (навіть з використання "недемократичних" прийомів тотального стеження), а також конкурентним аналітичним технологіям. Контртерористичні акції спецслужб стануть звичною рутиною способу життя, а *Безпека* — тією "*Мрією*", яку постійно підживлюватиме страх перед небезпеками.

Сучасна Америка намагається зіграти у "*глобальному селі*" роль "глобокопа" й провідника «найвищих вартостей і пріоритетів». А тому й викинула на смітник дотеперішній панамериканський ізоляціонізм (бушевське перевидання доктрини Монро), перейшовши до остаточного наведення у світі нового світового панамериканського ладу (Pax Americana). Конкретно це означає необхідність для усіх інших країн (включно з Україною) неухильно підпорядкуватися США в ім'я наведення цього "антитерористичного" порядку. Що ж до іракської проблеми, то вона виступає у цій новій ситуації лише лакмусовим папірцем, покликаним встановити, хто й наскільки підпорядкувався єдиній наддержаві.

Йдеться, таким чином, про ціну, яку доводиться платити за свободу й демократію, з одного боку, та безпеку, — з іншого. Оскільки тут далеко не завжди виникають безхмарні кореляції. Зокрема, буржуазний ідеал гедоністичного суспільства масового споживання "*наввипередки*", безумовно, таїть в собі небезпеку саморуйнації. І міжнародний тероризм є лише однією із видимих, найбільш демонстративних ознак подібної саморуйнації.

Комунікативні дилеми надзвичайних ситуацій: колізії між правом людини на інформацію й на захист персональних даних. Відомий американський фахівець із антикризового медіа-комунікативного менеджменту Пітер Сендмен зазначає, що маємо тут, зазвичай, справу із, принаймні, десятьма дилемами. При чому, варто підкреслити, що це саме дилеми. Тоб-

то мова не йде про вибір альтернативного типу, коли одна із двох альтернатив більше відповідає ситуації, аніж інша. У випадку надзвичайних ситуацій мова йде саме про дилемність вибору. Тобто йдеться навіть не про вибір "меншого зла", а "*більшого добра*" й необхідність залишити "поза дужками" так зване "*менше добро*" з усіма відповідними маловтішними наслідками.

Хоча сам Пітер Сендмен схиляється до вибору першої дилеми серед десяти, ним перерахованих, це зовсім не означає, він не усвідомлює суб'єктивності свого вибору й необхідності "платити" за цю суб'єктивність неминучу у подібних випадках ціну. Отже йдеться про дилеми:

- щиросердність проти секретності;
- спекуляції проти опори на точні факти й відмови від спекуляцій;
- ставка на сумніви проти довіри;
- алармування проти самозаспокійливого убезпечення;
- загальнолюдський підхід з позицій "здорового глузду" проти професіоналізму;
- апологія прав людини проти владного охоронництва;
- децентралізація проти централізації;
- демократія й індивідуальний контроль проти прийняття рішень, заснованих на експертних оцінках;
- наставляння на применшування загроз проти наставляння на сіяння паніки;
- наставляння на попередження загроз проти наставляння на їх ігнорування.

Так або інакше проблема існує і розв'язати її за рахунок енергійного "*струшування повітрям*" неможливо. Неважко помітити головний "*нерв*" цієї проблеми у протиріччі між правом людини знати та необхідністю у обмеженні цього права у надзвичайних ситуаціях, коли потреба у поінформованості, навпаки, загострюється до крайніх меж й, здавалося б, має сповна задовольнятися.

Але, оскільки масове інформування здійснюється за принципом "*всім, всім, всім*", тобто не є вибірково-цілеспрямованим, то інформація, яка поширюється подібними каналами масових комунікацій, може потрапляти до надто різних людей, які, у свою чергу, можуть використовувати її з різними, — іноді злочинними, — намірами. Принаймні, це саме той випадок, коли більшість страждає із-за непевної поведінки меншості.

Зрештою, йдеться про проблему безпеки масових комунікацій. З одного боку, людина або цілі групи людей мають право на поінформованість, щоб приймати компетентні рішення у звичайних й, тим паче, — у надзвичайних ситуаціях. Але необхідним доповненням до цього права є інше, спрямоване на збереження таємниці персональних або корпоративних даних. Його забезпечення особливо важливе в ситуаціях, коли виникають (або невдовзі можуть виникнути) загрози й ризики для життя і здоров'я.

Отже, важко заперечувати ситуації, за умов яких вповноважені на те державні органи мають право призупиняти дію гарантованого чинним законодавством масового інформування та жорстко регламентувати таке інформування.

Але, знову ж таки, — обмежувати у достатньо прозорих вимірах часу й простору, передбачуваних чинним законодавством. Держава та її уповноважені до того органи й служби мають, зокрема, знати майже все про наміри тих громадян (тим паче, негромадян), чия поведінка за певних обставин може бути загрозливою як для безпеки самої держави, так і для безпеки суспільної й персональної.

З точки зору загально-правової тут усе нібито зрозуміло. Цензура та її пряме доповнення у вигляді обмеження права громадян на збереження таємниці персональних даних є безпосередніми наслідками медіа-комунікативної складової антикризового менеджменту. Проте, ця зрозумілість існує лише in *abstracto*, але вельми й вельми проблематична in concreto, тобто у конкретних надзвичайних ситуаціях з їх нерозв'язальними дилемами, коли "підеш направо, — голову втратиш, а підеш наліво, — коня" (колись ці втрати були майже тотожними).

Контроверсійні кроки російської влади, окрім "*мовчазної більшості*" у самій Росії, знайшли підтримку у головного організатора світової антитерористичної кампанії, — американського президента Джорджа Буша, який відразу ж заявив, що сповнений розуміння до украй важких рішень, що їх довелося прийняти президенту Володимирові Путіну. "Родичі (загиблих під час газової атаки російського спецназу) звинувачують Володимира Путіна, — сказав Президент США, — але звинувачувати вони повинні терористів".

Такі слова не є простою даниною у відповідь на політику російського президента, який свого часу першим серед світових лідерів підтримав Буша в його війні проти "Аль-Каїди". Ця риторика американського президента спрямована передусім на виправдання його власної політики щодо американських мас-медіа, які він невпинно "перевиховує" від самого моменту 11 вересня 2001 р. й початку антитерористичної операції.

Наприкінці грудня 2002 р. "New York Times" у матеріалі під промовистою назвою "Великий Брат у всеозброєнні й готовий діяти" повідомляла, що електронні служби Пентагону з метою боротьби з тероризмом готові до тотального моніторингу інформації щодо поведінки цивільного населення [201]. Йдеться про систему, яка отримала умовну назву *Тотальної інформаційної обізнаності* (Total Information Awareness initiative).

Станом на 23 грудня 2002 р., Білий Дім отримав вже біля 9 000 пропозицій щодо зазначеної ініціативи з тотального інформаційного стеження («Washington Times», «Insight magazine»). В Росії така "ініціатива", що стосувалася посилення СОПЗ ("*система оперативно-пошукових заходів*"), свого часу теж обговорювалася, але була, я відомо, "*заблокована*" Верховним Судом.

Так або інакше, наслідком чергової кризи у стосунках журналістів з російською владою стали спроби законодавчого врегулювання поведінки журналістів в екстремальних умовах та прийняття поправок до існуючих законів, які перевели б далеко не однозначну проблему "*ЗМІ й тероризм*" у площину правового регулювання.

Слід віддати належне російським законотворцям, які виявили тут чудеса оперативності та, водночас, — російському президентові, який вкотре підтвердив високе реноме "непогрішимого арбітра" в гостро-конфліктних ситуаціях. Як відомо, трагічний фінал операції зі звільнення заручників припав на 26 жовтня 2002 р. А вже 1 листопада нижня палата російського парламенту (Дума), а слідом за нею 13 листопада й верхня палата (Рада Федерації) ухвалили доповнення й поправки до законів про ЗМІ та про боротьбу із тероризмом, спрямовані на те, щоб максимально "зістикувати" ці два закони. У цьому часовому проміжку, 3 листопада, з'явилися відповідні "*методичні рекомендації*" очолюваного Михайлом Лесіним Міндруку РФ.

У будь-якому разі, зазначені поправки істотно обмежили свободу дій журналістів у висвітленні як актів тероризму, так і контртерористичних операцій. Внесені зміни не дозволяли, зокрема, поширювати у ЗМІ інформацію, що могла стати на заваді проведенню контртерористичних операцій і створювала б загрозу для життя людей. Заборонялося також поширювати інформацію, що розкривала би без згоди на те відповідальних осіб персональні дані щодо співробітників спецслужб й спецпідрозділів та членів оперативного штабу із проведення операцій, а також щодо осіб, які надають їм підтримку.

При цьому, коментуючи висвітлення ЗМІ теракту із захопленням заручників, скоєного у театральному центрі на Дубровці, деякі російські сенатори небезпідставно стверджували, що журналісти мимоволі допомагали терористам у своїх репортажах, висвітлюючи пересування спецназу тощо. Частина правди в таких звинуваченнях, безумовно, є. Крім того, не є особливою таємницею, що на час московської драма, яка тривала 57 годин від 23-го до 26 жовтня 2002 р., чеченські терористи примушували заручників обдзвонювати не лише родичів, але й провідну пресу, щоб та "чинила тиск" на Кремль.

Також про добре відомий "*синдром заручників*", згідно якого через певен час перебування в заручниках спостерігається парадоксальна тенденція до підтримки терористів, солідарності з їхньою позицією. Російські журналісти, коли описують феномен заручників, захоплених чеченцями, пригадують, зокрема, своєрідну "*повагу*" терористів у їх наставлянні до захоплених.

Більше того, задовго до трагічних подій на Дубровці «*свобода слова*» набула в Москві та в інших великих містах Росії таких гротескних вимірів, що почала заперечувати не менш важливу свободу громадян на збереження персональних даних. За дуже помірну плату, зокрема, на вулицях Москви можна, приміром, придбати компакт-диски із персональними даними на майже усіх

без винятку діячів політики, економіки й культури. Не важко здогадатися, ким і з якою метою може бути використана подібна персональна інформація. Започаткували, до речі, такі "*інформаційні викиди*" діячі із охоронної служби підпорядкованого на той час Михайлу Гусинському телеканалу НТВ.

Тож, нічого немає дивного в тому, що, попри усю слушність й своєчасність, російські законодавчі ініціативи як всередині країни, так і на Заході були зустрінуті або вкрай вороже, або "*без належного розуміння*".

Більшість коментарів зводилась до тези, — під приводом боротьби з тероризмом Росія впроваджує цензуру мас-медіа. Зокрема, Гєнсек Спілки журналістів Росії Ігор Яковенко розцінив прийняті Радою Федерації поправки як "повернення до цензури".

Справді, на час трагічних подій на московській Дубровці з фактами неприхованої цензури зіштовхнулися чимало не лише російських, але й іноземних журналістів, акредитованих у Москві. Загальновідомими є, зокрема, події довкола телеканалу "Московія" (російський аналог українського ICTV), газети "Версии" та радіостанції "Эхо Москвы". У Ганса Вільгельма Штайнфельда із норвезького телебачення агенти російської спецслужби конфіскували відеокасети й стерли всі записи, які стосувалися чеченських біженців. Інцидент спричинився навіть до офіційного протесту норвезького уряду.

На думку деяких критиків, усе це — ознаки повернення до "*темних сторінок минулого*", "*відродження старого апарату репресій*" тощо. Проте, інші, менш критично налаштовані оглядачі, вважають цензурування інформації за умов проведення антитерористичних операцій цілковито виправданим, а відтак виправдовують й особливий "інформаційний режим" аж до перехоплення персональної інформації громадян в інтересах їхньої ж безпеки.

Доречно зауважити, що до числа таких "*особливих оглядачів*" належить рішуча більшість пересічних громадян Росії, — тих, кого Річард Ніксон відніс свого часу до "мовчазної більшості". За даними опитування громадської думки, проведеного в Росії у листопаді 2002 р. Агентством регіональних політичних досліджень (1 600 респондентів із різних регіонів Росії), ***61%*** респондентів схвалюють цензуру й лише ***35%*** ставляться негативно до обмеження прав мас-медіа (***4%*** - "не визначилися"). Вельми прикметно, що відсоток тих, хто схвалює цензуру, помітно вищий у середніх за розмірами містах (до півмільйона населення) й, навпаки, — є помітно нижчим у містах-мільйонниках.

Внесені російським парламентом поправки до законів про ЗМІ й боротьбу з тероризмом були сформульовані, на думку багатьох правозахисників, так, що могли бути застосовані не скільки проти "медіа-терористів", скільки стосовно "*неугодних*". Закон, насправді, настільки широко потрактував "антитерористичні" ситуації, що до них можна було віднести практично будь-який репортаж про війну в Чечні, не кажучи вже про розслідування таких

спірних моментів, як несвоєчасне надання медичної допомоги жертвам недавнього теракту із захопленням заручників. Передбачалося строго регламентувати кореспонденції про перебіг «антитерористичної операції» в Чечні. Адже відомо, що офіційну "антитерористичну" точку зору Кремля щодо характеру подій в цій кавказькій республіці поділяють далеко не всі політики й журналісти.

У свою чергу, вельми двозначно можна було, спираючись на щойно ухвалені поправки, тлумачити «пропаганду на користь терористів». За бажання до неї можна було легко зарахувати не лише розлоге цитування висловлювань бойовиків, але й надто "суб'єктивні" журналістські тлумачення поведінки терористів або представників спецслужб.

Але найголовніший "прокол" російських законотворців полягав у тому, що вони вирішили за журналістів, як тим себе поводити в екстремальних ситуаціях, не порадившись з самими журналістами. Тож не дивно, що група із 23 провідних журналістів Росії підписала звернення до Володимира Путіна з проханням накласти вето на закон, уже схвалений обома палатами Федеральних Зборів.

Отже, російський президент мав усі підстави вирішити, що "важливо знайти баланс між обмеженням свободи преси і можливістю повного доступу громадськості до інформації", дорікнувши заодно деяким ЗМІ, що вони висвітлювали події, пов'язані із захопленням заручників у Москві, безвідповідальним чином аби підвищити свої рейтинги й наклади.

До речі, це думка не лише російського президента. Генеральний директор першого російського телеканалу «ОРТ» Костянтин Ернст, у свою чергу, зазначав, що преса в екстремальній ситуації припустилася цілого ряду помилок. Щоправда, він відкинув звинувачення на адресу преси в тому, що вона начебто зумисне порушувала вказівки оперативного штабу.

Досі залишається відкритим питання, *де* і в *чому* російський президент вбачає грань між свободою ЗМІ й турботами про безпеку держави та її громадян і в чому полягатиме "кращий баланс між контролем над ЗМІ й інформацією, що не дає державі почуватися непогрішимою». Але підлягає жодному сумніву, що таку грань слід шукати не лише російському президенту і що за умов антитероризму її пошуки стали вельми нагальними.

Медіа + тероризм = Медіа-тероризм. Поза сумнівами, медіа й тероризм створюють вадливе коло, бо, демонструючи сцени ігрового чи реального терору, мас-медіа продукують "*терористичну свідомість*" з усіма наслідками так званого "*секондного тероризму*". Ця закономірність добре відома західним фахівцям із спецслужб. Отже, виникає цілковито обґрунтована підозра, що саме ці фахівці часто-густо й диригують масовими кампаніями на захист "*свободи мас-медіа*" у нових незалежних державах від будь-яких спроб державного регулювання.

Але чи розуміють вони, що сприяють деградації масової свідомості у "нових демократіях", це вже "інше запитання". Тим часом, за умов низької

платоспроможності населення та майже повної економічної залежності нових "демократичних мас-медіа" від іноземного та вітчизняного капіталу термін "свобода слова" звучить майже само як "*гарячий лід*" (філологи називають такі словосполучення оксюморонами). Кампанії на захист "свободи мас-медіа" активно підтримують місцеві медіа-магнати, зацікавлені у зростанні доходів від реклами.

Для здійснення психологічного терору використовуються не лише друковані ЗМІ та мережі ефірних й кабельних мас-медіа, але й Інтернет, електронна пошта, різноманітні електронні іграшки, компакт-диски, аудіокасети тощо. Особливим різновидом медіа-тероризму є відверта "*нахабна*" пропаганда. Ще в 1938 р. в США вийшла серія книг, присвячених розвінчуванню прийомів такої терористичної пропаганди. Виокремлювалося 7 її типових прийомів: називання речей "*своїми іменами*" (Name-Calling), "*блискучі узагальнення*" (Glittering Generality), звернення до "*заповітів предків*" (Testimonial), звернення до "*простих людей*" (Plain Folks), "*завищення ставок*" (Card Stacking), передача "*важливих повідомлень*" (Transfer), "*гуркотлива таратайка*" (Band Wagon).

До речі, слово "пропаганда" у вітчизняній літературі звучить іноді у позитивному сенсі, хоча у західній (особливо — у протестантських країнах) — має однозначно негативне забарвлення й означає "шахрайські" впливи на масову свідомість з метою формування фальшивих цінностей ("аттитюдів").

З початком інформаційної революції можливості подібної терористичної пропаганди й маніпулювання масовою свідомістю значно посилилися. З легкої руки французького постмодерніста Жака Бодріяра з'явилося поняття "симулякр". У згаданого автора є навіть робота, датована 1991 р., "Війни у Перській затоці не було", у якій він доводить не те, що подібної війни взагалі не було, а те, що справжня війна не мала нічого спільного з її образами, з якими знайомилися на екранах своїх домашніх телевізорів глядачі CNN. На тлі терактів, здійснених 11 вересня, та наступної "*антитерористичної війни*" США і їх союзників цих симулякрів у різних мас-медіа помітно побільшало.

У випадку медіа-інформаційного тероризму йдеться про зловживання інформаційними системами, мережами та їх компонентами для здійснення терористичних дій та акцій. Такий різновид тероризму характеризується як множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами й спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує його ризики, бо чим більш інформатизованим є суспільство, тим більш воно піддатливе до впливів масово-психологічного терору.

Для України, де інформаційна діяльність поки що не отримала належного розвитку, головні загрози у сфері медіа-інформаційного тероризму є не скільки внутрішніми, скільки зовнішніми. Їх переважно створюють іноземні держави, міжнародні терористичні та інші злочинні угруповання й організації,

які користуються нерозвиненістю і слабкістю відповідних державних структур. Організовуються й спеціальні деструктивні медіа-кампанії та спецоперації, спрямовані на поширення в "*нових демократіях*" дезінформації та дифамації, насаджування духу ненависті та нетерпимості щодо певних суспільних груп (*етнічних, класових, конфесійних* тощо). Досвід сусідніх країн показує, що такі кампанії разом із актами психологічного терору проти "чужинців" передували громадянським конфліктам та війнам. У 2000 р. спроба організувати таку кампанію на тлі подій, пов'язаних із трагічною смертю композитора І.Білозора, була здійснена у Львові.

Йдеться також про відверту медіа-пропаганду діяльності груп терору та політичних або релігійних екстремістів, які видаються за "захисників свободи та незалежності", "справжніх патріотів", "невинних правдолюбців та шукачів істини" тощо. Японія, зокрема, зустрілася свого часу з такою пропагандою діяльності деструктивних культів типу "Аум сінрікьо" (в Україні свого часу так само безкарно пропагувалося "Біле Братство").

З виявами медіа-терору Україна зустрілася також на час так званого "касетного скандалу". Й лише недостатність медіа-ресурсів та відсутність в Україні "медіа-кілерів" високої кваліфікації завадила організаторам цієї акції досягти поставленої мети, - ліквідації інституту президентства.

Мас-медіа використовуються насамперед з метою психологічної обробки масової свідомості для ліквідації "імунних бар'єрів" самозбереження та самозахисту, ігнорування елементарними правилами особистої та громадської безпеки, насаджування відчуття приреченості тощо. Для цього використовуються прийоми зняття природжених табу та естетизація психопатичної поведінки та різноманітних збочень включно із вбивствами та фізичним і психологічним насильством , героїзація криміналітету й, навпаки, - дегероїзація працівників спецслужб, правоохоронних органів, ветеранів війн та праці тощо. У цьому розумінні медіа-тероризм часто передує актам "матеріального" тероризму.

Після того як в американських школах почастішали акти насильства і вбивств спеціальною комісією Конгресу США була проведена експертиза різноманітних «трилерів», яка виявила, що серед героїв цих фільмів приблизно порівну «хороших» й «поганих» хлопців так само як і сцен психологічного терору та фізичного терору. Що ж до України, то, здається, жодних серйозних спроб аналогічного аналізу програмної політики провідних медіа-каналів радіо й телебачення ще не робилося, хоча "неозброєним оком" помітна необхідність у такому інформаційно-психологічному аналізі з усіма належними висновками.

Особливу увагу слід звернути на формування позитивного "антитерористичного" іміджу України як суспільства і держави у західних мас-медіа, оскільки останнім часом вони систематично насаджують гротескно-спотворений імідж України як країни, що надає нібито притулок терористичним групам, продає зброю "*проблемним*" країнам, які підтримують тероризм тощо.

Україну постійно й на всіх рівнях репрезентують як наскрізно корумповану та криміналізовану державу, у якій масово поширюються ВІЛ-інфекція та наркоманія тощо. При чому, більшість негативних сюжетів західних масмедіа з "мазохістською завзятістю" підхоплюють вітчизняні медіа. Часто вони й самі "підкидають" такі сюжети Заходові. Прикладом тому є дезінформація напередодні "атак на Америку" (отримана буцімто каналами СБУ й згодом спростована СБУ) щодо діяльності в Україні до десятка зарубіжних терористичних центрів. Що ж до системи контрпропаганди, то вона, попри усі розмови про її необхідність, у державі фактично відсутня.

Держкомтелерадіо України та парламентський комітет з питань свободи слова та інформації обмежуються переважно абстрактними або електорально (постелекторально) спрямованими розмовами про "*свободу слова*" замість того, що вжити заходів щодо активного державно-правового регулювання інформаційних процесів і відвернення інформаційних загроз, а також приведення національного інформаційного законодавства у відповідність з нормами міжнародного права за умов одночасного захисту національних інтересів в інформаційній сфері. Тим часом, особливістю негативних інформаційних впливів включно з актами медіа-інформаційного терору є їх непрозорість або напівпрозорість, вони можуть бути виявлені лише в результаті спеціальної експертизи, яка й має стати справою справжніх фахівців з медіа-інформаційної політики.

Додаток 1. Методические рекомендации по освещению в СМИ чрезвычайных ситуаций, представляющих угрозу безопасности людей (проект Минпечати РФ)*

Учитывая стремление СМИ находиться в центре событий, обеспечивая право общества на получение достоверной информации, журналистское сообщество считает необходимым создать устойчивую систему необходимых действий и принципов при освещении чрезвычайных ситуаций, представляющих угрозу безопасности людей. Опыт последнего времени позволил разработать следующие методические рекомендации:

1. СМИ и журналисты при работе в чрезвычайных ситуациях должны строго соблюдать действующее законодательство о СМИ и о борьбе с терроризмом.
2. Всегда иметь в виду, что сообщения в СМИ являются общедоступными, в том числе и для тех, кто намеренно создает критическую ситуацию. Их реакция на ваши сообщения может быть неадекватной;
3. Избегать детальных подробностей о действиях профессионалов, занятых спасением людей;
4. Исходя из того, что доступ к СМИ с целью изложения своей позиции в большинстве случаев является одной из главных целей террористов, журналистам необходимо:

* http://www.mptr.ru/user/index.cfm?tpc_type=3&msg_id=1465&tpc_id=6

- не брать у террористов интервью по своей инициативе
- не предоставлять им возможности выйти в прямой эфир без предварительных консультаций с правоохранительными органами
- помнить, что прямая трансляция может использоваться террористами для передачи условных сигналов сообщникам в других местах
- быть готовыми в любой момент прервать прямую трансляцию с места события
- не комментировать и не анализировать требования террористов на дилетантском уровне, без профессиональных консультаций
- отдавать себе отчет в том, что заложники террористов являются и заложниками ситуации, в определенный момент превращающимися в инструмент давления и на государство, и на общественное мнение

5. Не пытаться получить доступ к секретной информации спецслужб, проводящих контртеррористическую операцию. Невольно проговорившись, вы можете не только сорвать освобождение заложников, но и погубить многих людей, в том числе тех, кто идет на помощь;
6. Учитывать, что спасение людей важнее права общества на информацию. Прямо сообщать, что часть информации закрыта по соображениям безопасности;
7. Помнить о своей обязанности информировать общественность, а не сеять панику. Следить не только за смыслом сказанного, но и за тоном;
8. При освещении события не мешать работать правоохранительным органам, медицинским и иным службам, чья задача спасти людей;
9. Стремиться быстро оценивать степень важности информации и ее потенциальную опасность для развития ситуации:

- помнить, что мировое сообщество отвергает связь терроризма с факторами расы, религии и национальности
- не стремиться намеренно оскорблять и унижать террористов, в руках которых жизнь заложников
- не использовать непроверенные источники информации

10. Быть тактичными и внимательными к чувствам родных и близких жертв терроризма;
11. Избегать излишней сенсационности и натурализма при показе жестокости и насилия, с уважением относиться к нравственным и религиозным чувствам своей аудитории;
12. Не допускать монтажа документальных материалов, при котором может исказиться или извратиться смысл происходящих событий;
13. Не предлагать лицам, вовлеченным в критическую ситуацию, предпринимать какие-либо действия для получения «удачных» фото- или видеокадров;
14. Не стремиться стать действующим лицом в критической ситуации. Не брать на себя роль посредника;
15. Если журналист оказался в числе переговорщиков, он должен воздер-

жаться от собственных публикаций до разрешения кризиса;

16. Своевременно предупреждать официальные органы обо всех ставших вам известными планах проведения или развития террористических актов, даже если они представляются вам маловероятными.

Додаток 2. О роли журналистов в международных усилиях по предотвращению и искоренению терроризма*

Федеративный Совет Союза журналистов России, напоминая о соответствующих резолюциях 1368 (2001) и 1373 (2001) Совета Безопасности ООН, а также о резолюциях 56/1 Генеральной Ассамблеи ООН и 31-й сессии Генеральной Конференции ЮНЕСКО, заявляет о своей решительной поддержке международных усилий по предотвращению и искоренению терроризма и считает необходимым:

1. Проведение силами мировой журналистской общественности под эгидой ООН и ЮНЕСКО международной кампании с целью формирования в общественном сознании активного неприятия терроризма

2. Включение темы разоблачения терроризма в учебные программы факультетов журналистики.

3. Разработку специальных международных рекомендаций относительно вклада СМИ в борьбу с терроризмом.

Кроме того, Федеративный Совет призывает всех коллег как в стране, так и за рубежом озаботиться скорейшей выработкой специальных профессионально-этических правил. Существующие международные, национальные и внутрикорпоративные этические кодексы могут дать лишь самые общие ориентиры журналистам, непосредственно освещающим акты терроризма и контртеррористические операции. В то же время именно эти ориентиры должны составить основу специальных правил, поскольку профессиональная этика неотделима от таких ценностей, как мир, демократия и свобода, тогда как акты терроризма попирают эти ценности и являются нападением на человечество в целом. И именно журналисты должны сами как выработать эти правила, так и обеспечить их соблюдение всеми, кто достоин называться журналистом.

В этой связи Федеративный Совет Союза журналистов России предлагает коллегам для обсуждения нижеследующий проект.

Правила профессионального поведения журналистов, освещающих акты терроризма и контртеррористические операции. При сборе информации журналист должен, прежде всего, думать о безопасности заложников и потенциальных жертв, их родственников, а также участников контртеррористической операции. Вот почему он должен:

- не предпринимать никаких независимых и неразрешенных правоохранительными органами действий, могущих подвергнуть жизнь заложни-

* www.ruj.ru/smi-teror.htm

ков и потенциальных жертв еще большему риску;

- избегать прямых контактов с террористами, поскольку это может затруднить работу участников контртеррористической операции и подвергнуть еще большей опасности жизнь заложников, а также создать угрозу жизни самого журналиста;
- проявлять особое внимание и чуткость к тем источникам информации, кому может быть нанесен ущерб в результате публикации журналистского материала с места события, и в первую очередь, в отношении детей, женщин, пожилых, а также беженцев;
- избегать идентификации родственников и друзей заложников и потенциальных жертв без их согласия;
- помнить, что спасение раненых и пострадавших, а также освобождение заложников и предотвращение дальнейших жертв имеет приоритет перед правом информирования общественности;
- собирать, анализировать и сопоставлять информацию из всех возможных источников, согласовывая свои действия с правоохранительными органами только в том случае, если в результате действий журналиста жизнь и здоровье заложников, потенциальных жертв и других затронутых лиц могут быть защищены;
- не брать на себя роль посредника между террористами и правоохранительными органами;
- не предлагать участникам контртеррористической операции предпринимать какие-либо действия для получения удачных видео- или фотокадров;
- не брать интервью у террористов во время совершения ими террористического акта;
- незамедлительно предать гласности ставшую ему известной информацию о готовящемся террористическом акте или об иной угрозе, исходящей от террористов.

Журналист должен быть особенно аккуратен и осторожен в подаче материала о террористическом акте и контртеррористической операции! Вот почему он должен:

- стараться не стать рупором для выражения взглядов и программы действий террористов, памятуя о том, что акты терроризма никогда не могут быть оправданы никакими мотивами;
- избегать прямой трансляции интервью с террористами, в том числе по той причине, что такая трансляция может быть использована террористами для передачи тайных сигналов своим единомышленникам, находящимся вне зоны контртеррористической операции;
- стремиться к тому, чтобы его изложение требований террористов было свободно от риторики и пропаганды терроризма; в частности, желательно, чтобы эти требования были перефразированы журналистом и сопровождены соответствующими правовыми комментариями;
- пытаться сохранить баланс между правом аудитории СМИ знать прав-

ду о подробностях террористических актов и правом обвиняемых в терроризме на беспристрастный суд;

- сопровождать сообщения о террористических актах точной информацией о фактической подоплеке событий; такие факторы как раса, вероисповедание, национальность или занимаемое положение террористов и их жертв следует сообщать только в тех случаях, если они имеют существенное значение; при этом нужно учитывать, что мировое сообщество отвергает связь терроризма с какой-либо конкретной религией, религиозной верой или национальностью, тогда как нетерпимость, дискриминация, неравенство, невежество, нищета и отчуждение наряду с прочими явлениями служат плодородной почвой для международного терроризма;
- учитывать тот факт, что в целях искоренения терроризма мировое сообщество нуждается в глобальном и всеобъемлющем видении развития, базирующегося на соблюдении прав человека, взаимном уважении, межкультурном диалоге и уменьшении нищеты на основе справедливости, равенства и солидарности;
- воздерживаться от неподобающей сенсационности и натурализма при показе жестокости и насилия со стороны террористов, уважая нравственные и религиозные чувства представителей аудитории СМИ и, прежде всего, проявляя должное уважение к страданиям жертв терроризма и чувствам их близких, дабы не усугублять их бестактным освещением событий;
- воздерживаться от публикации мемуаров террористов, если это может содействовать оправданию или преуменьшению значения терроризма;
- защищать право общества быть информированным обо всех существенных для него сторонах терроризма и борьбы с ним, исходя из того, что не основанный на законе и не являющийся необходимым в демократическом обществе запрет на публикацию информации неприемлем.

При работе в зоне проведения контртеррористической операции журналист должен принять необходимые меры по обеспечению собственной безопасности! Вот почему он должен:

- поставить в известность руководителя контртеррористической операции о своем намерении освещать события;
- иметь при себе и по первому требованию предъявлять редакционное удостоверение или иной документ, удостоверяющий личность и полномочия журналиста в зоне проведения контртеррористической операции;
- стараться укрыться при перестрелке; не разгуливать в зоне видимости террористов, так как даже в оптический прицел снайпер может не отличить журналиста от участника контртеррористической операции, либо, напротив, выслеживать именно представителя СМИ;
- не брать в руки оружие и не надевать камуфляжную или иную униформу, используемую участниками контртеррористической операции, за ис-

ключением случая, когда террористы атакуют участников контртеррористической операции и могут захватить журналиста; в этом случаев журналист вправе самостоятельно решать свою судьбу и, либо попытаться остаться нейтральным наблюдателем, либо взять в руки оружие и вступить в бой;

- в случае захвата в заложники немедленно заявить о своей профессиональной принадлежности, не обещать выкуп, постараться передать в редакцию пленки и видеозаписи, сделанные в ходе работы, чтобы информация о захвате журналиста как можно быстрее дошла до редакции и правоохранительных органов.

1.8. Медійні війни в Україні та світі: сутність, методи та засоби здійснення

Зважаючи на роль інформації у сучасному світі, американський дослідник М. Маклюен виводить цікаву тезу, яка звучить так: «Істинно тотальна війна — це війна за допомогою інформації».

Мета інформаційної/медійної війни - послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Очевидно, що інформаційна війна — складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх здійсненні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до них. Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням цілком співмірні, а часом і перевищують наслідки збройних війн.

Що ж таке інформаційна/медійна війна, як саме науковці пояснюють таке явище в сучасному світі?

Відомий науковий дослідник інформаційфних/медійних війн Д.М. Прокофьев визначає інформаційну війну як дії, розпочаті для досягнення інформаційної переваги шляхом руйнації, модифікації або спотворення інформації чи несанкціонованого проникнення в інформаційні системи супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації та інформаційних системах. Основні методи інформаційної війни — блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника.

Інформаційна/медійна війна розглядає інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну/медійну війну можна розглядати як якісно новий вид бойових дій, активна протидія у інформаційному просторі. Інформаційна війна — це атака інформаційної функції, незалеж-

но від засобів, які застосовуються.

У веденні стратегічних інформаційних війн застосовується специфічна зброя. Ця зброя не наносить фізичної шкоди але може призвести до справжньої війни.

Інформаційна/медійна зброя — сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій або служб інформаційної інфраструктури в цілому або окремих її елементів. Основна дія інформаційної зброї — бокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника.

Можна зазначити, що багато з сучасних війн починається саме з інформаційних. Приводом для бомбардування Багдаду Сполученими Штатами стала поширена через усі світові ЗМІК інформація, що режим Саддама Хусейна нібито має зброю масового знищення. Війна в Іраку триває, а зброю так і не знайшли. Війну інформації також розпочинають тоді, коли треба досягти якоїсь мети. Експерти висувають різні версії, щодо справжньої мети нападу на Ірак. Головна — метою знищення Іраку була зовсім не зброя масового ураження, а велика кількість нафти, яку прагнув взяти під свій контроль американський уряд чи просто давні непорозуміння родини Бушів з Саддамом Хусейном. Тільки раніше приводу не було розпочати цю війну, треба було людству якось пояснити таку позицію, довелося провести цілу низку виливів інформації на маси, таким чином виправдати позицію американського керівництва.

Зрозуміло, що інформаційні війни частіше використовуються на міжнародному рівні. Україна і Росія вже не один рік ведуть саме таку війну. Росія постійно провокує гучними заявами український уряд та і просто зневажливо ставиться до українців у своїх інформаційних матеріалах. То Україна краде газ, то українців називають малоросами, або ж всі українці продалися американцям. І що дивно — це працює! Росіяни — братній народ, потроху починає ненавидіти українців. І якщо на початку цієї війни пересічним громадянам було байдуже, то зараз зневажливе ставлення проявляється не лише на рівні керівництва, а і на рівні мас.

Що стосується інформаційних війн місцевого масштабу, то такі війни точаться не лише між країнами і охоплюють міжнародну аудиторію, такі війни починають вести і на місцевому рівні. Зокрема, українські політики, як нікоди, вивчили технологію ведення інформаційної війни.

Останнім часом дедалі популярнішим серед українських політиків стає знищення опонента за допомогою інформаційних бомб. Одну з таких колись викинула Юлія Володимирівна Тимошенко, коли заявила, що Партія Регіонів підписала коаліційну угоду з Нашою Україною. Знаючи електорат НСНУ, зрозуміло, що таке рішення на ура не пройде і, що саме завдяки такому злиттю партія загубить більшу частину своїх прихильників, бо вони просто не зрозуміють такого об'єднання. Можна сказати, що людина, яка має такий вплив

на українські маси, зробила стратегічний хід, завдяки якому змусила розчаруватися деяких українців у своїх лідерах і прибільшила кількість прихильників у своїх лавах.

І якщо розібратися в суспільних процесах, то можна зрозуміти, що третя світова вже давно почалася. І що вона набагато страшніша, бо знищення відбувається завдяки інформації. І, якщо кулі і снаряди відомо звідки летять, то інформаційні бомби з'являються несподівано і в невідомому місці, і іноді відбити таку атаку взагалі неможливо. І чомусь саме інформаційним потокам маси довіряють більше. А маючи у руках таку зброю і хоч невеличке вміння впливати на аудиторію, можна завоювати світ. Напевно, що й «солдатам» стала вже не цікавою війна зі зброєю у руках, інформаційна війна – жорстокіша і цікавіша. В такій війні рідко конкуренти «виживають».

Як стверджує фахівець з інформаційних/медійних війн Ю.Бабенко, війна інформації на сьогодні стала одним з найнебезпечніших видів зброї. Користуватися компроматами, "*виливанням бруду*", "*підкиданням*" неправдивої інформації, намагання за допомогою інформації ввести в оману стало для багатьох сенсом життя. Інформація має вплив на маси, тобто за умови *вдалого маніпулювання свідомістю* мас, можна досягти практично будь-якої мети – знищити опонента, прибрати з дороги конкурентів чи розпалити війну, як це було з Іраком.

Що ж, журналісти тримають у руках зброю, тільки не завжди використовують її за призначенням. На тлі останніх подій, які відбуваються в Україні можна зрозуміти, що основна боротьба між політичними силами відбувається за допомогою інформації, тобто в країні почалася інформаційна війна...

США *починають* "*інформаційну війну*", яка буде частиною операції проти терористів. Телекомпанія Ен-бі-сі навела висловлювання неназваного представника міністерства оборони США, який не виключив, що у відносинах зі ЗМІ американській владі доведеться вдатися до дезінформації. "Це буде найбільш інформаційно інтенсивна війна, яку тільки можна уявити", — заявило пентагонівське джерело.

Представник Пентагона повідомив, що противники США також будуть *забезпечувати пресу явно помилковою інформацією*. "Якщо це інформаційна війна, то "погані хлопці" також будуть брехати", — попередив він.

Американські ЗМІ вже помітили, що останнім часом в США різко поменшав обсяг інформації про операцію, яка готується проти терористів. Спостерігачі чекають, що найближчим часом з боку влади контроль за відомостями, які передаються у пресу, ще більше посилиться.

Прес-секретар Білого дому А. Флейшер особисто звернувся до керівників і головних редакторів усіх *провідних ефірних телекомпаній* США, газет "*Нью-Йорк таймс*", "*Вашингтон пост*", "*Уолл-стріт джорнел*" та інших ЗМІ з проханням не повідомляти жодних подробиць про військову операцію, яка готується США проти терористів.

Як стало відомо "Вашингтон пост", Флейшер просив також керівників ЗМІ про те, щоб телекомпанії і газети не повідомляли про графік роботи і переміщень президента США Джорджа Буша і віце-президента США Річарда Чейні. Керівників ЗМІ, крім того, попросили не передавати даних про заходи безпеки навколо Білого дому. Розголосу тепер не підлягають і новини про джерела і методи збору розвідувальної інформації, яку США отримують для операції проти терористів.

За даними газети, на цьому тижні керівництво прес-служби міністерства оборони США збирається знов зв'язатися з провідними американськими ЗМІ і провести зустрічі із завідуючими їхніх вашингтонських бюро.

В Афганістані "*Талібан*" заборонив співробітникам ООН користуватися комп'ютерами, автомобілями і засобами радіозв'язку. В іншому разі їх чекає смертна кара. Як передає АР, ці погрози відносяться лише до співробітників-афганців, оскільки всі іноземці, які працювали в представництвах ООН, покинули Афганістан. Проте, в Організації стурбовані таким розвитком подій. Поки що співробітникам офісів ООН в Кабулі і Кандагарі рекомендовано виконувати розпорядження талібів, щоб не наражати своє життя на небезпеку.

Оскільки саме поняття "*цивілізації*" містить значну інформаційну складову, то кожен конфлікт суспільств із різними цивілізаційними (або нижчого рівня) цінностями неодмінно включав елементи інформаційної війни. Однак на початках цивілізацій і до закінчення середньовіччя суспільства на підкорених територіях (чи ті, які планували підкорити) розглядали як відновлюваний ресурс території і ніколи як інформаційне середовище. Інформаційні зіткнення суспільств, звичайно ж, відбувалися, але процес інформаційної боротьби був стихійним, сторони його не усвідомлювали.

Оминаючи перехідний період, в якому відбувалося усвідомлення того, що інформація подекуди є зброєю, потужнішою від гармат, можна сказати, що всі конфлікти минулого століття мали потужну інформаційну складову. Багато прийомів інформаційної війни, яка, схоже, стає головним театром дій у глобалізованому світі, відпрацьовані саме тоді – інша річ, що вони не систематизовані та не описані в підручниках для новітніх військових училищ, які мали б готувати командирів для цього поля бою. Іронічна посмішка недовірливих недоречна – Сполучені Штати, які мають нині абсолютну військову перевагу в зброї шостого покоління чи над будь-якою державою світу, чи над найнеймовірнішим союзом держав, добре усвідомили недостатність цієї переваги в сучасному світі.

Аналіз діяльності американських спеціальних операційних сил (SOF) показав, що найпотужніша у світі держава не в змозі ефективно використовувати їх без застосування інформаційної зброї. Тому 30 жовтня 2003 року міністр оборони США Дональд Рамсфелд підписав "дорожню карту інформаційних операцій" (IO Roadmap) для міністерства оборони США. Вона визначила інформаційні операції як "інтегроване використання можливостей

електронної зброї, комп'ютерних мережевих операцій (CNO), психологічних операцій (PSYOP), операцій із військової дезінформації і дезорганізації та операцій безпеки (OPSEC) для використання можливостей впливу на людську свідомість із метою руйнування, розкладання або й узагалі перехоплення впливу на ухвалення рішень противника, при цьому захищаючи наше власне, (рішення)". Якого ще доказу потрібно, щоб довести, що інформаційна війна — це не фантастика, а реалії сьогодення?

Шкода, але ні чинна українська влада, ні суспільство загалом чи частково не сприймають події від помаранчевої революції й донині як велику інформаційну воєнну кампанію. У кращому разі "інформаційною війною" називають окремі сутички цієї кампанії — наприклад, пов'язані з газовим конфліктом або маяками. Найгірше, що всі ці бої місцевого значення розглядають відокремлено від безперервної інформаційної війни, одне від одного та від помаранчевої революції (яка, по суті, була великою битвою цієї війни, важливою битвою, але аж ніяк не всією війною). Крім того, їх розглядають на найпростішому рівні операцій, які годилося б називати словом "пропаганда". Водночас росіяни, попри вразливість їхніх власних позицій, у боротьбі з Україною сповна використовують те, що експерти Рамсфелда назвали "використання можливостей впливу на людську свідомість із метою руйнування, розкладання або й узагалі перехоплення впливу на ухвалення рішень противника". Відсутність повноцінного розуміння національною елітою та нацією загалом пріоритетності такого поняття як "національна солідарність", наявність такого чинника як вибори дозволяє їм ефективно здійснювати кампанію дезінформації та дезорганізації в лавах українських політиків, урядовців, просто громадян.

Чи може Україна встояти в цій безперервній війні за збереження свого "*Я*"? Безумовно! Перебіг помаранчевої революції, аналіз окремих інформаційних сутичок у ній і засобів, які використовували сторони, свідчить, що асиметричні дії українських "інформаційних партизанів" (на жаль, не можна знайти іншого терміну, позаяк діюча в той час влада аж ніяк не стояла на боці питомих українських інтересів) ефективно зруйнували російський план, нейтралізували російські інформаційні удари, а подекуди й дезорганізували роботу російського штабу.

Це стало можливим винятково тому, що для мобілізації українців наша сторона мала два креативи фундаментального значення: права людини і права нації. Будуючи національний опір на цих двох фундаментальних поняттях, які мають у своїй основі чи не первинні інстинкти живої істоти, українська сторона звела нанівець російський план, під який було задіяно чималі засоби і який насамперед покладався на домінацію росіян в апаратних засобах інформаційного простору України.

Інформаційні війни велися й будуть вестись. CNN та «Аль-Джазіра» ніколи не будуть однаково висвітлювати події в Іраку. Але чому завжди знаходяться ті, хто безсоромно кидає каміння у власний народ? Ворог може викликати повагу, але зрадник — лише зневагу.

Викладене вище дозволяє зробити висновок, що якщо Україна хоче стати незалежною державою, вийти на рівень європейських держав, то вже сьогодні необхідно вирішувати ряд проблем у галузі інформаційної безпеки. Головними з них, на наш погляд, є :

- створення системи підготовки та перепідготовки кадрів, включаючи кандидатів та докторів наук;
- організація та координація наукових та дослідно-конструкторських робіт в галузі інформаційної безпеки;
- створення національних стандартів та контролю якості діючих стандартів, включаючи криптографічні системи;
- розгортання національної конкурентоспроможної промислової бази в галузі захисту інформації;
- створення системи експертизи та сертифікації систем та засобів захисту інформації тощо.

Сьогодні процес інформатизації суспільства, його державних та суспільних інститутів, розвивається стрімко і як правило непередбачено і некеровано [202-204]. Суспільство, на наш погляд, з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки впливу високих технологій на власну життєдіяльність.

Основними складовими захищеного інформаційного простору держави можуть бути:

- національна інформаційна інфраструктура (НІІ) з відповідними показниками захищеності;
- національна оборонна інформаційна інфраструктура (НОІІ);
- елементи та засоби Глобальної інформаційної інфраструктури (ГІІ).

Очевидно, що основними об'єктами інформаційної війни, по суті мішенню інформаційної зброї є і будуть НІІ та ГІІ. В цілому об'єктами застосування інформаційної зброї можуть бути виробництво, силові відомства, зв'язок, транспорт та енергетика, фінанси, наука та освіта, засоби масової інформації та інше. Але в першу чергу інформаційна зброя буде націлюватись на розв'язання суперечок в економічній, політичній та ідеологічній областях, ця зброя буде націлюватись на збройні сили, підприємства оборонного комплексу, силові структури, відповідальні за безпеку держави. При цьому імовірніше всього, що найбільший розвиток та використання інформаційна зброя знайде в економічній області – шпигунство через електронні системи, знищення та підробка інформації, введення в оману та інше – реалії сьогоднішнього дня. В таких складних умовах вижити може тільки держава, яка створить і буде повсякчасно покращувати якість національної оборонної інформаційної інфраструктури.

Сьогодні Україна стала відкритою в інформаційному відношенні державою, уже сьогодні вона підключилась до Глобальної інформаційної інфраструктури (системи Інтернет, Глобалстар, GSM та інші), володіє замкнутими інформаційними системами низького рівня. Вказане робить Україну особливо вразливою інформаційною зброєю. Тому створення та безперервне вдоскона-

лення систем та засобів захисту інформаційної інфраструктури України, створення оборонної інформаційної інфраструктури, є першочерговою задачею, вирішення якої забезпечить національну безпеку України.

Чи має Україна шанси в цій війні нового тисячоліття? Якщо йдеться про протистояння з Кремлем, то безумовно! Головною проблемою росіян у намаганні здійснити план "*ліберальної імперії*" є відсутність єдиної ідеї, здатної працювати в усіх цільових групах їхнього суспільства. Держава, позбавлена інформаційного запілля, дуже вразлива навіть на власні засоби інформаційної/медійної війни. Врешті, таким є висновок американців після трьох років досвіду PSYOP: їх застосування нагадує зарин, який може уразити навіть "*своїх*". Окрім того, під час газової війни росіяни створили кілька стійких понять, які створюють велику небезпеку для РФ як цілісної держави.

Віднині європейці знають, що Росія може використовувати газ як важіль економічного і політичного тиску. Вони також знають, що для збільшення рівня власної безпеки треба диверсифікувати джерела постачання газу. Вся небезпека проблеми для росіян у тому, що диверсифікувати постачання можна не лише в рамках сучасного світового ладу — будь-який лад є тимчасовим явищем. Диверсифікувати можна і на території існуючої держави, якщо її спіткає доля СРСР. Розпад Росії став явищем, економічно вигідним для Європи, — і це найгірший для Москви наслідок газової війни. Звичайно, дипломати та державні особи говоритимуть чемності та заперечуватимуть причетність своїх держав до тих чи інших подій у нестабільних регіонах.

РОЗДІЛ 2

МАНІПУЛЯТИВНІ ТЕХНОЛОГІЇ В МІЖНАРОДНИХ ВІДНОСИНАХ

2.1. Манипулятивные стратегии XXI столетия

На рубеже столетий, тем более тысячелетий, стало традицией обращаться к сакраментальным проблемам человеческого бытия, судьбам страны и мира, стремиться вписаться в этот исторический интерьер. Не многим поколениям такое дано. И воистину, это время необходимо сполна использовать для того, чтобы выйти за пределы обыденности, соприкоснуться с вечностью и ощутить глобальность пространства, постичь их смысл.

В такие периоды закономерно тяжесть основных свершений ложится на избранных. Соединенные Штаты Америки зримо и сполна это ощутили уже на одиннадцатый день девятого месяца третьего тысячелетия. Немного ранее чашу сию испили Балканы - некогда райский уголок Европы. До этого было падение последней тоталитарной империи. И поныне геостратегические и геоэкономические силы, под натиском которых пал СССР, во многом определяют пути внутреннего развития государств-осколков, особенности и характер их внешней политики.

Формирующийся общий мир манит и соблазняет "потерпевших" и от глобального натиска, и от мирового терроризма. Идет формирование нового мирового порядка, когда и былые заслуги могут абсолютно не приниматься во внимание. И сакраментальный выбор нового времени состоит в том, продолжить ли слепо отдаваться воле глобальной судьбы или же осознанно принять вызов и заняться поиском собственных путей развития.

Конец ушедшего тысячелетия, казалось, очертил основные контуры будущего мироустройства, ведущие направления и тенденции всемирного развития, перспективы доминирования западной цивилизации и возможные ответные реакции Востока. Процессы формирования нового мирового порядка обозначились стремлением Запада обособиться в элитарном клубе себе подобных — уповающих на мощь денег и святость правопорядка, расчетливых, преклоняющихся перед торговыми балансами и финансовыми показателями, но в высшей мере — перед Вещью. Коммерческий расчет и выгода оказались заложены не только в фундамент Всемирной торговой организации, которая, по сути, определяет этику современной мировой политики (а она-то сегодня все больше походит на торг), но и в основу формирующейся общеевропейской идентичности. На откровенном расчете и двойных стандартах строился и "западный гуманизм", реализуясь в экзальтированном виде в форме так называемых "гуманитарных интервенций".

Существенной составляющей нового мироустройства виделась инновационная ориентация хозяйственной деятельности, как ключевой фактор постиндустриального развития. Но как оказалось, инновационная активность имела свою как реальную, так и виртуальную составляющую. С одной стороны, она синхронизировалась с известными кондратьевскими экономическими циклами (с определенным сдвигом). Вероятно, она стала проявлением

прорыва на новый уровень технологий вследствие общественно-производственной унификации, стимулированной процессами глобализации или же своеобразной реакция технократии, стремящейся выжить в быстро меняющейся природной и социальной среде. С другой стороны, эффект лопнувшего "мыльного пузыря" "новой экономики" означил и целый пласт наносного, связанного с системой "виртуальной отчетности".

"Теневая" сторона научно-технического прогресса засветилась и в других сферах. Мир вещей, техники, технологии и научных парадигм опутал своими сетями живую человеческую природу и, похоже, для некоторых даже стал ее "желанной" компонентой. Збигнев Бжезинский небезосновательно полагает, что человечество находится на грани "спонтанного использования растущих возможностей науки для улучшения, переделки и создания человеческой личности. В итоге может возникнуть новое неравенство в условиях жизни, которое будет выражаться не неравенством в доходах, а неравенством в органических условиях жизни".

Предыдущий Папа римский Иоанн Павел II был более критичен в своих предвидениях: "Технические средства, которыми располагает нынешняя цивилизация, несут не только возможность самоуничтожения человечества в результате военного конфликта, но также возможность "мирового порабощения" отдельного человека, социальных групп, целых обществ и наций".

Одной из проявляющихся ныне особенностей процесса вхождения мира в информационную фазу развития стала всеобщая виртуализация общества — его тотальное погружение в искусственно конструируемые виртуальные текстовые, смысловые поля, иллюзорную сферу чувств и эмоций. Фактически на наших глазах раскручивается сценарий развития цивилизации, многократно описанный фантастами как бунт киборгов против людей, к тому же многократно усиленный возможностями клонирования человеческой плоти.

По сути, ареной развернувшейся борьбы стала личность и человеческое сообщество. Вызревший в их недрах технотронный монстр уже стремится подчинить человеческую сущность, вогнать ее в лоно покорной зависимости от техники и технологии. Посредством так называемых "гуманитарных" технологий индивидуальное и общественное сознание может быть расколото, чтобы потом искусственно создавать самые невероятные социальные химеры, продавая их оптом и в розницу новоявленным Мефистофелям. А заполнивший СМИ "черный PR" — стал только "цветочками" технократического разложения личности. Мир означил неумолимое движение к своему Апокалипсису, когда "мертвые будут судить живых".

На этом фоне главенствующая в политике либерально-демократическая парадигма уже в конце столетия выглядела реальным анахронизмом. Для президентов, премьеров, генералов и рядовых, элиты и просто граждан стран западного мира - это фетиш, который с мессианским фанатизмом проецировался (да и продолжает по инерции проецироваться) на весь мир. Ею "пропи-

тано" современное западное бытие и сознание, ее яркий антураж ослепляет и бесконечно репродуцируется в образцах поведения кумиров, массовой культуре и масс-медиа. Стало уже расхожим международным ритуалом для одних заверять в приверженности демократическому выбору, для других — постоянно требовать доказательств в подтверждение этого.

Подобную живучесть и экспансионизм либеральной иллюзии можно объяснить разве только тем, что она паразитирует на самом "духе свободы". А он-то и живуч, и притягателен, и жизненно необходим. Только личность, а тем более общество, сформировавшиеся как свободные, без принуждения и насилия, способны и к эффективной конкуренции, и к полноценному сотрудничеству.

Теракты 11 сентября 2001 г. стали, с одной стороны, закономерным проявлением накопившейся в мире критической массы деструктивности, с другой, - спусковым крючком, запустившим механизмы глобальных общественных трансформаций.

Масса журналистских изысканий, экспертных оценок, обращений к историческим аналогам, эмоционально накаленных политических заявлений, сводок о военных приготовлениях, обрушившихся на ошарашенное мировое сообщество после 11 сентября, создали плотную стену "белого ментального шума", которая отгородила массовое сознание от ответов на сакраментальные вопросы. И, прежде всего, о тех, кому оказалась выгодной начавшаяся кампания террора, о целях ее "застрельщиков" и реализуемом ими проекте будущего мироустройства. В сложившейся ситуации эти знания являются, пожалуй, ключевыми.

НАТО в своем решении от 12 сентября особо отметило, что террористическое нападение на США будет рассматриваться как такое, что подпадает под действие статьи 5 Вашингтонского договора, если будет доказано, что оно "совершено из-за границы". Тем самым Вашингтону была дана подсказка, где искать врага, дабы рассчитывать на консолидированную поддержку партнеров. Возможно, это послужило дополнительным стимулом для американцев спешно конструировать безальтернативную картину внешней угрозы с традиционным арабско-мусульманским следом, ведущим к главному заказчику — Усаме бин Ладену. Формальные доказательства, необходимые для оправдания последующих боевых акций, нашлись уже в результате их проведения. Но сама первоначальная американская трактовка происшедшего, а особенно презентация ответных действий, то ли в виде "нового крестового похода", то ли актов "безграничной справедливости", оставила больше вопросов, чем прояснила суть дела.

Чтобы пролить немного света на тайные механизмы террора и его жрецов, попытаемся взглянуть на происходящее через призму психотехнологической насыщенности событий, прямо или косвенно относящихся к 11 сентября. Нет особой необходимости доказывать, что в современных условиях именно психоинформационные технологии составляют основной инструментарий для

конструирования мировой политики. А их проявление свидетельствует о следе "сильных мира сего" или тех, кто с ними был в тесном контакте.

Первая эмоциональная реакция на происходящее, зачастую, несет наиболее значимые его оценки. Президент США Джордж Буш (из обращения к нации 11 сентября): "Эти акции массового убийства были призваны запугать нашу нацию, вызвать состояние хаоса и отчаяния". Тогдашний посол США в Украине Карлос Паскуаль (из интервью "Зеркалу недели"): "Я не должен поддаться тому страху, который мне пытаются навязать террористы. Я отказался верить в то, что они могут разрушить мою жизнь". Президент и посол достаточно точно отразили то, что составляет сердцевину террора. Его кульминация — ужас, охватывающий и подавляющий широкие массы. Но и само устрашение в большинстве — еще не цель, а только средство для навязывания определенной линии поведения, образа мыслей и способа действий.

В этом контексте современный западный социум представляет собой "благодатную" почву для возделывания страхом. Еще до известных событий американский психолог К. Изард провел исследование, в котором изучалось отношение представителей ряда развитых стран (США, Англии, Германии, Швеции, Франции, Греции и Японии) к различным эмоциям. Большинство опрошенных в ответ на вопрос: "Какой эмоции вы больше всего боитесь?" назвали страх. Одно из лидирующих мест в этом опросе заняли американцы: половина женщин и треть мужчин назвали страх доминирующей в их жизни мучительной эмоцией.

Фактически страх, как специфическое переживание и поведение, проистекающее из ожидания угрозы или опасности, входит в число системообразующих черт современного американского общества (страх лишиться работы, имущества, остаться без денег, страх уличного насилия, сексуального домогательства и т.п.). Вытесненный глубинный страх, желание обезопасить себя любой ценой лежат в основе большинства важных выборов, совершаемых американцами, определяет общий эмоциональный фон и сущность всей системы общественных отношений, а институты безопасности составляют фундамент государственного устройства.

Похоже, об этих особенностях американского социума было хорошо известно инициаторам терактов в Нью-Йорке и Вашингтоне. Эти лица, без сомнения, осведомлены о действии основных естественных активаторов страха, в число которых входят боль и восприятие боли других людей, необычность события и объекта и т.п. Была принята в расчет и специфика функционирования американских масс-медиа, "зацикленных" на интерактивности, стремлении донести до потребителя живую картинку, какой бы жуткой она ни казалась. Похоже, что 11 сентября мир столкнулся не только с невиданной по размаху и степени варварства акцией устрашения, но и с беспрецедентной по цинизму и тонкости расчета манипуляцией общественным сознанием.

Страх — самая токсичная и самая пагубная эмоция. Ужас как крайнее проявление страха сопровождается чрезвычайно высоким уровнем возбуж-

дения нервной системы, что заставляет организм работать на грани срыва. В умелых руках манипулятора возникший массовый психоз канализируется в "управляемый хаос", создает предпосылки для радикальных общественных трансформаций в заранее означенном русле. Он может быть превращен и в гнев, когда перепуганному народу указывают на "истинные" источники опасности.

В процессах такого массового внушения всесильным становится тот, чей голос доходит до большинства в краткий период массового шока. Поэтому после традиционного теракта осуществившая его сила пытается как можно быстрее донести смысл своих требований и установок до массовой аудитории, привлекая к себе внимание масс-медиа. И в этом принцип "свободы слова", как никогда, работает на террористов — им-то и предоставляется приоритет в доступе к микрофону.

В событиях 11 сентября многих удивило то, что никто не взял на себя ответственность за теракт. Коль так, то "застрельщиков" необходимо искать за теми силами, которые наиболее активно пытались навязать свое мнение шокированной Америке. В разноголосом хоре четко выделялись две тематические линии:

- арабско-мусульманского терроризма, с указанием широкого спектра "врагов" в лице "государств-изгоев";
- неспособности существующего либерально-демократического режима обеспечить защиту американских граждан.

Таким образом, вероятнее всего, "застрельщиками" терактов Америка априори программировалась вовне на конфликт с арабским миром, и как следствие усиление милитаристских приготовлений, внутри - на ужесточение порядка и сворачивание демократических свобод. По сути, этот сценарий и реализовался впоследствии в оккупации Афганистана и Ирака.

Почерк провокации всегда в достаточной степени узнаваем. В этой связи можно вспомнить подноготную Освальда, "назначенного" убийцей Дж.Кеннеди. В свое время тот эмигрировал из США в СССР, и длительное время проживал там, после чего попросился обратно в Америку. Закономерно, что он был завербован КГБ, чего, впрочем, особо и не скрывал в своем американском окружении. После ареста Освальда, в отношении которого уже формировался имидж "советского агента" - убийцы американского президента, только молниеносная реакция советского руководства, незамедлительно представившего американцам все материалы его агентурной разработки, способствовала восстановлению доверия между двумя странами и отодвинула мир от мировой катастрофы.

Наиболее серьезным вызовом 11 сентября для американской администрации Дж. Буша стала демонстрация неспособности правительства, всей военной и правоохранительной машины государства (как известно, армия, спецслужбы и военно-промышленный комплекс являются основной опорой американского президента) защитить население от "неведомой" угрозы. Бо-

лее того, страх, посеянный посредством "белого порошка" в рядах вашингтонских парламентариев и чиновников, заставил их быть намного сговорчивее с властью. В итоге произошел стремительный рост доверия американцев к Бушу.

У нынешнего страха терроризма есть еще одна откровенно американская особенность — он жестко пронизал всю мировую финансовую систему. Теперь благополучие доллара определяется не столько экономическим потенциалом Америки, сколько уровнем страха его "уронить".

Как оказалось, в социокультурных запасниках американской нации по всем ведущим позициям не оказалось более действенного инструмента общественной мобилизации, чем страх. В связи с этим вспоминается разговор с Самуилом Хантингтоном. На замечание, что американская нация, если она претендует на мировое лидерство, должна быть носителем своеобразной "суперкультуры", одним из существенных элементов которой являются механизмы сверхмобилизации в условиях смертельной опасности, возражение метра было жестким: "но ведь это — тоталитаризм".

Сегодня глобальный страх подталкивает США, а вместе с ней и весь западный мир, к мобилизации ригидного образца — попыткам выстроить несоразмерно огромную систему контроля и самоизолироваться от опасных с их точки зрения регионов мира. Повсеместно принимаются законы, идущие в разрез с постулируемыми либеральными ценностями.

Ставки в начавшейся 11 сентября Игре высоки. Мир возопил о грядущей глобальной катастрофе. И в качестве основной версии активно раскручивается хантингтонская идея конфликта цивилизаций. Но, похоже, что межцивилизационные противоречия являются разве что горючим для поддержания высокого накала конфликтности. В горниле этого конфликта и идет приготовление "нового глобального элитарного социального сплава, легированного страхом", который адекватно отвечал бы новому миропорядку. Цена такого действа — Господство над миром.

По сути, то, что представляется ныне глобализацией, и есть большая игра, где задействованы сотни миллиардов долларов. Эти деньги постоянно вращаются на столе большого мирового казино, подминая под себя страны и целые регионы. И при принятии решения в расчет принимаются, прежде всего, великие символы. Всякие "мелкие", с точки зрения этих игроков, проблемы - интересы, судьбы стран и народов, людские жизни в этой игре уже мало что значат, отходя на отдаленный план. Главное - сам процесс с его процедурами и системой формальных признаков. Именно такого рода молох и стремиться распространить свою власть над миром.

Современный уровень развития ядерных, психо-, нано-, био- и иных новейших технологий поставил мир перед дилеммой: человечество должно повзрослеть или исчезнуть. Повзрослеть для Америки — это отказаться от подростковых игр в "Креатура", безоглядно, по своему усмотрению манипулирующего предметной и человеческой реальностью, формирующего произ-

вольные социальные организмы и государства-гомункулы. Уроки трагедии в Ираке прямо указывают на это.

Для остального мира повзрослеть — значит самоопределиться, осознать ущербность и опасность пребывания в инфантильном зависимом состоянии, перепоручая одной стране, пусть даже невероятно технологически развитой, всю полноту ответственности за судьбы мира.

Начавшиеся глобальные процессы антитеррористической консолидации, по сути, только очертили те мировые тенденции, которые нарастали в последние десятилетия прошлого века. В качестве прогрессирующей идеологии, традиции, основы разработки современных социальных технологий, фундамента формирования нового мирового уклада в мире устойчиво утверждается корпоративизм. Он вездесущ, реализуясь в разных ипостасях — региональной интеграции, политических союзах, социальном партнерстве, усилении корпоративных начал в экономике.

В формирующемся едином мировом экономическом пространстве основными действующими лицами становятся не государства, а транснациональные корпорации, в среде которых идут процессы активного слияния и поглощения. Мерилом эффективности работы компаний все более становится не величина прибыли, а степень охвата рынка. Интернет стремительно накрывает планету своей "паутиной", создавая глобальную среду для взаимодействия. Проведение торговых и расчетных операций в международной компьютерной сети изменяет саму структуру бизнеса.

В мировой политике начинают доминировать союзы, альянсы, коалиции и консорциумы. На корпоративных принципах (а, по сути, в рамках жесткого безальтернативного выбора - "кто не с нами, тот с террористами") идет строительство США антитеррористической коалиции. НАТО и Европейский Союз, хотя формально и придерживаются при принятии важных решений принципа консенсуса, фактически в своей деятельности все больше руководствуются жесткими корпоративными принципами. И в этом они остаются более действенными, чем ООН, организация, принципиально придерживающаяся "консенсусных" начал. Жесткая реакция французского президента на особую позицию вновь принятых в ЕС восточно-европейских стран по вопросам поддержки США в войне с Ираком стало наглядным примером вразумления "неофитов" по поводу необходимости поддерживать "корпоративный дух Евросоюза". Европа в ходе последней балканской войны "поступилась" своими этическими принципами в пользу применения силы из корпоративной солидарности, а боевые действия активно покрывались "коллективной ответственностью".

В политической сфере большинства постсоветских стран властно хозяйничают отраслевые, силовые и региональные структуры и кланы. Феномен российских олигархов — результат эффективной реализации корпоративных технологий в бизнесе в сочетании с использованием властных и информационных рычагов. В политике сегодня закончилось время одиночек, и

рассчитывать на успех можно только в рамках мощных финансово-политико-информационных корпораций.

Однако мировым "демократическим бомондом" наложено негласное табу на корпоративизм. О нем до последнего времени не говорили с трибун представительных мировых конференций, молчат МВФ, Всемирный банк и сонм западных советников, наводнивших постсоветское пространство. В таком молчании Запада сквозит затаенный умысел — нежелание делиться с "диким" Востоком ноу-хау, которые сегодня ложатся в основу современных технологий экономического и социального управления. Вместо этого мы слышим старую песню о свободах и правах, частной собственности и приватизации.

Вместе с тем можно понять европейцев, которые тяготятся воспоминаниями о корпоративном государстве Муссолини, воспроизведенном впоследствии в расширенных масштабах Гитлером. Да и сталинский режим иначе как "колхозным" (т.е. все тем же коллективистко-корпоративным) не назовешь. Энтузиасты идеи пытаются как-то выкрутиться, подыскивая замены типа неокорпоративизм или корпоративизм, что сути не меняет. Ситуация весьма напоминает ту, которая сложилась в СССР вокруг геополитики, опять-таки в силу активного использования ее доктрин фашистским режимом.

Однако в такого рода подобии есть и более глубинная взаимосвязь. По сути, и корпоративизм, и геополитика основываются на приоритетности коллективного начала, положенного в фундамент организации общественной деятельности, а также функционирования внутри- и внешнеполитических институтов.

Издревле индивидуальное и коллективное начала служили ключевыми компонентами в определении особенностей социализации личности и ориентации социума. В современной же человеческой цивилизации, похоже, развивается тенденция к усилению личностного начала на коллективном общественном фундаменте. Западное сообщество демонстрирует приоритетность индивидуализма — приверженность свободе личности и свободе слова, частной собственности, свободному рынку и конкуренции. На евразийском пространстве преобладает коллективизм: братство, дружба, патриотизм, "**чуття єдиної родини**" — его ключевые символы.

Одновременно и само историческое время поочередно проявляет, образно говоря, свойства индивидуализма или коллективизма, что наглядно проявляются в характере общественного устройства, образе жизни, музыке, литературе, архитектуре и пр. Возможно, это связано с тем, что на конкретных этапах последовательно активизируются преимущественно индивидуалистские или коллективные архетипы бессознательного, что и определяет доминанту общественного развития. При этом на каждом этапе коллективное и индивидуальное гармонично согласуются. "Коллективным по духу" периодам гармонично соответствуют "индивидуалистские по форме" стили управ-

ления (усиление диктаторских, авторитарных и тоталитарных режимов). И, наоборот, в "индивидуалистское" время доминируют коллегиальные формы правления (доминируют политбюро, ЦК, правления и пр.).

В каждом временном отрезке обозначаются характерные для него события и явления, а исторические процессы обретают специфическую окраску. Сообразно реагируют на время и конкретные социумы, общественные системы и уклады, политические и экономические институты и организации — они, как правило, чувствуют себя комфортно в "своем" времени и испытывают неудобства, трудности и потрясения в "чужом". При этом накопление не свойственного обществу "чуждого" потенциала, как и неготовность, адекватно подготовиться к наступлению "чуждого" периода, способно приводить к революционным ломкам, последствия которых ощущаются продолжительное время (порядка 9 лет) и в последующей фазе развития.

Как представляется, длительность каждой фазы составляет 36 лет (с общим периодом 72 года), начало "коллективистской" ломки приходится на 1989, 1917, 1845 и т.д. годы, "индивидуалистской" — на 1953, 1881...

Политические и социально-экономические феномены каждого времени проявляются в поведении пассионарных социумов. Так, начало "индивидуалистской" фазы 1881 года обозначилось убийством Александра II и последующей волной индивидуального террора в России и Европе. Выяснения отношений между монархами привели к цепи бессмысленных и слабо мотивированных войн, закончившихся первой мировой. Накопленный "либеральный" потенциал вначале вызвал революционный шторм 1905 года, а после и вовсе разрушил Российскую империю. Вслед за ней пали Германская и Австро-венгерская империи. На просторах Европы воцарились беспредел и анархия, усмирять которые пришлось уже новым "корпоратизаторам" — "чрезвычайным комиссарам" на Востоке, а также "коричнево - и чернорубашечникам" на Западе.

Нечто подобное наблюдалось и после смерти Сталина (1953) — разоблачение культа личности, "хрущевская оттепель", разрыв с Китаем, венгерские и пражские события, либеральные реформы, закончившиеся крахом соцлагеря (1989) и последующим развалом СССР и Югославии (1991). На этот период пришлись распад колониальной системы, массовые волнения в США, Франции, культурная революция в Китае, резонансные убийства, разгар "холодной войны", карибский кризис, войны "за принципы" — США во Вьетнаме и СССР в Афганистане.

В то же время в "коллективистской" фазе (1917—1953) после 12-летнего периода социальных экспериментов, шатаний, проб и ошибок начали зримо обозначаться консолидационные процессы. Принципиальный перелом произошел после 1929 года. Посредством тотальной мобилизации, принуждения и террора в качестве ведущей мировой державы утвердился СССР. На корпоративных принципах сформировались фашистские государства в Италии, Германии, Испании. Шел активный военный и дипломатичес-

кий передел мира. Были образованы Лига Наций, а впоследствии ООН, Варшавский Договор и НАТО.

Уже на новой волне (после 1989-го) объединилась Германия, началось активное расширение блока НАТО, экономическое и политическое усиление ЕС. Да и ГКЧП был своеобразной, пусть и неудачной, попыткой коллективного противостояния индивидуалисту Горбачеву. После дефолта 1998 г. консолидационные процессы в России активизировались. "Добровольный" уход Б. Ельцина и вхождение во власть В. Путина - наглядное тому подтверждение. 2001 год (современный аналог 1929 г.), несомненно, стал переломным не только в трансформации всей системы международной безопасности, но и формировании нового мирового порядка. Наблюдающееся ужесточение внутренних порядков в самих Соединенных Штатах в свете выше изложенного выглядит "исторически обусловленным", а не является только следствием ситуативной реакции на теракты.

На "коллективистское" же время приходятся самые тяжкие испытания для финансовой системы, имеющей явно либеральную природу. Великая депрессия в США и финансовый кризис в Европе (1931), кризисы в Мексике (1995), Азии (1997), России (1998), нынешние периодические крахи на американских фондовых рынках. Так что небезосновательно ведущие мировые эксперты предрекают трудные времена для мировой финансовой системы.

Правда, на указанных исторических этапах финансовое неблагополучие с лихвой компенсировалось способностью общества к мощной мобилизации имеющихся ресурсов. В этом и кроется успех быстрого послевоенного восстановления разрушенного хозяйства воевавших стран. Да и известный план Рузвельта по выходу из депрессии, к которому так часто сегодня апеллируют, базировался именно на корпоративных технологиях. После соответствующего обобщения Кейнсом в 1936 году и появилось в знаменитой "Общей теории занятости, процента и денег" само понятие "макроэкономика". Да и последние экономические успехи США (до 2001 г.) на волне т.н. экономической "дисинхронизации" — не что иное, как плоды экономической политики, в частности "рейганомики", базирующейся на "антицикличности".

Стремительное нынешнее развитие процессов консолидации, вероятно, во многом обусловлено еще и тем, что возросшая техногенная мощь человека в условиях глобального кризиса подвела природу к "последней черте", а человечество — к "моменту истины". И нет альтернативы практической реализации провозглашенной еще великим анархистом — князем Кропоткиным — "стратегии взаимопомощи и кооперации как основы совместного выживания", которая, правда, сегодня должна быть подкреплена и механизмами коллективной ответственности.

Степень зрелости социума во многом определяется его способностью адекватно реагировать на изменения в пространстве и времени (в т.ч. на его "индивидуалистские" и "коллективистские" вызовы). Нынешняя сила западной цивилизации во многом и состоит в ее способности "обуздать" циклич-

ность социально-экономических процессов, отслеживать наметившиеся тенденции и принимать превентивные профилактические меры.

Вместе с тем в ответ на внешние и внутренние дестабилизирующие факторы (к их числу можно отнести и навязываемые модернистские и постмодернистские социальные схемы) социумы инстинктивно "уходят в себя", находя надежную опору в своих сущностных началах — традициях. К слову сказать, и современная цивилизационная дифференциация, о которой не устает напоминать Самуэль Хантингтон, очень походит именно на такого рода "откат" к истокам в ответ на откровенное наднациональное давление.

Ветры "нового корпоративного" времени все более клонят к "первоистокам" даже западный мир, который ныне находится в пике своего величия и продолжает модернизироваться. И что же там открывается? Увы, в нынешней фазе отнюдь не культурные слои эпохи Возрождения. На поверку — в первых шеренгах традиции былого имперского величия, мессианской роли в освоении "туземного мира", искоренения еретиков, геноцида краснокожих и рабства чернокожих. Так что усмирение Багдада и Белграда, активизация радикальных политических сил и усиливающаяся их поддержка в массах — звенья одной цепи. "Бог войны" возрождается. А о благостном "конце истории" Френсиса Фукуямы придется забыть эдак на четверть века.

Синхронно происходят процессы и на Востоке, у другого украинского стратегического партнера — России. Добровольный исход из власти "адепта" российского либерализма Бориса Ельцина означил победу корпоративизма на вершине российского политического Олимпа. Произошедшее по-царски оказалось переполненным символизма — с покаянием и паломнической миссией (но с президентским эскортом) в Святую землю не только для моления у "ясел Господних", но и миротворчества. Себя-то Борис Николаевич с лихвой вписал в политический интерьер конца ушедшего тысячелетия. В результате Россия стремительно стала преобразовываться в корпоративное государство, где каждая политическая или экономическая группа имеет свой пакет акций. Вот только контрольный пакет контролируется ситуационно силовиками и олигархами.

Сегодня в России происходит мощный неуправляемый спонтанный откат к коллективным государственным традициям. Но совсем не похожи на традиции земскости, на которые уповает Солженицын, или просвещенной монархии, киномифологизированной Михалковым. Для власти ныне более насущными оказываются боевые действия, военная доктрина и концепция безопасности. В российской политике все больше чрезвычайщины. И за прошедшее семидесятилетие по сути-то и мало что изменилось — разве что место "чрезвычайных комиссаров" заняли "чрезвычайные ситуационщики". Но в этом Россия все больше походит на современную воинствующую Америку, как и консолидирующуюся и забюрократизированную Европу. На этой основе и происходит их сближение, тесно замешанное на прагматических национальных интересах.

Как уже неоднократно бывало в истории, Украина оказалась на стыке двух миров, отличных по своему духу, но похожих по форме общественной организации. Какое место ей уготовлено в таком мире? Сможет ли она отстоять свое право на самобытность? Окажется ли "точкой раздора" в борьбе или "разменной монетой" в торге сильных мира сего? Станет ли показательным объектом совместной "воспитательной" работы Запада и Востока, или же будет служить "немым укором" двум выясняющим отношения мирам? А может, все же найдет в себе силы достойно принять предложенные временем вызовы.

Для того чтобы ответить на подобного рода вопросы, как и понять причины наших насущных бед и проблем, необходимо зреть в культурный корень социума. Речь о культуре в ее широком понимании, как о некой сущностной матрице (программе), определяющей основы мировосприятия, миропонимания, установки и стереотипы поведения, способы действия и приспособления к изменяющейся социальной и природной среде, которая устойчиво воспроизводится через систему совместной жизнедеятельности и образования.

Именно социокультурные начала выступают системообразующим стержнем политического устройства государства, хозяйственных укладов, общественных традиций, норм нравственного поведения социума и личности. И величие культуры народа определяется тем, в какой мере она способна мобилизовать и поддерживать духовные, душевные и физические силы человека и общества, прежде всего в тяжкие годины испытаний.

Чем же определяется наша социокультурная среда сегодня и каковы ее перспективы в контексте стратегических направлений развития человеческой цивилизации? Какова наша национальная карма в свете цивилизационных приоритетов?

С активным включением Украины в мировые процессы представилась возможность не только глубже познать мир, но и лучше увидеть в их зеркале самые потаенные уголки своего национального характера. Начавшийся в Украине с крушением империи активный процесс национальной самоидентификации серьезно обозначил проблему социокультурной неоднородности страны. Ведь держава в ее нынешних границах — суть советский проект собирания земель и народов, консолидация которых до 1991 года обеспечивалась сугубо тоталитарными методами. Последовавший затем период "вольницы" хотя и обнажил проблемы, однако не обострил их до крайности. Сегодня же ситуация в свете происходящих на планете процессов и явлений кардинальным образом меняется.

Западная Украина, стабильно отягощенная европейским выбором (дают о себе знать и историческая память, и влияние западной диаспоры), периодически срывается на откровенную русофобию. Восток и Юг, хотя и пребывают до сих пор в своеобразной "этнической спячке" (в основном вследствие маргинализации населения), все же приоритетно расположены к связям с Россией. И начавшиеся процессы консолидации российского общества

в определенной мере влияют на Украину, не говоря уже об активной экономической экспансии российского капитала. Активизируется крымско-татарское национальное движение, к интересам которого неравнодушны наши южные соседи. Центр, в свою очередь, все более тяготеет к идее самодостаточности и равноудаленности. И не считаться с этим нельзя.

Нарастание этнической и цивилизационной дифференциации отмечается не только в постсоветском пространстве. Так, благополучная Австрия в "период Хайдегера" в порыве национального эгоизма откровенно бросила вызов единой Европе. Впоследствии Франция и Германия проявили свой норов в отношении военных приготовлений США в отношении Ирака. В свою очередь, новые кандидаты в ЕС проигнорировали "европейские ценности" в порыве своей поддержки США. По сути, наблюдалась "нормальная" традиционалистская реакция на мировые глобальные изменения.

Проявляющийся в подобных случаях национализм, с одной стороны, является той пробивной силой, которая рушит имперские системы (так распались СССР и СФРЮ), расчищая тем самым путь для "нового мирового порядка". С другой стороны, он создает барьеры не только для процессов интеграции, но и для социальной модернизации и реформирования. Украина в полной мере это ощутила на себе. А потому дабы осознать социальные ресурсы реформирования, целесообразно разобраться в своих "национальных чувствах". В какой же мере культура украинского социума способна стимулировать процветание Украины в XXI веке?

Завороженность идеями либеральной демократии в начале 90-х создала в Украине иллюзию, что их постижение и внедрение в общественную практику будет способствовать активному вхождению в западный мир. Тем более что, казалось, украинцы "генетически обречены" на либерализм. Но такая украинская либеральная демократия оказалась крайне неуживчива не только с корпоративными требованиями времени, но и насущными потребностями общества: разногласия во власти, отсутствие социальной солидарности и политического согласия, разрозненность и непримиримая конкуренция политических движений, олицетворяющих гетманские амбиции отдельных лидеров или бизнес-групп, непомерно разросшаяся политическая и экономическая теневая деятельность.

С началом становления украинской государственности многие министерства и ведомства превратились в своеобразные бюрократические корпорации-"вольницы", прибравшие к рукам целые сферы народного хозяйства. Попытки реформировать государственно-административную машину и экономическую систему разбивались о своеволие чиновников. А чего стоит только один "институт льгот"? И сколько было поломано сверхприбыльных коммерческих схем, требовавших объединения интересов нескольких "групп влияния"?

В таких условиях естественными стали деградация и разбазаривание таких сложных структур, как Черноморское пароходство, огромные пробле-

мы в обеспечении функционирования нефтеперерабатывающих комплексов и электроэнергетических систем. Создание финансово-промышленных групп остается только в мечтах и проектах, "вакуум" фондового рынка так и не заполняется. Некогда могучие украинские компании перестали интересовать стратегических инвесторов, поскольку оказались в весьма плачевном состоянии из-за бездарного руководства ими. А построенный на "хуторянский" принципах нефтепровод "Одесса-Броды" без соответствующего его корпоративного обеспечения пока что оказался только дорогостоящей "железякой", зарытой в землю.

С великим "облегчением" Украина отказалась от технологически насыщенных контрактов и пошла на стратегические политические уступки в обмен на сырье, прощение долгов, кредиты или обещания развивать малый и средний бизнес. Фактически без боя были сданы позиции в борьбе за инвестиции в высокотехнологические сферы и доступ своей интеллектуально емкой продукции на мировой рынок. Действующие единичные высокотехнологические производства как "оазисы" в промышленной пустыне — их можно пересчитать по пальцам.

По существу, Украина очутилась в плену своих страстей за формулой Леонида Кравчука - "маемо те, що маемо". Заклинаниями по поводу наших несуразиц уже никого не удивишь. Но в вопросах вскрытия причин пока что в головах политиков и экспертов полный разброд. Некогда популярные ссылки на тяжесть тоталитарного наследства не убеждают. Разве что еще продолжают по инерции использоваться в рамках некоторых политических ритуалов. По-моему, дело обстоит не столько в отсутствии единства взглядов, сколько в недостатке смелости беспристрастно всмотреться в самих себя, не пеняя на зеркало... А тем более констатировать не вполне приятные для себя вещи.

В частности, признаться себе в том, что трудности во взаимоотношениях Украины с "расчетливым" Западом и "жестким" Востоком нередко возникают в силу того, что демонстрируемые украинцами особенности поведения и способы действий не всегда адекватно вписываются в контекст принятых в современном мире норм. И в условиях заведомо проигрышного противостояния с технократическим миром "невостребованные" и даже антагонистичные ценностные ориентации и свойства национального характера вытесняются в область подсознательного, формируя именно тот комплекс "меншовартості", который не только мешает жить, но и порождает "теневой имидж нации", эксплуатируемый украинскими недругами и недоброжелателями.

Чрезмерная конкретно-предметная ориентация (по принципу "краще курка в руці, ніж журавель в небі") не только в личном общении, но и в конкретных политических и коммерческих делах, проявляется в пренебрежительном отношении к сложным интеллектуальным процедурам принятия решений, игнорировании информационных ресурсов как фундамента современных систем управления, а также зацикленности на вопросах владения собственностью в ущерб эффективного управления ею.

Затаенная углубленность украинской души, склонность к общению со своим внутренним миром, уединению или созданию малых групп на основе взаимных симпатий — трансформировалась в идеал "моя хата скраю" как символ партикулярного местечкового патриотизма, декларирование нейтральности и внеблоковости — эдакой формы отстраненности от участия в мировых политических корпорациях. Социальная пассивность, консервативность, нежелание рисковать, стремление к обособлению и персональной свободе без надлежащей ответственности, дисциплины и организованности, как и отсутствие устойчивого целеполагания, становятся серьезным тормозом для корпоративных действий и инновационной деятельности.

Украинский этнонациональный психотип приоритетно "живет вне времени", предпочитая углубляться в прошлое с его архаикой и символикой. Вследствие этого прошлое сверх меры тяготеет над настоящим, окрашивая его в депрессивные тона (в этом контексте характерным есть явное преобладание ритуалов поклонения жертвам, а не героям). При этом будущее практически оказывается вне поля внимания — о нем в большинстве предпочитают не думать (к слову сказать, футурологические прогнозы в среде украинских интеллектуалов не в чести). Но если какие-либо проекты и появляются, то в них иллюзорность и виртуальность значительно преобладают над реалистичностью просчетов. А потому-то и закономерна судьба наших "планов громадья".

Серьезными проблемами сопровождаются и процессы глобального пространственного обустройства. Это явственно проявляется как в геополитических и геостратегических колебаниях государства, так и в опаске заняться серьезным административно-хозяйственным обустройством страны. Украинцы больше тяготеют к организации микропространств ("садок вишневий коло хати..." и пр.). К слову сказать, именно в пространственно-временной ориентации рельефно проявились сущностные отличия украинской и российской ментальности (россияне приоритетно ориентированы в будущее и на обустройство пространства в глобальных масштабах).

Процесс возрождения этнонационального украинского начала в культуре страны, хотя и сказался благотворно на ряде сфер общественной жизни, вместе с тем обнажил ряд болезненных проблем, касающихся социальных последствий возврата к традициям и вскрытия культурных слоев и архетипов коллективного бессознательного. И как оказалось, именно в "преданиях старины глубокой" коренятся многие из тех "несвоевременных" качеств украинского характера, которые вызывают "аллергию" в мире.

К месту задуматься над предупреждением авторитетного "американского" украинца Осипа Мороза, что "вряд ли можно брать прошлое за образец", а присущая украинцам "селянская ментальность хороша для селян да и то в определенное время и определенном месте, но она не полностью дается целой нации". "Самооправдания" по типу того, что в условиях возможных глобальных экологических катаклизмов особая психофизиологическая живучесть и гармоничная вписанность украинцев в природу сгодятся, пока не

сбываются. И хотя способность выживать в самых невероятных обстоятельствах украинцы демонстрировали в течение всей своей истории, социальные катастрофы, как и внутриполитические разборки XX века свидетельства серьезных "неполадок" украинского социокультурного механизма. Прежде всего, в той его части, которая ответственна за коллективные формы выживания.

Столкнувшись с серьезными внутренними проблемами и не найдя сил для их разрешения, на определенном этапе общественного развития украинцы, даже при всей обращенности внутрь себя, в поисках "точки опоры" активно стали уповать на внешнюю помощь.

С одной стороны, Запад прельщал уровнем жизни, успехами в организации эффективного производства и управления. Но со временем иллюзии по поводу того, что мы быстро "заразимся" этим опытом, миновали. От западных политиков и экспертов пришлось выслушать сонм поучений, претензий, укоров и требований. В "сухом остатке" помощи остались сдвижки разве что в вопросах развития мелкого и среднего бизнеса, отработки элементов международной политики и сфере безопасности и ... огромные финансовые долги.

Какой уж там корпоративный опыт... А зарубежные транснациональные корпорации в Украине — это и вовсе "вещь в себе" под покровительством международных организаций и правительств ведущих мировых держав. Что же касается американского опыта социального партнерства, основанного на принципах "этнонационального плавильного котла", то его внедрение в Украине и вовсе губительно для общества. Однако вряд ли стоит корить Европу и Америку в том, что они не желают продвигать Украину технологически - не в их культурных традициях глубоко рефлексировать по поводу "непонятных" сторон украинской ментальности.

Как бы то ни было, украинскому социуму предстоит нелегкий путь приспосабливания к нормам и нравам глобального корпоративного мира, его жесткому правовому порядку и прагматичности. Если мы задумываемся всерьез о своем экономическом, технологическом, культурном и даже политическом процветании в третьем тысячелетии, то должны активно приобщаться к мировому опыту модернизации, реформируя не только политическую и экономическую систему, но в первую очередь себя. Если мы сознательно не укротим "буйство национальной архаики", о национальном суверенном будущем можно и не помышлять.

Достойное существование человечества в XXI веке современная цивилизация обуславливает, прежде всего, степенью гуманизации всех сфер жизнедеятельности социума. Общественное богатство ведущих мировых держав все в большей степени определяется "интеллектуальным капиталом". В этом контексте даже деструктивные явления, окрасившись в гуманитарные тона, приобрели особую силу. Не от того ли гуманитарный интервенциализм стал предтечей "нового мирового порядка",

своеобразным тараном, взламывающим существующую мировую систему безопасности?

В гуманитарной сфере, прежде всего в культуре этносов, наций и человечества в целом, похоже, и следует искать ответы на самые актуальные вопросы и вызовы времени. Именно там (и уж точно не в финансово-банковских запасниках) сокрыты секреты доступа к кладовым человеческого знания и опыта. Национальное процветание в современном мире немыслимо без активного овладения новейшими социальными технологиями формирования прогрессивных хозяйственных укладов. Но досконально постичь их можно только при полноценном приобщении к культуре, живым духовным, нравственным, интеллектуальным ценностям и традициям, в рамках которых они сформированы.

Для украинцев формирование фундамента жизнеустройства и гармоничного развития, наряду с разумным восстановлением национально-культурных основ, требует бережного отношения ко всему копившемуся столетиями культурному наследию. Особое место в нем принадлежит русской культуре. Ведь, по сути, она явилась той гармоничной средой, в которой на протяжении столетий совместно развивались и с которой фактически и произрастают нынешние украинская и российская культурные ветви. В этом синтетическом лоне вызревал гений Тараса Шевченко, Николая Гоголя, Владимира Вернадского. Пора признать и то, что русская культура послужила и своеобразной "защитной оболочкой", позволившей украинской культуре сохраниться и развиваться во враждебном политическом окружении. А выкуп Тараса Шевченко из крепостничества деятелями русской культуры стал архитипическим сюжетом, новым мифом современной украинской культуры.

Последние столетия русская культура служила для украинцев реальным проводником к мировому социальному опыту и научно-техническим достижениям человечества. Наша история наглядно свидетельствует — синтез культурных начал способен многократно усилить культуру каждого народа.

Традиции социокультурного единства испокон веков живучи в славянском мире. Ведь и само православие на Руси, как духовный стержень народа, приобрело нынешние свои очертания в результате интеграции византийской культуры и языческих традиций, а украинская мелодика гармонично слилась в нем с литургическими молитвами. Да и вклад украинцев в остов российской и советской культуры, науки и образования вряд ли кто сможет умалить.

Особый морально-нравственный, гуманистический дух украинского национального характера являются благодатной "почвой" (особенно на жестком "насте" западного прагматизма, с одной стороны, и российского идейного мессианства в союзе с византийской традицией в политике, с другой) для формирования как принципов общечеловеческих отношений в новом мире, так и основ построения демократического общества и в Украине, и в России.

По сути, в Украине в миниатюре повторяется цивилизационная конфигурация России. Вот только алгоритм разрешения конфликтов предлагает-

ся иной. И если он окажется эффективным — как знать, возможно, он укажет России эффективные пути выхода из внутренних межэтнических конфликтов, — в этом может состоять одна из существенных украинских компонент в здании украинско-российского стратегического партнерства.

Особое место в полноценном приобщении к культуре, духовным, нравственным, интеллектуальным ценностям и традициям принадлежит языку. По сути, он является не только средством коммуникации, но и ключом, позволяющим вскрывать закодированные в культуре сакраментальные смыслы. Эффективное приобщение к культурному достоянию происходит не столько путем ознакомления с предметами, текстами и символами, сколько через непосредственное общение с живыми носителями идей и традиций, представителями научно-технических или художественных школ.

Но вот о таком сущностном назначении языка (особенно когда речь заходит о функционировании русского языка в Украине), похоже, мало кто задумывается или же предпочитает этого не замечать. Общественный диалог о последствиях ускоренной украинизации сфер образования, профессиональной подготовки, производственной деятельности, управления (как свидетельствуют последние социологические опросы именно в них, да еще в СМИ, наиболее активно идут процессы расширенного использования украинского языка) и вовсе выведен из общественного обсуждения. О нем, как о покойнике, — или хорошо, или ничего. Хотя социологические опросы показывают достаточно устойчивое использование языков в быту — 50:50.

Исподволь навязывается безальтернативное мнение об украинизации как сугубо техническом процессе — просто все и всех перевести на один язык. И беспокоиться вроде бы не о чем — некоторые высокотехнологические производства и новые хозяйственные институты работают не хуже российских. Да и не переводятся ученые с мировым именем, а украинские школьники продолжают занимать призовые места на международных олимпиадах.

Но давайте же посмотрим, благодаря чему это все "дышит", кто составляет костяк научно-технической и управленческой элиты Украины? Ответ прост — ведущие ученые и технические специалисты, а также удачные бизнесмены, предприниматели и квалифицированные менеджеры, интеллектуально взращенные в лоне советской (а по сути русской) научной и образовательной традиции. Именно той традиции, которая позволила СССР дважды после уничтожительных гражданской и отечественной войн, в условиях жесточайших репрессий против интеллигенции быстро воспроизводить интеллектуальный потенциал и выводить страну на передовые позиции в мире. Именно в рамках этой традиции удавалось осуществлять немыслимые для остального мира социальные и экономические реформы. Последнее для Украины сегодня актуально как никогда. То, о чем только начали вещать западные лидеры, мы уже имели. Вот только продолжаем ли владеть им сейчас? А главное, хватит ли ума, чтобы возродить "разумное, доброе, вечное"?

Не будем закрывать глаза и на то, что вопросы реального распространения и функционирования русского языка в Советской Украине во многом определялись не только властными мерами, но и насущными культурными и хозяйственными потребностями общества. Так, интенсивная "русификация" 70-80-х годов обусловливалась не столько административным принуждением, сколько активным интересом украинцев к новым общественно-политическим веяниям, исходящим из Москвы или ретранслируемым из-за рубежа центральными СМИ. Но, прежде всего — потребностью овладевать новыми специальностями в соответствии с запросами активно развивавшихся в Украине машиностроительных комплексов, поскольку необходимые знания и навыки можно было получить только в рамках русских научно-технических и технологических школ.

Сегодня же именно там, где произошла повальная деиндустриализация, в рамках означенного уже процесса "наступления села на город" и возрождения "идиотизма сельской жизни", наблюдается активный возврат к украинскому языку. Радоваться ли этому — вопрос риторический. Как и тому, что значительная часть русскоязычных детей не умеют грамотно писать по-русски. Не в этом ли причина нынешнего исхода украинских специалистов в Россию?

Ныне в Украине развивается уже другой подобный процесс вестернизации общества как следствие приобщения к западному техническому и технологическому сервису, системе стандартов, Интернету, международным вещательным каналам и пр. Дай-то Бог с умом к этому отнестись.

В глобальном мире многоязычие — великое благо, которым, правда, нужно уметь распорядиться. Постигшие это страны успешно развиваются и процветают. Мнение бывшего премьер-министра Израиля Биньямина Нетанияху характерное тому свидетельство: "Репатриация из России и СНГ изменила Израиль, усилила Израиль, превратила Израиль во всемирную державу в области технологий, в мировую державу в области культуры и в очень многих других областях. ... Израиль, тот, который я помню десять лет назад, и Израиль сегодняшний — это очень большой прорыв вперед... Наша связь с Россией, с русской культурой — это не только плод последней большой волны репатриации... Мои родители знали русский, я был воспитан на русской культуре, читал Достоевского, Толстого".

Украина — не Израиль. У нее нет широких возможностей "импортировать" русских интеллектуалов (кстати, Израиль с большой помпой уже встретил миллионного "эмигранта из России"). Но зато есть более значимое — возможность воспроизводить непосредственно у себя русские культурные традиции, носители которых и обеспечивают нынешнее процветание Израиля, как и США. Украина пока еще сохраняет уникальную возможность остаться страной гармонично поликультурной и многоязычной. И в обществе существует настоятельная потребность в этом.

Насущными для Украинского государства и общества сегодня представляются даже не вопросы обеспечения т.н. "диалога культур", а задачи их

"кооперации", полновесного и равноправного существования в рамках новой культуры страны. Необходимо продвигаться в направлении построения общества на принципах социокультурного синтеза (промежуточной ступенью может стать внедрение принципов мультикультурализма). Только в этом случае мы вправе будем рассчитывать на синтез принципиально новых основ общественного развития.

Вдохновляющие результаты мультикультурного существования наглядно демонстрирует "четырехъязычная" Швейцария, устойчиво процветающая в условиях жесточайших европейских конфликтов XX столетия. Поражают успехи "двуязычной" Финляндии, сумевшей в короткий исторический срок преобразиться из окраины Российской империи в авторитетное европейское государство, своеобразную "колыбель" современной системы европейской безопасности. Характерно, что именно эти страны занимают одни из высших позиций в рейтинге стран с наиболее высокой инновационной активностью (в компании с Японией, США, Швецией и Германией). Соединенные Штаты в интересах эффективной интеграции латиноамериканцев в социум решают вопрос об официальном статусе испанского языка в южных штатах.

Транснациональные корпорации — эти локомотивы современного индустриального развития — активно занимаются решением вопросов т.н. "культурного многообразия", благодаря чему им удается формировать и поддерживать высокий инновационный и творческий потенциал.

Многоязычность социума благотворно влияет и на уровень его толерантности. Так, проводившиеся в Украине социологические исследования подтвердили более низкий конфликтный потенциал респондентов, которые свободно владеют и русским, и украинским языками, в сравнении с "моноязычными". На востоке Украины этнографы уже отмечают феномен формирования синтетического сообщества, которое равным образом идентифицирует себя с обоими этносами. Не в этом ли кроется основа той социальной терпимости, которую устойчиво демонстрировал украинский социум? Не здесь ли искать ресурсы для сдерживания традиционалистских "откатов" и осуществления модернизационных прорывов?

Особые эффекты многоязычности, связанные с глубинным постижением заложенных в текстах смыслов, можно наблюдать и на микроуровне. Вероятно, каждому, владеющему свободно несколькими языками, приходилось сталкиваться с интересным феноменом. При авторском переводе текста или одновременной работе с идентичными текстами на разных языках интенсивно выявляются неточности и нечеткости изложения, незаметные при работе только с одним языком. К слову сказать, ведь для качественной законодательной работы — это кладезь.

Другой феномен — активное использование иностранных слов в специальных областях. Как правило, это не столько дань уважения или результат преклонения перед иностранным, сколько насущная необходимость придать адекватные смыслы тем явлениям, событиям или техническим устрой-

ствам, которые в рамках своей культуры еще не "созрели", а потому и не имеют подходящих аналогов в языке.

В процессе поиска путей развития международного сотрудничества особое внимание Украины сегодня обращено на мусульманский мир. В этой связи актуальным представляется использовать возможности формирования в Крыму в региональном масштабе мультикультурного сообщества на фундаменте русской культуры с полноправным украинским и крымско-татарским компонентами. Это не только способствовало бы желанному межэтническому согласию на полуострове, но и создало бы предпосылки для формирования нового поколения, способного достойно представлять Украину и продвигать ее интересы в тюркский, а возможно, и в весь мусульманский мир. И это не плод авторского воображения. Так, в Крыму вопросами развития культурного многообразия в студенческой среде активно занимается ректор Крымского государственного индустриально-педагогического института Февзи Якубов. В частности, им разработан проект создания Центра полиэтнической культуры молодежи как эффективной формы культурного взаимообогащения студентов-педагогов. Не надо быть пророком, чтобы предсказать, что будущее за воспитанными именно в такой атмосфере специалистами. Они же и будут основными носителями и проводниками межнационального согласия в обществе. Подобные процессы устойчиво развиваются и в Закарпатье.

В свете изложенного, не только русофобия, но и стремление придать русской культуре и языку статус иностранных, равно как и игнорирование в Крыму крымско-татарской культуры — бесперспективны, вредны и опасны. Это путь к культурной деградации, распаду общества и развалу страны, при которых Украину ожидает участь "европейского хутора", "певческо-шароварной резервации", свалки ядерных, химических и гуманитарно-технологических отходов. Осознают ли те, кто ратует за установление "моноязычного" диктата, в какой ад ведет дорога, выстланная такими "благими намерениями"?!

Динамично меняющийся мир торопит. Вслед за коротким периодом надежд, соблазнов и иллюзий, который прошел для Украины в благостной дреме, наступает пора жестких требований и прагматических решений. Время настойчиво диктует свои условия и принципы организации общественного бытия — энергичное внедрение инноваций и корпоративных норм управления, гармонизацию национальных традиций с потребностями общественной модернизации.

Украина не в состоянии противостоять технократическому натиску современной цивилизации. Да и нет потребности в таком "геройстве". Надобно меняться самим в модернизирующемся мире. И только при условии, что общество окажется в состоянии сдерживать буйство своих этнокультурных страстей и расчетливо задействовать максимум доступных культурных механизмов и ресурсов, Украина сможет рассчитывать на достойное существование в новом столетии и тысячелетии [205-214].

2.2. Конвенциональное и операциональное манипулирование в международной политике

Манипулирование в международной политике на определенных этапах исторического развития - явление чрезвычайно распространенное. Похоже, что в периоды мирного (или квазимирного) сосуществования манипулирование активно компенсирует, замещает и даже вытесняет силовые методы воздействия. Последние же применяются как раз тогда, когда манипулятивные технологии дают сбой. Да и в этих случаях военные действия или спецоперации становятся только прологом для последующих более жестких манипуляций. Наглядный тому пример - боевые действия на Балканах и последующая смена режима в Белграде. Таким образом "тотальное манипулирование" фактически стало своеобразным прологом к "всеобщему примирению".

Но, пожалуй, наиболее впечатляющий результат манипулирования в международном масштабе - развал Варшавского Договора и Советского Союза, последующие внутренние трансформации на постсоциалистическом пространстве и всей системы международных отношений. Более близкий для нас образчик - мощное внешнее влияние на систему межгосударственных отношений в рамках СНГ.

Это требует не только серьезного политологического, социально-психологического, но и методологического осмысления. Основные исследования в сфере манипулирования, как правило, касаются изучения особенности поведения личности, социальных групп и целых социумов в условиях психологического воздействия манипуляторов.

Из выделяемых пяти основных видов манипулятивного воздействия (эксплуатация личности; манипулирование образами и символами; манипулирование духовностью; конвенциональное и операциональное манипулирование) наибольшее отражение в социально-психологической литературе нашли первые три вида. И это закономерно, поскольку именно они лучше всего подходят для изучения личности или человеческих сообществ как социально-психологических целостностей.

Однако международные отношения - система более сложной природы, которая в значительной степени определяется организационными структурами - государственными, надгосударственными и внегосударственными (как национальными, так и международными). Изучение особенностей эффективного манипулирования именно в такой международной среде требует серьезного рассмотрения, прежде всего, конвенциональных и операциональных технологий.

Конвенциональное манипулирование. В самом названии этого вида манипулирования заложена технологическая формула, предусматривающая использование в манипулятивных целях некой договоренности — конвенции.

Досконально его рассмотреть применительно к международным связям сам Бог велит. Вся современная система международных отношений и пост-

роена на системе международного права — от Устава ООН, основополагающих международных договоренностей (таких как Хельсинские соглашения или Договор о нераспространении ядерного оружия, разного рода международных и региональных хартий), вплоть до межгосударственных договоров и соглашений. В своей основе договоренности обуславливают признание некой системы интересов и ценностей (в частности, свободы слова, либерального и демократического выбора), ограничений и запретов, следование общепринятым процедурам взаимоотношений (в части, разрешения конфликтных вопросов и споров), а также стандартизацию форм институциализации и т.п.

Однако любое новое государство, вступающее на конвенциональное игровое поле априори слабее старожил. А значит автоматически в целом обречено на проигрыш. Тем более что "правила" периодически уточняются, приобретают новые трактовки и т.д. Что же затягивает "неофитов" в это своеобразное "международное казино"? Вероятнее всего ребяческая жажда игры, инфантильные иллюзии о возможности быстрого обогащения в результате приобщения к "цивилизованному сообществу". Такова природа не только отдельного человека, но и человеческих сообществ. Происходящее в мире очень походит на глобальный дрейф человечества от "человека мыслящего", через "человека играющего" к "человеку манипулируемому".

Конвенция выступает своеобразным "глобальным вирусом", внедряющим в общество (в обход его "иммунной" системы) инородные идеологические клише, мифы и символы. Принимая ту или иную идеологию, человек начинает пользоваться ей, как топографической картой, говорить на ее языке, подключаться к имплицированным в ней ценностям. Так, незаметно для себя, он оказывается во власти иллюзий и моделей, наработанных этой идеологической машиной, всецело встраивается в формат ее дискурса.

Сегодня уже можно посмеяться над понятиями умершей идеологии - "развитой социализм", "всенародная поддержка партийных решений" или "братский союз социалистических стран". Однако когда дело доходит до аналогичных словосочетаний ныне торжествующей идеологии — "открытое общество", "демократизация", "общечеловеческие ценности", "рыночные реформы" или "гуманитарная военная операция", "борьба с международным терроризмом" критическая прыть явно угасает.

Что касается международной политической практики, то здесь власть господствующего идеологического дискурса остается более чем внушительной. В современной практике наглядно можно наблюдать внешнеполитические санкции в отношении стран, обвиненных или в авторитаризме, или сдерживании рыночных реформ, или нерадении о свободе слова, или заподозренных попытках продажи оружия "странам-изгоям" и т.п.

"На службе" у либеральной конвенции находятся сегодня основные силы информационно-пропагандистской индустрии. Управление умозаключением массовой аудитории строится по принципу прямых позитивно-негатив-

ных подкреплений: в этой стране больше демократии, быстрее идут реформы — сюда будут направлены деньги мировых финансовых институтов, экономика и социальная сфера получат поддержку. Здесь, напротив, страдает демократия и рыночные реформы - население этой страны должно задуматься о международной ответственности за собственное "плохое" правительство, а заодно и последствиях возможных бомбардировок.

Сила подобного "втягивания" настолько могущественна, что позволить себе отступничество могут только сверхдержавы, инородные цивилизационные блоки (мусульманский, буддистский и т.п.) или либо "отчаявшиеся" государства. Отношение США к договору по ПРО, принятие новой Стратегии национальной безопасности, устанавливающей право наносить на собственное усмотрение превентивные удары в любой точке земного шара - наглядный тому пример.

Хроника международных конфликтов последних десятилетий - события в Персидском заливе, Югославии, Афганистане - свидетельствует, что с начала 90-х гг. в международной политике начинает доминировать стремление сломать сложившуюся систему правил и процедур, утвердить в международных отношениях принцип "двойных стандартов".

В качестве примера можно привести ситуацию вокруг Южной Осетии. Как известно 12.11.06 в этой республике прошел третий со времен провозглашения независимости референдум, вновь подтвердивший стремление народа республики к выходу из состава Грузии.

Задолго до того, как состоялось голосование, Европа и США заявили, что считают его не легитимным. С подобными заявлениями выступили представители Совета Европы, Европейского Союза, НАТО и Государственного департамента США. Заместитель госсекретаря США Даниэл Фрид заявил, что "Проводить параллели между Абхазией и Южной Осетией, с одной стороны, и Косово - с другой, является исторически ошибочным. И Косово нельзя приводить в качестве примера, потому что это уникальный случай". Уникальность косовской ситуации в отличие от южноосетинской заключается в том, что, по мнению западных экспертов, в Косово был геноцид местного населения, а в Южной Осетии геноцида не было.

Более глубокий анализ свидетельствует как раз об обратном. Еще в сентябре 2001 года Суд ООН, заседавший в Приштине, пришел к выводу, что действия сербских войск в Косово в 1998-1999 годах нельзя расценивать, как геноцид. Не было выявлено ни единого приказа со стороны политических или военных властей Сербии, чтобы убивать именно албанцев или разрушать албанские памятники культуры. Война шла с так называемой армией освобождения Косово и в этой войне, как и во всякой другой гибли мирные люди разных национальностей.

Судебная комиссия подробно расследовала все так называемые факты массовых этнических чисток албанцев и пришла к выводу, что эти факты сфабрикованы информационной службой освободительной армии Косово. Один

из таких "фактов" – известная ситуация вокруг села Рочаг, когда журналистам были представлены трупы 38 человек якобы мирных жителей, якобы убитых сербскими полицейскими. В ходе детального расследования выяснилось, что в действительности это были не мирные граждане, а убитые в боях, или раненые в боях и добитые потом самими же боевиками члены албанских боевых организаций.

Однако о решении суда ООН, не признавшего факт геноцида в Косово, известно лишь узкому кругу специалистов, а вот о не существовавших массовых казнях албанцев по приказу Белграда, благодаря западным СМИ, слышали во всем мире. Потому что миф о геноциде нужен был для оправдания американских бомбардировок Югославии и свержения президента Милошевича.

В Южной Осетии ситуация прямо противоположная. Осетинское население реально несколько раз в своей истории подвергалось этническим чисткам со стороны грузин. Еще в 20-м году были совершены 3 карательных операции грузинскими вооруженными силами в отношении осетин. Результат этих операций: 18 тысяч осетин, то есть, 4-ая часть населения, были уничтожены, 50 тысяч - бежали в Северную Осетию, 95 сел было сожжено. В январе 91 года правительство Гамсахурдиа попыталась установить власть Тбилиси над Цхинвали силой. Тогда более 3 тысяч осетин погибло, 300 пропали без вести, 40 тысяч бежало в Россию.

Тем не менее, Запад настаивает, что в Южной Осетии геноцида местного населения не было, а в Косово геноцид был. Такова реальность современного конвенционального манипулирования: договорились считать черное белым, а белое черным; соответствующим образом "проинформировали" мировую общественность и теперь оперируют своими конвенциональными установками (результатами сговора) как аксиомами реальности, на основе которых следует строить логические умозаключения и принимать политические решения.

Операциональное манипулирование. Основной мишенью данного вида манипулирования являются операциональные схемы деятельности государственных и надгосударственных структур и их чиновников, алгоритмизирующие процесс принятия управленческих решений, управленческой деятельности в целом.

Всем, кому приходилось непосредственно заниматься управлением, знакомо особое удовольствие от хорошего системного изложения проблемы, наличия качественной процедуры выработки решений или участия в работе слаженной управленческой команды. Ответственный чиновник по роду своей деятельности расположен к восприятию и признанию над собой власти нормы, организующей системы или управленческой процедуры.

Власть нормы признается и "исповедуется" не только чиновниками, но и учеными, юристами и методологами. По мнению последних, представление о характере того или иного управленческого решения можно составить задол-

го до его принятия, проанализировав концептуальный аппарат разработчиков данного решения.

Международные правовые нормы также разрабатываются в определенном концептуальном формате, вокруг которого разворачивается основная борьба. Принципиальным в политике является то, в каком понятийном языке мы анализируем международные события и принимаем решения, насколько этот язык наш - понимается нами и обслуживает наши интересы. Остальное - дело техники.

Отчаянная борьба на международной арене относительно понятия "гуманитарная интервенция" или в Украине вокруг ратификации европейской Хартии региональных языков или языков национальных меньшинств, языковой реформы, как и вопроса вступления в различные международные организации - наглядное тому свидетельство.

Яркий пример нормативно-правового манипулирования в Украине – это семантические игры вокруг Европейской хартии региональных языков и языков меньшинств. До 15 мая 2003 года русский язык в Украине имел статус языка межнационального общения. После ратификации Украиной Европейской хартии региональных языков и языков меньшинств, подписанной от имени страны еще 2 мая 1996 года в Страсбурге и представленной как уступка русскоязычной общине, русский язык получил статус языка национальных меньшинств. То есть реально потерял в статусе.

Событие была разрекламировано как величайшее достижение демократии – теперь, мол, начнется реальная защита языковых прав граждан, все будет, как в Европе (на каждых трех иноязычных детей по специализированному классу и т.п.). Однако, когда после долгих проволочек 1 января 2006 Хартия в Украине, наконец, вступила в силу, выяснилось, что снова "хотели как лучше, а получилось как всегда". Никаких конкретных мероприятий по реализации положений Хартии в Украине не запланировано и денег на нее в бюджете не предусмотрено.

Таким образом, если отринуть словесную шелуху и пустые обещания, в сухом остатке – очередное поражение русского языка в статусе: с уровня языка межнационального общения до уровня языка национального меншинствастваа. Такая себе меньшина в половину населения страны (согласно различным социологическим опросам, количество людей в Украине, пользующихся русским языком как основным в повседневной и деловой жизни колеблется в пределах 46-54% от общего числа граждан). Указанная диспропорция между тем, что есть и тем, как это называется и, соответственно, что из этого следует, является питательной средой для роста центробежных и экстремистских настроений в Украине.

Нередко случается так, что отдельные государственные чиновники, не способные к зрелой методологической рефлексии основ международной нормативно-правовой базы, впадают в одну из двух крайностей: крайность пренебрежительного отношения к международным правовым нормам, что очень

болезненно воспринимается мировым сообществом, или противоположную крайность — неадекватное благоговение перед второразрядными инструкциями и иноземными институтами, плодящими эти инструкции.

В одном из документов эпохи холодной войны под общим названием "Silver Key" содержится набор рекомендаций сотрудникам спецслужб по методам подавления интеллектуального потенциала противника в сфере науки. Вот некоторые выдержки из этого документа:

"...Важно навязать противнику ложные цели научных исследований. Для этого можно использовать рекламу той или иной неверной научной теории, концепции технологического развития, методики исследований.

Ложная цель, поставленная перед научным коллективом (или даже перед целой отраслью), является действенным механизмом "омертвления" финансовых и материальных средств...

Неверная методика исследований приводит к консервации перспективной научной идеи и способна отбросить противника в той или иной отрасли на годы (и даже десятилетия)...

Психологической обработке легче всего поддаются руководители научных коллективов, которые, как правило, мало разбираются в конкретной тематике и осуществляют лишь общее (партийное) руководство. Однако это не лишает их амбиции "крупного ученого", каждое слово которого коллектив должен воспринимать как руководство к действию... Его (руководителя научного коллектива) можно пригласить на международную научную конференцию (симпозиум), где исподволь внушить необходимое нам направление исследований... ". И так далее в том же духе.

Хотя приведенный выше документ относится, главным образом, к противоборству в научной области, его выводы вполне применимы к сфере государственного управления, а контекст понятен любому чиновнику.

Одним из аспектов действия власти нормы является референтная власть - способность ссылаться на какие-либо примеры, тем самым, оказывая влияния на управленческие решения, действия и поведение других. Такими примерами могут служить: стандарты, этика, общественное мнение, правовые акты, законы. Подобная ссылка призвана "помочь" другой стороне сделать "правильный вывод", вразумить, наставить на путь истинный — иными словами, принять психологическую установку, выгодную манипулятору. Кроме того, соответствующий пример может подтолкнуть оппонента к нужному действию (власть прецедента) или указать на вещи, запрещенные и недопустимые.

В современном мире ускользающим является сам феномен власти, основанной на вере и согласии. В отличие от традиционного общества, где власть искала поддержку в общественной морали, сегодняшнее административное управление осуществляется за счет регулярно возобновляемого насилия или манипуляции.

Во все времена правители всячески поддерживали легитимирующие идеологии, которые и были частью собственно механизма власти. Власть все-

гда заботилась о своей символообразующей функции: чтобы общество имело язык, на котором оно могло бы разговаривать, а также общественно признанные проекты будущего, способные регулировать тревогу неизвестности. Язык власти всегда несколько отличался от языка народа своей риторикой и опорой на ключевые символы.

Сейчас любой риторический дискурс, идущий от власти (или против нее), будет на утро деконструирован в газетах. Нет смысла употреблять риторику и ссылаться на общепризнанные авторитеты, когда назавтра газеты объяснят, что это все риторика и что за ней скрывалось. Риторика будет легко деконструирована из позиции прагматики, административной игры, из соображений кто и за кем стоит. По факту это означает отстранение правящей группы от претензий на сильную власть и длительную легитимность, что делает ее саму объектом для манипуляций со стороны международных финансовых и медиа игроков.

Процедурная власть — способность организовать процесс с поэтапными шагами, направленными на решение сложной проблемы или запутанного конфликта. Сила (человек, команда, организация, страна, группа стран), способная навязать собственную процедуру решения спорного вопроса практически стопроцентно гарантирует себе победу. Так в переговорах по урегулированию межнациональных конфликтов последних десятилетий достаточно взглянуть на состав посредников и предлагаемую процедуру переговорного процесса, чтобы еще до начала переговоров ответить на вопрос об их исходе.

В украинской внешней политике долгое время существовала ситуация фактического расщепления: когда на переговоры с руководством ЕС и НАТО ехала одна группа политиков, а на переговоры в Москву — другая. Только совсем недавно стал формироваться общий внешнеполитический дискурс, равно применимый как для переговоров с западными, так и с восточными партнерами.

Процедурная власть - очень серьезный тип власти, к сожалению, не достаточно используемый украинскими политиками. То, что ясно каждому мало-мальски грамотному бизнесмену: к важным переговорам нужно тщательно готовиться, беспрерывно уточнять свои интересы, выделять собственные главные и второстепенные вопросы для обсуждения, определять максимальные запросы и допустимые рубежи отступления (торга), навязывать партнеру свой сценарий ведения переговоров. Все эти простейшие вещи, используемые в переговорах ценой в десяток тысяч долларов, порой игнорируются в серьезнейших переговорах, касающихся миллионов государственных средств, национальных интересов в целом.

Экспертная власть - способность использовать знания, опыт и осведомленность в каком-либо вопросе для влияния на решения, поведение и действия других. Однако экспертная власть часто используется с неэкспертными целями.

В современном мире в качестве одного из ключевых инструментов реализации политики мягкого (непрямого) давления в отношении независимых государств выступает деятельность международных экспертных организаций, проводящих по всему миру разного рода оценочные исследования и экспертизы. Зачастую такие организации, зарегистрированные под вывеской научных фондов, независимых аналитических институтов и экспертных групп вырабатывают понятия и оценки, попадающие впоследствии в доклады политиков и чиновников высокого уровня.

Если данные, полученные от международной экспертной организации или фонда, используются в дальнейшем при принятии важных решений (например, об инвестициях или о предоставлении помощи), роль такой организации для оцениваемой стороны непомерно возрастает. В какой-то момент, подобно фонду Сороса в Грузии, такая организация может занять необоснованно высокое место в политико-государственной структуре страны. Нужно помнить о том, что даже те "независимые" фонды и аналитические структуры, которые сегодня не способны влиять на ход международных, региональных и внутригосударственных процессов, в большинстве своем стремятся обрести такое влияние.

В основе содержания отчетов подобных организаций находятся те или иные оценочные конструкты, в рамках которых проводятся измерения. Применяя подобные конструкты в различных ситуациях и по отношению к различным странам можно эффективно удерживать их в рамках скрытого манипулирования по шкале: "состоявшееся — не состоявшееся" государство. Например, если государство несговорчиво в плане экономических и внешнеполитических уступок, но при этом демонстрирует высокие темпы экономического и социального роста, его можно "измерить" по другой шкале: "приверженность демократическим ценностям" и т.д.

Для того чтобы оценочный конструкт не утрачивал своей эффективности как инструмент психологического и политического давления, его необходимо постоянно совершенствовать, делая все более сложным и наукообразным за счет создания новых шкал и факторов. Поэтому число таких шкал имеет тенденцию к неуклонному росту, а их названия приобретают порой гротескные формы. Так одним из социальных индикаторов, используемых агентством "Fund For Peace" для определения стран, приближающихся к определению ошибочных, является фактор: "Коллективная обида групп, стремящихся реализовать потребность в мести или групповая паранойя".

Имеются в виду, прежде всего, этнические и социальные группы, пережившие в прошлом незаконные притеснения и испытывающие сегодня последствия данной психологической травмы в виде повышенного фона социального недоверия и социальных страхов, а также склонности к проявлениям защитной агрессии. В данном случае, как и во многих других в подобных экспертизах, шкала измерения приобретает мерцающий, сугубо оценочный характер, предоставляя оценивающей стороне широкое поле для манипуляций.

Прежде всего, за рамки исследования выносится контекст исторической травмы, ее характер и причины. Государство или отдельные политические силы, участвовавшие в нанесении "исторической обиды", как правило, демонизируются, позиционируясь в роли преследователя в треугольнике: "преследователь – жертва – спаситель". Примером такого одностороннего позиционирования является демонизация югославских властей в период до начала и во время всей военной фазы косовского кризиса.

Всегда существует пространство для манипуляции в информационном преподнесении страхов, испытываемых той или иной этнической группой. Часто подобные страхи у "угнетаемых" этнических групп являются либо демонстративными трюками с целью привлечь к себе внимание международной общественности либо следствием (теневой стороной) собственных агрессивных намерений в отношении других этнических групп. Так, например, рост активности рассуждений об исторических притеснениях крымских татар, а также активизация их фобии преследования со стороны власти автономии часто происходит накануне новых самозахватов земли представителями крымскотатарской общины.

Одним из существенных отличий рассматриваемых экспертных оценок является зачастую полное игнорирование их авторами общего социального и экономического контекста, определяющего общественно-политическую ситуацию в стране. Так, игнорируя неэффективность слепого переноса неолиберальной экономической модели на постсоветское пространство как причину охватившего эти страны масштабного социального кризиса, международные эксперты сознательно или неосознанно проходят мимо вопиющих фактов абсурда и диспропорций в экономике и социальной жизни, одновременно акцентируя внимание на несущественных деталях.

Именно засилье с начала 90-х в правительственных органах постсоветских стран иностранных экспертов, стремление сверять свои решения с иностранными советниками или аналитическими центрами обусловило ряд известных экономических и социальных провалов. "Чрезмерная опека" притупила чувство ответственности местных руководителей, исказила выработанные опытом государственного управления собственные здравые представления о развитии страны, навязала некоторым управленцам иллюзорные (неактуальные или невыполнимые) цели.

Иерархическая власть. Необходимым условием осуществления этого типа власти является наличие формально закрепленной связи между сторонами - участниками властных отношений, - связи, предполагающей неравноценные позиции, социальные роли (отношения 1 – 0 по Э. Берну). Разноуровневые отношения, как и отношения равноценные, партнерские - явление, четко определенное и индексируемое во всех мировых культурах (отношения ребенок - родитель, ученик - учитель, проситель - кредитор, последователь - ведущий, стремящийся к идеалу - идеал).

Авторитет властных институтов в общественном сознании, являясь (психологически) продолжением родительского авторитета в семье, играет роль опорного объекта. Функция опорного объекта: объяснять и регулировать социальную реальность ("понимать, что и как нужно делать", а также "действовать разумно"). Социальные процессы обладают сами по себе внутренней интенцией к росту энтропии. Если энтропию искусственно усиливать, подвергая непрерывным информационным атакам властные институты, а также персонально отдельных лидеров и их управленческие решения – это в конечном итоге может привести к хаотизации общества.

Информационная атака на властные символы приводит к размыванию опорного объекта, что естественно усиливает нестабильность в обществе. До какого-то уровня общество способно нейтрализовать эти страхи, компенсируя данную угрозу. Однако по прохождении некоего рубежа – точки бифуркации, в стране могут начаться неуправляемые процессы взрывоподобного роста социальной энтропии, способные привести к непредсказуемым последствиям.

Кроме того, для осуществления властной функции необходимо наличие политической и психологической субъектности – суверенитета власти, допускающего строго ограниченную степень зависимости от внешних субъектов. Если эти границы нарушаются, совершенно естественно возникновение стремления у доминирующей стороны продемонстрировать свое властное превосходство над зависимой.

В этой связи вызывает изумление поведение некоторых политиков, болезненно реагирующих на менторские интонации в высказываниях представителей МВФ - организации, с которой Украина находится в отношениях проситель - кредитор (0 – 1). Столь же странными кажутся обиды на поучения или указания со стороны европейских властных институтов. А ведь именно мы неоднократно заявляли и продолжаем заявлять, что учимся у Европы демократии, учимся организовывать свою жизнь по-европейски, идем в Европу, стремимся быть принятыми в Европу (политическую и культурную, естественно, право относить себя к Европе географической мы вроде бы сохранили)? Мы сами проиндексировали собственную позицию ученика, последователя, просителя (0 - 1) и теперь возмущаемся, что нами пытаются распоряжаться.

Такое поведение в международной политике весьма рискованно. Если у нас есть проблемы с ролевой идентификацией, то на Западе с этим все в порядке. Непоследовательность в ролевых отношениях, завышенная претензия на зрелость, требования со стороны финансово зависимой страны равноправного, партнерского к себе отношения все чаще вызывают у "сильных мира сего" на Западе не прежнюю доброжелательную "родительскую" улыбку, а трудно скрываемое раздражение.

Раздражение вызывает также упорное неприятие объективной реальности – факта своей зависимости и незрелости. Мы помним, какой вздох об-

легчения на Западе вызвало заявление В. Януковича о том, что Украина не будет в ближайшее время атаковать ЕС своими требованиями о скорейшем принятии ее в эту организацию.

Власть вознаграждения и власть наказания - часто применяемые в политике типы манипуляции властными отношениями, предусматривающие произвольное, несанкционированное международной практикой использование вознаграждения и/или наказания для влияния на решения, действия и поведение лидеров других стран. Сюда относятся лесть, всевозможные политические авансы, раздаваемые публично или наедине, приглашения на престижные форумы и встречи "без галстуков", присуждение премий и награждение орденами, предоставление лечения, образования и отдыха для членов семьи и многое другое. На противоположном конце шкалы - угрозы, запугивание, давление на личность (компромат, оскорбления, карикатуризация и демонизация), а также другие приемы, традиционно относимые к сфере "черного PR".

Наглядным свидетельством комплексного использования приемов операционного манипулирования при разрешении конфликтов различной природы (международных, межнациональных, межэтнических, межконфессиональных и пр.) является концепция "многоплановой дипломатии". Согласно ей кроме "первого плана" (официального, государственного) действий по установлению мира, существует "второй план" - деятельность негосударственных структур, а также иные "планы" -сфера бизнеса, коммуникации частных лиц, область совместных исследований и образования, массовая политическая активность, сферы религии, филантропической деятельности и средства массовой информации.

В целом же манипуляции в международных отношениях, как правило, эффективно проводятся в отношении объектов (им может выступать общества отдельной страны или отдельные социальные слои, госаппарат в целом или его внешнеполитического ведомства и т.п.), которым присущи:

- фрагментированное сознание, неспособность воспринимать мир целостно и диалектически;
- искаженные механизмы рефлексии (т.е. способности адекватно отображать и осознавать действия и поступки как свои, так и чужие);
- трансформации нормативной базы сознания и критериальных механизмов оценивания.

Соответственно защита от манипулятивных воздействий должна базироваться прежде всего на:

- формировании национальной идентичности и идеологии защиты национальных интересов;
- формировании в элитарном, а при возможности и массовом сознании целостной картины мира. Технологически это связано, прежде всего, с созданием разветвленной системы информационно-аналитического обеспечения процессов принятия государственных решений;

- особом внимании к вопросам образования, прежде всего высшего, а также системе специальной психологической подготовки высших государственных чиновников.

Каждый потенциальный объект психологического манипулирования (начиная с отдельного человека и заканчивая страной или группой стран) должен осознавать, что лучшим средством.свести на нет все усилия манипуляторов является хорошее знание себя - своих интересов, целей и ценностей [215-218].

2.3. Язык международной политики как способ сотрудничества и манипулирования

Философско-методологическая сущность манипулирования. Во всех его всевозможных видах и формах манипулирование в межчеловеческих отношениях основано на квазисубъектности - той ситуация, когда объект межличностных и/или межгрупповых отношений продолжает мнить себя субъектом, хотя в действительности таковым уже/еще не являясь. Когда такой квазисубъект воображает себя свободным в жизненном выборе, став заложником манипулятивных ситуаций, исключающих свободу выбора "по определению", мнит себя управителем ("хозяином судьбы"), являясь на самом деле управляемым. В неразрывной связи с подобной квазисубъектностью находится феномен квазиполитики [219], включая и политику международную. Манипулирование в социально-политической практике неизбежно в той мере, в какой неизбежной является такая человеческая слабость как "бегство от свободы" и переход в состояние "добровольного рабства". Ведь свобода сопряжена с рисками и неопределенностью, тогда как рабство дарит иллюзию безопасности и полной определенности. Поэтому всегда будут находиться значительные группы людей, которые вопреки призывам стать "гордыми буревестниками", будут отдавать предпочтение "социальным машинам" манипулирования. Именно они добровольно выбирают участь "маленьких винтиков", "премудрых пескарей", "пингвинов, тело жирное прячущих в ущелье" и т.п. Если критическая масса таких, по определению Л.Н.Гумилева, "субпассионариев" слишком велика и часть из них обретает "элитный" статус, то малозавидная манипулитивная участь квазисубъектов может ожидать на каких-то витках истории даже целые страны, народы и континенты.

В современных политических коммуникациях, как это убедительно доказали Толкотт Парсонс и Юрген Хабермас, происходит трансформация объектов манипулирования. Ныне таковыми являются представители "новой публики", сами себе кажущиеся очень "раскованными", на которых массированное воздействие оказывают профессиональные манипуляторы, специализирующиеся в искусстве политической рекламы и лоббирования посредством масс-медиа партикулярных интересов. В результате, возникает феномен коммуникаций без "коммунальности". От диалогового субъект-субъектного дис-

курса общественно-политические институты переходят к монологовому режиму внушений на сознательном и бессознательном уровнях с использованием различных изощренных психотехник и психолингвистических приемов.

1. Манипулятивный комплекс. Манипулятор и манипулируемый образуют "сладкую парочку", - некую дуальную или полигональную целостность. Этот манипулятивный комплекс сродни хорошо известному психологам садомазохистскому комплексу и его психологической первоосновой, несомненно, является негативная самоидентификация. То есть идентификация не посредством собственного хорошо "заякоренного" индивидуального "Я" или коллективного "Мы", а посредством негативистского "не-Я", "не-Мы" и т.п. Не случайно, наиболее благодатными объектами всевозможного манипулирования являются инфантильные особи и, в частности, - подростки. Ибо им, ищущим "делать жизнь с кого", изначально присуще подобное негативное самоопределение со всеми вытекающими отсюда последствиями (негативизмом, максимализмом и т.п.). Как известно в своей трехуровневой схеме трансакционного анализа ("ребенок - взрослый - родитель") Эрик Берн весьма убедительно доказал, что в "играх, в которые играют взрослые", то есть сценариях всевозможного манипулирования, мишенью манипулятивного воздействия всегда выступает наш внутренний ребенок с его многочисленными "хотениями", не уравновешенными "возможностями".

2. Манипулирование и негативная национальная самоидентификация. Молодая украинская нация, пребывающая в подобном подростковом возрасте, в свою очередь, идентифицирует себя через всевозможные "не" ("Мы - не русские"; "Мы - не турки"). Даже попытки позитивной идентификации ("Мы - европейцы") немедленно влекут за собой негативы. В 1925 г. украинский поэт, национал-большевик Микола Хвильовый сформулировал известный лозунг "Геть от Москвы, - равнение на культурную Европу", который и поныне кажутся очень актуальным некоторой части украинских национал-патриотов. Против позитивной второй части этого лозунга возражать бессмысленно. Но почему, спрашивается, "европейское выравнивание" должно сопровождаться "бегством от Москвы"? Точно также непонятным, на первый взгляд, кажется утверждение в тексте украинского гимна, написанного Павлом Чубинским, которое сводится к тому. что только гибель врагов обеспечит украинцам господство на собственной земле ("згинуть наші воріженьки, як роса на сонці, запануємо ми браття у рідній сторонці"). Ведь задача ставится явно утопическая, поскольку дождаться полной гибели врагов еще не удалось ни одной нации. Но в том-то и дело, что для манипулируемого сознания крайне важным представляется бегство от юнгианской "тени", спроецированной на "Своего Иного". Такой "тенью" для украинцев какое-то время были турки и поляки. Затем на их место пришли русские. Вполне понятно, что незавершившийся переход украинской нации к позитивной самоидентификации создает удобную подпочву для манипулирования массовым сознанием украинцев. Впрочем, - как и постсоветским массовым сознанием в целом.

3. Манипулятивная фетишизация как бегство от реальности. В субъектном отношении с разной скоростью и разными результатами деградируют оба, - как манипулируемый, так и манипулятор. Они непременно становятся заложниками фетишей средств манипулирования, означающее "бегство от свободы" или "бегство от реальности" (в данном случае это понятия однопорядковые).

Манипулирование и фетишизация - две стороны одного целого, поскольку с необходимостью подразумевают друг друга. Фетишизация, как известно, означает обретение мертвыми объектами магических жизненных смыслов и значений, тогда как жизненные объекты, напротив, превращаются в искусственно безжизненные, хотя (благодаря тем же фетишам) продолжают усиленно имитировать "живую жизнь". Манипулятивные "стратегемы" как и сводятся к тому, что "мертвое хватает живое", а лишенное жизни делает вид, что "живее всех живых".

Не случайно известный пролетарский поэт приписал подобную "сверхжизненную силу" ("наше знанье, сила и оружие") некой мавзолейной мумии, которая, будучи сверхфетишизированной советской правящей верхушкой, на протяжении нескольких десятилетий, вела страну "правильным курсом". Уже сам тот факт, что советские лидеры ритуально наставляли восторженные толпы манипулируемых во время парадов и шествий, водрузившись на Мавзолее, говорит сам за себя.

Итак, первейшая опасность заключается в том, что манипуляция убивает жизнь, подменяя ее жизнеподобными фетишами, нарушает естественное развитие событий и ситуаций, подменяя естественного человека и естественное общество их искусственными дериватами.

4. Языки манипулирования. Средств и технологий манипулирования предостаточно. Но наиболее действенное среди них - язык. Особое распространение лингвистические психотехники манипулирования приобрели в XX веке, добрая половина который прошла под знаком засилья тоталитарных идеологий. Не случайно советский диктатор Иосиф Сталин на старости лет пришел к убеждению, что является крупным специалистом "в языкознании познавшим толк". Недавно ушедший в сферу "исторического бытия", XX век вообще заслужил репутацию века "словарной инфляции", передав это сомнительное наследие новому веку.

Способ подачи информации об окружающей реальности сплошь и рядом деградирует до пустого, "простого, как мычание" звука. Способов подачи информации становится все больше, а содержательной реальности в передаваемых сообщениях все меньше. Герберт Маклюэн выразил эту ситуацию в удачном афоризме "Сообщение само является содержанием".

В результате, остро встает проблема дезинтеграции мировосприятия, когда символ и имидж существуют вне прямой взаимосвязи с сущностью предмета. В духе подобного чрезмерного резонерства оценки и комментарий предшествуют фактам, а иногда даже их подменяют. В особенности этой свойственно практике партийно-парламентской риторики.

Философской модой XX столетия стало противопоставление реальности не сознанию, а именно языку. Возникла даже гипотеза лингвистической относительности (Сепира-Уорфа), в соответствии с которой не язык определяется реальностью, а реальность - языком. Тотальность такого "оязыковления" реальности подвела к логическому выводу, что межчеловеческие отношения не строятся свободными в своем выборе субъектами, а всецело определяются знаковыми системами, в паутине которых "запутались" эти субъекты.

Такая "паутина" называется дискурсом. Знаковыми фигурами становятся не только социальные институты, но и сами люди как знаково-символьные носители определенных типов отношений. В итоге, получается, что вся ткань социальных отношений состоит из сплошных дискурсов, - политических, экономических, конфессиональных и т.п. Дискурс - своеобразная знаково-манипулятивная машина и, перефразируя известное выражение, можно заявить: "Скажи мне, в каком пребываешь дискурсе, и я скажу кто ты".

Действительно, как знаково-семантическая система язык не только создается людьми, но и сам создает людей и межчеловеческие отношения. Он непосредственно влияет на осмысление и оценку внутренних и международных событий. Он является способом создания разнообразных символов и имиджей, организации политических дискурсов и особым искусством "называть вещи не своим именем", именуемое политической корректностью, которая фактически сводится к употреблению разнообразных эвфемизмов, - словесных формул, которые было бы весьма рискованно толковать в их непосредственных смыслах и значениях.

На языке подобной политкорректности денежную эмиссию называют "умным управлением денежной массой", войну - "гуманитарной акцией", безнадежно отсталые страны - "развивающимися" и т.п. Американцы, придумавшие эту "корректность", иногда даже шутят, что на этом "птичьем языке" труп - это на самом деле и не труп вовсе, а "организм с особым обменом веществ".

Как средство психосемантичного манипулирования язык эффективен прежде всего потому, что, неся в себе "живую жизнь", одновременно отягощен различной "мертвечиной" в виде языковых стереотипов, бессодержательных абстракций, ложных символов и т.п. Поэтому он неотъемлем от манипулятивной политики и властных манипуляций. Особенно нагружен подобными образами психосемантического манипулирования язык международной политики.

Не случайно дипломатию иногда характеризуют как искусство овладения специфическим языком, способным скрывать настоящие мысли и намерения дипломата и, вместе с тем, создавать иллюзию конструктивной содержательности. Правда, такое толкование "вершин" дипломатического искусства в сегодняшнем неделимом или "полуделимом" мире с его прозрачными или полупрозрачными границами надлежит признать анахроничным. Ибо старая формула манипулятивной дипломатии, не раз уже подводившая мир к опасной черте войн и конфликтов, заставляет вспомнить поучительную

притчу о строителях Вавилонской башни, которых постигло "смешение языков".

Поэтому вовсе не исключено, что дипломатия, перегруженная двусмысленной манипулятивной психосемантикой, в свою очередь, может превратить строителей "нового мирового порядка" в устроителей "нового мирового беспорядка".

5. От "деспотической речи" - к "манипулятивной демократии". Влияние политики и властных отношений на структуру и функции языка побудило Ролана Барта разделить языки на энкратические, сформированные под конкретные запросы власти и нужные ей идеологические механизмы и акратические, призванные противодействовать тем, кто осуществляет власть. Энкратические языки - это по большей части языки всевозможных утопий включая и маркетопию, - столь модную нынче на постсоветских пространствах рыночную утопию.

Анализируя специфику политического языка, С. Зимовец заметил, что произвольные статистические выборки политических выступлений указывают на их языковую чрезмерность вплоть до 95-99%, что "отвечает проценту чрезмерности при олигофрении где резонерство имеет терапевтически компенсаторный характер" [220]. Не следует, конечно, спешить с выводом о дебильности политиков. Речь идет о другом - о стремлении "дебилизировать" реципиентов информации, чтобы как можно успешнее манипулировать их поведением и мировоззренческими стереотипами. Чем менее селективной и более массовой (стало быть, неопределенной по своему мировоззренческому "фону") является аудитория политика, тем более он склонен прибегать к подобной запутанной, языково избыточной аргументации.

В этом "бегстве от определенности", есть, безусловно, свои веские резоны. В отличие от политолога или политического аналитика, который может себе позволить "роскошь" логически стройных, семантически экономных открытых текстов, политик вынужден строить тексты закрытые (герметичные), рассчитанные на адекватное понимание лишь той частью людей, которые "посвящены" в истинные цели и намерения такого политика.

Понятно, что подобная политическая речь является сомнительной привилегией только режимов "манипулятивной демократии". Откровенно тоталитарным политикам такие изысканные приемы манипулирования ни к чему.

Комментируя сталинские театрализованные политические процессы 30-х гг., Валерий Подорога очень точно подметил особенности "деспотической речи": "Слово не является тем, что можно произносить свободно, в разбросе колеблющихся, условных семантических потоков. Слово включается в жесткое сцепление деспотического письма. Произносимое слово - признание - приговор" [219].

Не случайно тот диктатор, который "в языкознании познал толк", часто цитировал выражение "Кто хорошо понимает, тот хорошо излагает". Конечно, он имел в виду тех, кто "хорошо понимал" его личные цели и намерения. "Недопонимающих" ждал ГУЛАГ.

Синдром "деспотической речи" вряд ли уместно смешивать с "естественностью" политического языка. Напротив, он становится заложником борьбы диктаторских режимов за мнимое языковое превосходство. Именно поэтому деспотичные правители никогда не оставляют в покое деликатную сферу языка и культуры, чтобы позволить им развиваться чисто природным способом. В послушных режиму деятелях культуры, которых они более-менее щедро "прикармливают" (в отечественной традиции они именуются "интеллигенцией"), такие правители всенепременно видят "инженеров человеческих душ".

Психолингвисты давно уже подметили непосредственную связь между политическим деспотизмом и избыточной нормативностью, некой усредненностью языка. Понятно, что протестным образом у манипулируемых нарастает тяга к языку ненормативному.

Чрезмерная насыщенность русского и украинского языков всевозможными прилагательными и, напротив, - их бедность по части имен существительных (даже этноним "русский" является не существительным, а прилагательным) являются наглядным подтверждением вышеназванного тезиса. Дефицит имен существительных приходится время от времени компенсировать заимствованиями из иностранных языков. Ныне это происходит, главным образом, за счет англоязычных заимствований, которые разрывают живую ткань естественных национальных языков и несут в себе немалую угрозу манипулирования уже не только на внутреннем, но и одновременно на внешнем уровне. Доходит даже до трагикомизма, когда часть "языковых патриотов" в борьбе с украинско-русским билингвизмом, более-менее естественным для ныне сущих в Украине поколений, предлагают использовать украинско-английский билингвизм.

Итак, за языковой избыточностью "манипуляторов от демократии" прячутся более-менее умело замаскированные "коды", направленные на создание у реципиентов ложного ощущения "информированности". Политик не хочет наступать на "любимые мозоли" уже состоявшегося или потенциального электората, потворствовать своим оппонентам и т.п. К примеру, чтобы избежать революционной ситуации, консервативный политик может включать в свою речь "избыточно хлесткую" псевдореволюционную или псевдореформистскую фразеологию, памятуя, что лучший способ уничтожить какое-либо политическое движение заключается в том, чтобы самому его возглавить.

6. Текстовая и внетекстовая реальность внешнеполитического манипулирования. Наиболее демонстративные типы и приемы манипулирования в международных отношениях связаны с "политикой кнута и пряника", которая приобретает формы несанкционированных международной практикой вознаграждений и/или наказаний для эффективного воздействия на решения, действия и поведение лидеров других стран. Сюда относятся льстивые характеристики, политические авансы (раздаваемые публично или наедине), пригласительные билеты на престижные форумы и встречи "без галстуков",

присуждение премий и награждения орденами, предоставление возможностей лечения, образования или отдыха в престижных учреждениях для политика и членов его семьи и т.п. На противоположном конце шкалы - угрозы, запугивания, давление на личности лидера и его окружения (компромат, карикатуризация, демонизация и т.п.), другие приемы "черного PR".

Изобретаемые каждый раз заново под длительные международные политические акции глоссарии (англ. - "vocabulary") - эти своеобразные "новоязы" в оруэлловском смысле - перегружены элементами образной выразительности. И это отнюдь не случайно. Уже известный структуралист Роман Якобсон обосновал значение элементов иконизма (образной выразительности) в естественных языках, особое внимание обратив на склонность реципиента информации некритически вносить текстовую логику во внетекстовую, а языково-формальные связи проецировать на реальные связи между действительными событиями и явлениями. Таким образом, структура языка непременно переносится на структуру объектов, что хорошо освоили политические технологи современности.

Еще большее значение в контексте языковой виртуализации имеет сюжетность, то есть внесение во внетекстовую реальность определенной субъективной логики. Однако, в случае идеологического кодирования между автором текста и его реципиентами обязательно возникают барьеры декодирования, - максимальные на идеологическому равные и минимальные на иконическом [221].

Именно это почти полное отсутствие барьеров декодирования на базисном иконическом уровне подвело политических психотехников к искусству навешивания на уши потенциальных реципиентов "виртуальной лапши" в малозаметных модификациях природно-языкового иконизма. Типичным примером является искусственная драматизация проблем геополитического выбора Украины частью западных политиков и западной прессы, когда акцент ставится на том, что слово "Украина" означает, мол, "*пограничная земля*". Отсюда делается вывод, что Украина уже "психосемантически" обречена на пресловутый "буферный статус", на то, что превратиться в поле битвы между Востоком и Западом. В этом случае отправным пунктом анализа является не реальное состояние событий и фактов, а топоним, якобы символизирующий украинскую "пограничную маргинальность", что затем тем успешнее производить психосемантическое манипулирование этим "пограничным" кодом.

7. Виртуализация и манипулятивные симулякры. До тех пор, пока власть предержащим, руководствуясь идеологически оправданными целями, будет выгодно перемещать людей в пределы виртуальной реальности мифов и симулякров, носители власти с необходимостью будут изобретать всевозможные оруэлловские "новоязы". Более-менее удачный термин "симулякр" изобрел один из метров современного постмодернизма Жак Бодрияр. Соответствующую психотехнику он ярко продемонстрировал в работе с красноречивым названием "Войны в Персидском заливе не было". Этим названием

Ж.Бодрияр вовсе не хотел сказать, что такой войны не было "в помине". В его работе речь шла о другом. О расхождении образа этой войны, который " американский (и не только американский) обыватель воспринимал в режиме "реального времени на экранах своего домашнего телевизора из сообщений CNN, с реальными событиями этой войны. Симулякры в толковании Ж.Бодрияра - это создаваемые властью за подспорьем масс-медиа виртуалии, выполняющие роль своего рода эфемерных мифологем "на злобу дня". Симулякр - нечто мифоподобное, но этот не сам миф. Скорее, это его пародирование, которое строится на "костях" погибших мифов. В подобный симулякр когда-то превратился "коммунизм". В такой же симулякр рискует превратиться "манипулируемая демократия" [221].

В последнее время на отечественном телевидении тоже начали появляться сюжеты на политические темы, связанные с апелляцией к интересам массовой аудитории, мысли которой подаются как некий vox populi. На самом деле речь идет об активной игре в симулякры, призванные "легитимизовать" или мысль ведущего телепередачи или, скорее всего, намерения его заказчика. Ни одна реальная аудитория в передаче участия на самом деле не принимает, а есть лишь воображаемый образ этой аудитории, то есть миф, который выдумал для себя и на потребу своему заказчику журналист. Изредка "секреты Полишинеля" из этой "телекухни" стают достоянием гласности.

8. Манипулирование международными рейтингами и показателями. Если изучать списки развитых стран, предлагаемые различными think tanks, то можно окончательно запутаться, поскольку их количество будет колебаться от 22 до 35, в зависимости от предпочитаемых критериев "развитости". Вполне понятно, что подобные критериальные оценки являются отнюдь не объективными, а непосредственно выражают манипулятивные цели и намерения "аналитиков" и их заказчиков.

К примеру, столь нелюбимая США кастровская Куба имеет показатели социального развития, соответствующие испанским или шведским и во многом превосходящие американские. Недавно это вынужден был даже признать президент Мирового банка (МБ) Джеймс Вольфенссон [222].

В распространенном 29 апреля 2001 г. 200-страничном обзоре МБ "World Development Indicators", Куба указана как пример "бедной страны с высокими показателями развития здравоохранения и образования". И тут же авторы доклада жалуются, что как только эта страна примет мировые условия "свободной торговли (trade off) ее социальные показатели немедленно покатятся вниз. Но ведь эту же trade off как панацею для экономического оздоровления как раз и навязывают развивающимся и "переходным" странам эксперты-манипуляторы МБ, МВФ и других подобных организаций.

Особняком в различных мировых "табелях о рангах" стоят "переходные страны" с Украиной включительно. Лондонский The Economist Intelligence Unit отводит Украіне 52 позицию в перечне 60 стран, относящихся к развитым и "переходным", что примерно соответствует экономическому развитию Ирака.

Следует заметить, что западные think tanks, начиная с 2000 г., вообще начали отводить Украине по всем показателям политической и экономической свободы более чем скромные позиции. Например, по данным The Heritage Foundation индекс экономической свободы в Украине упал в 2000 г., по сравнению с предыдущим, сразу на 17 пунктов. Учитывая, что определявшее в 2000 г. экономическую политику правительство Виктора Ющенка теми же западными think tanks (а затем и западными масс-медиа) было признано "наиболее реформистским", невольно напрашивается вывод о манипулятивной ситуации. Причем такого рода, когда "правая рука не знает, как манипулирует левая".

Из 191 стран мира, по состоянию на 2000 г., 126 относились к реципиентам экономической и финансовой помощи, причем больше половины этих реципиентов уже "созрели" до уровня "тяжело задолжавших стран" - их долги признаны безнадежными и "Большая Семерка" на саммите 1999 г. решила их списать. Украине, внешний долг которой составил к концу апреля 2001 г. US$13 млрд., подобный аутсайдерский статус пока не угрожает, хотя на выплату процентов по долгам уже приходится отдавать 9% валютной выручки от экспорта. Предоставление же новых международных кредитов стало предметом длительного торга с нескрываемыми попытками вмешательства во внутренние дела страны.

Кстати, принадлежность к эксклюзивной "Большой Семерке", которую, как будто, пытаются превратить в "Большую Восьмерку", тоже является предметом откровенного манипулирования. "Восьмой", как известно, посчитали Россию, но при условии, что она будет себя "хорошо вести". Поскольку Россия путинская не столь сговорчива, как Россия ельцинская, то уже накануне Окинавского (2000 г.) саммита предлагалось поменять Россию на Китай. В свою очередь, накануне Генуэзского саммита 2001 г. новым попыткам исключить Россию из "эксклюзивного клуба" воспрепятствовала страна-хозяйка Италия.

Таким образом, язык "манипулятивной социологии", столь популярный на украинской "внутренней кухне", пользуется не меньшим спросом и на "международной кухне". Особенно, когда речь идет о различных показателях развитости и неразвитости, экономической и политической свобод, уровней коррумпированности и т.п., по которым западные аналитические центры (think tanks) ранжируют страны и народы [223;224].

2.4. Манипулятивные технологии воздействия на общество и методы противодействия им (мнения экспертов)

Мнение первое. Манипулофобия – довольно позднее явление. Лишь несколько лет тому назад страх перед манипуляциями достиг в нашей стране критического уровня, заставившего выделить манипулятивные технологии в

отдельный срез социокультурной реальности. Тема манипулятивных воздействий обычно остро переживается не только в среде образованных людей, имеющих лишь косвенное отношение к разработке и использовании манипулятивных технологий, но и в среде специалистов, которые, казалось бы, должны холодно и профессионально относиться к продуктам своей работы и их последующему использованию. По сути дела, именно эта иррациональная тревога отделяет собственно манипуляции от огромного массива способов формирования личностных структур, культурных и поведенческих норм, предпочтений и представлений о приемлемых и неприемлемых формах поведения, лежащих в основе любой культуры.

Эти способы, как и манипуляции, также реализуются в поле, лежащем за пределами осознанных и критических оценок внедряемых форм поведения и ценностей, но не вызывают той тревоги, которые вызывают целенаправленные попытки изменить культурные нормы отдельных социокультурных групп при помощи средств массовой информации, сетей распространения слухов и анекдотов или технологий воздействия на бессознательные структуры человеческой психики.

Часто бывает трудно отделить культурный текст, повествующий о манипуляциях, от собственно разработки манипулятивных техник. "Князь" Макиавелли — это явление культуры, а инструкция по проведению боевых информационно-психологических операций — пособие по манипулятивным воздействиям. То же самое можно сказать и в отношении политической практики. Жесткие методы унификации поведения и внутренних ценностей в условиях тоталитарных режимов вызывают протест, но отнюдь не страх перед манипуляциями, характерный именно для периодов либерализации обществ.

Характер основных опасений может быть выведен умозрительным путем, поскольку одинаковая картина мира у представителей одной и той же этнокультурной системы предполагает и сходную реакцию на одинаковые стимулы, в частности, на ставшее для современного человека сильным стимулом слово "манипуляция". Однако разные люди выделяют в качестве основных разные стороны одного и того же явления. В 2001 году нами был проведен анализ 20-ти сочинений на тему "Почему для меня неприемлемы манипуляции и чем манипуляции отличаются от других форм взаимодействия людей между собой". Половина этих сочинений была написана студентами факультета прикладной психологии Университета эффективного развития (лица с высшим образованием в возрасте 25 — 40 лет, ориентированные на получение высшего образования по специальности "психология"), половина — активистами политических партий и организаций умеренной направленности. Если отвлечься от проекций индивидуальных проблем, основными были названы три причины опасений. Рассмотрим их и прокомментируем.

Первый тревожный момент связан с механическим характером манипуляции (цитаты из сочинений: "мне не нравится, что на мне как на клавиатуре можно нажать на клавишу и получить автоматический ответ", "манипуляция

как невидимая клетка, из которой нельзя вырваться потому, что ее не видишь", "меня оскорбляет, когда со мной обращаются как с вещью, а не с живым человеком" и т.д.).

Известны по меньшей мере три типа картин Мира, проистекающих из них концепций и технологий воздействия на окружающий нас мир: Мир как машина; Мир как живой организм; Мир как воля. Воздействия, которые могут быть расценены в машинной картине Мира как манипулятивные, в организмической картине выступают как естественные моменты культурного процесса, придающие культуре вполне определенную форму. Таковы культурные образцы, внедряемые в сознание людей с момента их рождения при помощи достаточно сложной и изощренной педагогики – начиная с управления процессом освобождения от продуктов жизнедеятельности, до формирования чувства вины и норм боевого товарищества и проч.

Организмические приемы формируют структуры сознания (и формирователь естественным образом остается за пределами этих структур), а механические – поведение, неконтролируемое сознанием (и формирователь поведения замещает собой волю и интеллект манипулируемого). Манипуляция механична по своей природе и именно это ее свойство рассматривается как угрожающее со стороны носителей немашинных, немеханических картин Мира. Проблема не в том, что манипуляция вынуждает объект манипуляции совершить нечто ему не свойственное (действие во внешней среде или изменение ценностей и целевых установок во внутренней), а в том, что манипуляция придает своему объекту машинный характер, что со стороны носителей организмических и волевых картин представляется как понижение онтологического статуса. Машина с точки зрения носителей организмического взгляда на мир ниже по своему статусу, чем организм, а с точки зрения волюнтаристического подхода организм ниже, чем воля. Таким образом, тревога в отношении манипуляций обусловлена наличием лиц с выраженным организмическим или волевым началом и не желающим уподобляться механическим системам.

Вторая причина тревожности нашей темы, расширяющая круг озабоченных манипулятивной проблематикой лиц - отсутствие точки отсчета, по отношению к которой личность выстраивает и свой онтологический статус и характеристики психического состояния ("я не знаю, где моя мысль, а где, внушенная телевизором", "страшно то, что невозможно отличить свои представление от навязанных", "я не знаю, кто прав на самом деле, а манипулятор быстренько мне все объяснит" и т.д.).

Секуляризация общественной жизни привела к размыванию, а в ряде случаев и к исчезновению абсолютных начал внутренней жизни личности. Истина стала относительной и множественной (процесс этот закреплен постмодернистской методологией и отражающих ее идеологий). Тысячелетняя церковная практика выработала методы, позволяющие сопротивляться внешним по отношению к личностному сознанию воздействиям (рассматри-

вая их как бесовские влияния). Но если раньше корпус христианских ценностей позволял отделять Истину от посторонних влияний, то с исчезновением абсолютной Истины (как факта если не индивидуального, то общественного сознания) исчезает и та точка отсчета, по отношению к которой можно произвести оценку правильности или неправильности той или иной установки или желания. Последствия посторонних влияний более не отличаются от личных страстей и порождаемых ими решений. Не имея возможности различить, что порождено его сознательной деятельности, а что является результатом воздействия, человек оказывается беззащитным перед влияниями, которые отныне называются манипуляциями.

Третья причина современной манипулофобии — криптократический дискурс, сформированный еще в восемнадцатом веке в масонской концепции тайной власти ("я не хочу жить в мире, где все, что происходит, придумывается никому неизвестными политиками и финансистами", "в мире все вычислено и все под контролем. Все, что можно придумать уже вычислено", и т.д.). Представление о тайном влиянии на ход истории имело своим последствием не только возникновение многочисленных конспирологических теорий, но и, как отражение этой концепции в культуре, формирование психоаналитических представлений о бессознательном, управляющим сознательными процессами.

Действительно, если бессознательные установки на самом деле определяют якобы осознанные мотивами, то доступ к бессознательным структурам должен обеспечить контроль над поведением в пользу манипулятора, замещающего собой бессознательное. Именно введение понятия бессознательного позволяет, с одной стороны, разрабатывать методы манипуляции сознанием, а с другой стороны, создает необходимые предпосылки для такой манипуляции — бессознательному приписывается более органический и всеобъемлющий характер по сравнению с осознанными структурами. Для безрелигиозного сознания бесссознательное становится чем-то более реальным и более ценным, чем рациональная сторона жизни, оно вызывает большее доверие, нежели сознательно сформулированные цели. Тем самым и невидимый манипулятор получает санкцию на воздействие, которой он был лишен в традиционном обществе.

Очевидно, есть и другие причины. Однако констатация, по крайней мере этих трех причин, создает предпосылки для разработки технологий выявления манипуляций и противодействия им. Выявление манипуляции — это выявление механичности, стереотипности и чужеродности изменений в установках и подходах. Но это возможно лишь при восстановлении ценностей воли и ясного, не подверженного никаким воздействиям извне сознания, соотносящего себя с абсолютными ценностями бытия. Чисто технологических предпосылок для этого недостаточно. Предпосылками контрманипулятивных технологий может стать только целенаправленное изменение культурной ситуации, без которого любые технические приемы останутся лишь локальны-

ми паллиативами. Изменение, которое представляет собой формирование новых культурных механизмов, надстроенных над текущей ситуацией и преодолевающих тотальность манипуляций.

Такое изменение требует наличия культурной и политической элиты с четкими ценностными и метафизическими нормативами. Ее же отсутствие делает саму задачу построения контрманипулятивных программ не на частном, а на государственном уровне, заведомо безнадежным делом. В нашей ситуации даже вопрос о том, являются ли принимаемые на высшем уровне решения продуктом собственной интеллектуальной работы или же это результат внешней манипуляции, не может рассматриваться как осмысленный вопрос. Манипулятивные техники стремительно развиваются, захватывая все новые и новые сферы, ранее принадлежавшие естественным процессам и отсутствие абсолютных точек отсчета в сознании элиты позволяет всегда найти подходы к управлению ее поведением.

На наших глазах происходит глубокая эрозия культуры как самодостаточного феномена и преобладающим и самодостаточным становится технологический мир. В случае появления в государстве элиты как ответственного и высокосознательного слоя, она с неизбежностью должна начать беспрецедентный в истории процесс — восстановления культуры и религиозной жизни в условиях их повсеместного закономерного угасания. Помощником здесь может стать концепция альтернативных технологических миров.

Концепция исходит из неустранимости из человеческого сообщества ценностных и метафизически ориентированных установок, которые продолжают свое существование несмотря на последовательную смену языков, на которых они выражаются. Те ценности, которые когда-то выражались на языке религиозных систем и верований, а позже — на языке культуры, ныне начинают выражаться на языке технологий. Памятуя о неизбежном противостоянии различных картин Мира и несовместимых религиозных и метафизических установок, мы вынуждены предположить, что это противостояние будет оформлено со временем как противостояние различных технологических миров. Если сейчас технологии являются проекцией видения Мира как механической машины (отсюда и механические технологии клонирования и трансформаций генома в биологии и механические же, пригодные для организации манипулятивного воздействия, техники нейролингвистического программирования в прикладной психологии), то противостоящие им технологические миры должны взять за основу кардинальные свойства живого и психического.

Первые шаги по формированию альтернативных технологических миров уже делаются — доктрины психонетики [225] (технологии, использующие для решения конструктивно поставленной задачи особые свойства человеческой психики, позволяющие преодолевать ограничения, обусловленные строением как психофизиологических систем восприятия окружающей среды, так и языков описания объектов различной природы), организмики (технологии управления процессами, протекающими в организмических объектах, в том

числе морфогенезом живых организмов, эволюции этнических и культурных систем и т.д.), универсального природного цикла [226] (информационно-энтропийной системной концепции, декларирующей фундаментальные законы развития и эволюции систем любой природы) и тоталлогии [227] (рассматривающей проблематику сохранения идентичности тотальностей, претерпевающих различные трансформации), не только изложены, но и начинают уже получать практическое воплощение. Так, психонетика позволяет строить заданные знаковые системы, позволяющие воспроизводить в знаковой модели кардинальные свойства моделируемого (или, точнее, отражаемого) живого или сознательного существа или социокультурной общности. Таким образом, формируются «языки», позволяющие выявить и ассимилировать механические и чужеродные элементы, на которых основаны известные нам манипуляции. Предпосылки для преодоления мира манипуляций могут созреть только внутри этого нового мира организмических и психонетических технологий, поскольку в сознании их носителей (а именно они озабочены и встревожены внедрением манипулятивных воздействий в социокультурную практику) организмический и психонетический миры надстроены над машинным миром, а, следовательно, должны располагать и средствами нейтрализации возможных манипуляций [228].

Но до того как эти иные технологические миры возникнут, манипуляции в известных нам формах будут оставаться неотъемлемым и стремительно расширяющимся компонентом социальной практики. Уже сейчас наше общество сталкивается с элементами грамотного воздействия на массовое сознание, использующего результаты исследований в гуманитарных науках. Приведем только три примера.

В последнее время наблюдается широкое использование в визуальной рекламе персонажей, принадлежащих к различным расовым типам. Не составляет труда понять, что этот прием, ничем не оправданный с точки зрения повышения эффективности воздействия рекламы на покупателя, готовит население к принятию идеи многорасового общества как первого шага к обретению статуса переселенческой страны. Не обсуждая правомерность такого проекта, отметим, что изменение подспудных установок населения производится без согласия самого населения и даже без вынесения этой темы на обсуждение.

Второй пример - внезапное появление обширной серии анекдотов об Иисусе Христе, подрывающих (за счет используемой иронии и снижения восприятия сакрального образа Спасителя до уровня обычного человека) основные ценностные ориентации культуры христианской страны. Одновременное появление большого количества анекдотов с "дозированным" уровнем иронии заставляет заподозрить не спонтанное, а целенаправленное их производство.

Третий пример – из недавнего прошлого. На протяжении 1999 – 2000 годов одновременно во множестве периодических изданий появились публи-

кации, сочувственно связывающие девиантное сексуальное поведение с образами наиболее популярных зарубежных артистов. Учитывая использующийся при этом феномен отождествления зрителя с любимым актером, можно предположить, что следствием этих публикаций будет либерализация отношения общества к носителям сексуальных отклонений и. как следствие, подрыв традиционных этических и эстетических установок народа, ставшего мишенью этой, казалось бы, безобидной атаки.

Как показывает опыт, разрыв теоретического исследования и разработки на его основе техники целенаправленной манипуляции составляет 15 - 20 лет. Какие же разработки последнего десятилетия XX века могут стать основой будущих манипулятивных приемов? К ним можно отнести, по меньшей мере, три направления психотехнических разработок, при этом наверняка многие абстрактные разработки, не попадающие в поле нашего внимания, обладают еще не распознанной манипулятивной потенцией.

Во-первых, это окончательно оформившиеся в начале 90-х годов XX столетия технологии, включающие в себя эффективные методы выявления бессознательной структуры и бессознательных значимых психических содержаний, методы ввода неосознаваемой информации, трансформирующей бессознательные структуры и меняющие глубинные поведенческие и ценностные установки людей [229]. Их адаптация к манипулятивной практике позволит повысить эффективность воздействия на массовое поведение.

Во-вторых, созревшие к концу 90-х годов психонетические технологии, позволяющие (при наличии определенных условий), создавать абстрактные визуальные образы, способные к самопроизвольному разворачиванию в сознании человека в сложные знания и навыки. В свете манипулятивных подходов не видно принципиальных препятствий для их превращения в своего рода информационно-психологические вирусы, вносящие в сознание людей новые идеи, убеждения и ценностные ориентиры и обеспечивающие целенаправленное распространение новых культурных норм и стереотипов.

В третьих, исследование различных форм и условий формирования измененных состояний сознания, экспериментальная отработка соответствующих психотехник и успешное использование полученных результатов в рамках синергетического подхода для разработки технологий провокации целенаправленных процессов личностной трансформации.

Не забудем и о ждущих своего доктринального оформления психотронных разработках. Появление концептуального и теоретического аппарата, описывающего соответствующие феномены переведет исследования из разряда маргинальных фантазий в технологическую сферу. Но это, очевидно, дело более отдаленного будущего. Современная манипулофобия представляется явлением, предвосхищающим этот грядущий мир.

В своей совокупности психотехнологические разработки приведут к формированию в течение ближайших 10 — 20 лет к новому массиву манипулятивных технологий и резко повысят манипулятивный потенциал госу-

дарств, обеспечивающих соответствующие НИР и ОКР. К этому необходимо готовиться и думать о разработке технологий выявления и подавления такого рода воздействий - контрманипулятивных технологий.

Рассмотрим общую схему выявления манипулятивного воздействия. Каковы кардинальные отличия манипуляции от других форм взаимодействия отдельных людей? В представлении о манипуляции с самого начала содержится противопоставление естественного и искусственно вызванного процессов. Следовательно, методология выявления манипулятивного воздействия должна включать в себя различение естественной траектории развития системы и возмущающих воздействий, деформирующих естественное развитие. В этом пункте и приходит на помощь представление о трансформации системы, сохраняющей ее индивидуальность, почерпнутое из концепции тоталлогии. Тоталлогия создает методологические предпосылки для разработки технологий различения естественного и искусственного, предлагая методы оценки сохранения идентичности объекта при его преобразованиях, в том числе и при воздействиях на него извне.

Концепции универсального природного цикла и тоталлогии дают представление о том, как строить процедуры ранжированной оценки степени манипулятивного воздействия на объект качественной оценки. В рамках концепции универсального природного цикла есть положение о резонансном взаимодействии системы с чужеродной информацией. В условиях этих взаимодействий степень дифференцированности и организованности системы снижается до уровня, позволяющего "растворить" механизмы отвержения чужеродной информации. Всякий раз, когда мы сталкиваемся с успешным манипулятивным воздействием, мы фиксируем именно это состояние снижения дифференцированности системы, "морфинг", говоря языком тоталлогии. Психологически это проявляется в инфантилизации психики, возврате к стереотипам поведения и оперативного реагирования, характерным для более ранних стадий развития человеческих сообществ, специфической ценностной дезориентации отдельных людей.

Психонетика также дает примеры разработки конкретных техник выявления воздействий и их нейтрализации в отношении отдельных людей.

Примером могут служить психотехники деконцентративного ряда, позволяющие выделить целостные, не получившие отражение в дискретных параметрах, характеристики системы.

Основой деконцентративных психотехник является целенаправленно формируемый процесс равномерного распределения внимания по полю перцептивных стимулов любой природы. Отвлекаясь от технических тонкостей, отметим, что результатом деконцентрации является разрушение организованных целостностей в сферах восприятия, формирования когнитивных конструкций и т.д. В состояниях глубокой деконцентрации мир предстает как единый слитный недифференцированный фон, из которого можно извлекать слабые, скрытые или замаскированные стимулы, т.е. те стимулы, которые яв-

ляются основой манипулятивного воздействия. Техника деконцентрации пригодна для выявления скрытых воздействий, в том числе и бессознательного плана. В ряде экспериментальных исследований было показано, что применения деконцентрации позволяло выявлять подпороговые стимулы и обнаруживать скрытые от наблюдения и замаскированные объекты [230].

Однако главная ценность деконцентративных психотехник не в этом. Перенос психотехнических приемов из сферы восприятия в другие области человеческой жизнедеятельности позволяет формировать состояния повышенной рефлексии и те особые состояния объемного сознания, которые позволяют одновременно видеть несколько альтернативных картин мира, подходов и т.д. Эти особые состояния одновременного видения различных альтернатив и скрытых возможностей, состояния объемного сознания, позволяют как преодолевать манипулятивные воздействия, так и строить адекватные траектории поведения и принятия решений, лишь минимально подверженные неявным воздействиям. Понятно, что на основе этой психотехнической линии формируется и новая психическая структура, отличная от той, которая преобладает у людей современных обществ. Если не впадать в очередной утопический миф, можно сказать, что преобразования сознания человека на основе использования в образовании и воспитании новых психотехнологий позволит создать культуру с мощным контрманипулятивным компонентом.

Использование современных психотехнологий для разработки контрманипулятивных технологий, отвечающих на вызовы сегодняшнего дня, пока кажется слишком радикальным и экзотичным. Однако не забудем, что средства поражения регулярно опережают средства защиты и эта закономерность не утратила своего значения при переходе от классических боевых действий к эпохе информационно-психологических войн. Завтра психотехники, кажущиеся экзотическими и излишними могут занять свое место в системе контрманипулятивной обороны, необходимой любому народу и государству для выживания в жестких реалиях начинающегося столетия.

Мнение второе. Разработанные в СССР методы манипуляции общественным сознанием считались, в свое время, одними из лучших в мире. Элементы идеологической борьбы и коммунистической пропаганды эффективно использовались и были опробованы не только в СССР, но и во многих странах мира. Подробно были разработаны элементы психологической войны. Большое внимание уделялось различным видам агитации и пропаганды: внешнеполитической, манипулятивной, "белой" и "черной", подрывной, контрпропаганде и др. В современной рекламе, пропаганде и технологиях PR с каждым годом разрабатывается все больше новых эффективных манипулятивных методов. Новые методы и техники все чаще используются различными финансовыми группами как для выборов, так и для сбыта своей продукции. Значительные финансовые ресурсы тратятся на исследования в области как электорального, так и потребительского поведения и разработке таких

техник и приемов. Одними из базовых отраслей, исследующих и применяющих манипулятивные приемы как в бизнесе, так и в политике являются *реклама* и *паблик рилейшнз*.

Термин Public Relations (PR) дословно переводится с английского, как "связи с общественностью". Это прежде всего методика формирования доверия, а также это деятельность, направленная на изменение убеждений, мнений и поведения разных групп людей по отношению к организации, ее продуктам, услугам, конкретным идеям. Также PR направлен на увеличение конкурентных преимуществ одной идеи в ущерб конкурирующим.

В последнее время часто употребляется термин "Черный PR" или "грязные технологии". Чаще, применительно к грубым манипулятивным действиям в политике и ассоциируется с запрещенными приемами. На методах черного PR, в контексте манипулятивных воздействий мы остановимся ниже. Но сначала речь пойдет о механизмах манипуляций.

Механизмы. Изучение и знание механизмов манипулятивных воздействий предоставляет "ключи" от многих дверей к воздействию и влиянию на большие массы людей. А в конкретной ситуации, учитывая ряд необходимых условий, можно добиться больших результатов воздействия. В данных случаях эксплуатируются инстинкты, стереотипы, архетипы, биоритмы человека и общественных процессов, механизмы восприятия информации.

"Один из главных рычагов Манипулятивной пропаганды – тенденциозный подбор информационных сюжетов с целью выпятить версии и "факты", которые воздействуют в первую очередь на такие элементы психики, как инстинкты и эмоции. ...В основе манипулятивных концепций пропаганды лежат принципы бихевиоризма. Широко используется заимствованный из практики буржуазной коммерческой рекламы метод подсознательного стимулирования, когда отношение массовой аудитории к тем или иным явлениям окружающей действительности формируется с помощью стандартизированных, упрощенных представлений (стереотипов и имиджей)" [231]. Это воздействие базируется также на групповых эффектах поведения. К числу таких эффектов относятся, как минимум, следующие: эффекты Рингельмана, Латейна, Выготского, законы Йеркса, Морено [232] и т.д.

Если говорить о мотивации электорального поведения, то она основана, по моему мнению, на четырех базовых разделах потребностей и рефлексов:

1. Потребность в вожде (отце) – потребность в реализации (социального) рефлекса субдоминирования (подчинения) и рефлекса следования за вождем.
2. Потребность в аффилизации – потребность реализовывать групповые (стадные) рефлексы (рефлекс групповой идентификации, коммуникативный рефлекс, рефлексы следования за группой, подражания, альтруизма). Сюда входит потребность быть членом группы, взаимодействовать с окружающими, оказывать помощь членам группы и принимать ее от них и т.д.

3. Рефлексах, основанных на стандартах поведения, традициях, привычках и штампах.
4. Иррациональном поведении, включающем в себя подражание, заражение и другие модели поведения.

Классификация манипулятивных методов в избирательных кампаниях ("Черный PR" или грязные технологии). Целью использования данных манипулятивных методов является положительный результат выборов. Законность применения данных методов регламентируется законодательством. Законы Украины: "Про вибори президента України", "Про вибори народних депутатів України", "Про вибори депутатів місцевих рад, селищних, міських голів", "Про центральну виборчу комісію", "Про інформацію", "Про телебачення і радіомовлення" и другие. Но часто во время избирательной кампании используются любые методы и рычаги влияния на ситуацию. Основными ресурсами кандидатов являются административный, информационный и организационный [233].

Данная классификация включает в себя четыре раздела: админресурс, манипуляции с оппонентом, агитацию и контрпропаганду, а также манипулятивные методы, влияющие на психические структуры избирателей (психоманипуляции). Следует отметить, что в каждом из всех приведенных ниже примеров используется несколько манипулятивных приемов.

Использование админресурса предполагает:

1. Использование ресурсов государственной власти во время выборов - работа с руководителями госучереждений (исполкомов, больниц, школ, ЖЭКов, транспортных предприятий – угроза увольнения). Использование аргументов налоговой администрации.

2. Манипуляции с регистрацией кандидатов, партий, блоков.

а) неправомерная регистрация в качестве избирателей (работа с базами данных)

б) манипуляции с процессом регистрации в качестве кандидатов.

в) манипуляции с избирательным законодательством. Лоббирование и принятие законов изменяющих "правила игры" на уровне Верховной Рады.

3. Нарушения правил финансирования выборов. "Помощь" дружественных организаций. Финансовые махинации.

4. Использование цензуры. Относится к стратегии запретов. Различные виды цензуры продолжают свое существование еще со времен Советского Союза.

5. Технологии фальсификации результатов выборов:

а) использование чужого права голоса на выборах;

б) подделка результатов выборов и неправильный подсчет голосов;

в) использование фальшивых бюллетеней для голосования;

г) порча бюллетеней для изменения результатов выборов

Манипуляции с оппонентом предполагают следующие действия:

1. Давление на кандидатов - угрозы кандидату и членам его семьи, организация "травли".

2. Срыв предвыборной деятельности кандидата – противника:

а) создание помех для производства и распространения агитационных материалов, включая умышленное уничтожение печатной продукции;

б) создание помех для публичных выступлений;

в) создание помех работе избирательной команды;

г) подкуп или экономическое давление на кандидата и его структуры.

3. Регистрация одноименных блоков, кандидатов-тёзок (двойников), и их раскрутка.

Можно упомянуть о выборах в Верховную Раду в 221 округе города Киева. Один из примеров метода двойников. Основным претендентом на победу был г-н Оробец, и большая часть населения хотела за него проголосовать, а в бюллетенях для голосования кандидатов с фамилией Оробец оказалось трое... Да еще один Горобец... Представьте рядового избирателя, который хочет проголосовать за г-на Оробца...

4. Дескридитация кандидата в неконтролируемой и агрессивной среде. На публичных выступлениях, пресс-конференциях, прямом эфире. Подготовка агрессивных, опасных вопросов и использование их при большом количестве журналистов, политиков, избирателей.

5. Разворачивание скандалов, сенсаций. Применение заказных компроматов. Показательными примерами служит история с компроментирующей видеозаписью на Генерального прокурора России Скуратова. Наш "кассетный скандал", также является ярчайшим примером, кстати, скандала международного уровня.

Агитация и контрпропаганда в контексте манипулятивных методов:

1. Агитация с нарушением закона;

а) агитация в запрещенный законом период;

б) агитация, возбуждающая расовую или национальную ненависть, содержащая призывы к захвату власти насильственным путем, связанная с разглашением государственной тайны, и т.д.;

в) выпуск агитационных материалов лицами и организациями, не имеющими на это права, а также распространение анонимных печатных материалов;

г) агитация, сопровождающаяся распространением ложных сведений о кандидате (дезинформация и дезориентация).

О эффективности этого метода говорит создание еще в 1923 году по решению Политбюро ЦК РКП(б) Специального межведомственного Бюро по дезинформации. Это не говоря о подобных структурах в ГРУ МО и КГБ СССР. Пример дезинформации ("утки"): "Кириенко – член секты сайентологов". В Государственной Думе России по этому поводу целое расследование учинили. В результате не подтвердились эти данные. Но пятно на репутации осталось".

2. Девизы и слоганы контрпропаганды. Составление обидных кличек, ярлыков, анекдотов, частушек, в общем "народного фольклора". Как о примере удачной контрпропаганды можно рассказать о судьбе слогана Мороза: "Тільки Мороз здатний перемогти Кучму" – на эту тему вышел сильный по креативу слоган – контрпропаганды: "Тільки Мороз здатний перемогти літо!". С помощью шрифта и специальных символов форма этой фразы закрепляется в сознании более удачно по сравнению с предыдущим слоганом. Плюс всё это усиливается всевозможными приколами "Ще не змерзла Україна!", "Мороз надовго і всерйоз". Остается только максимально широко распространить этот "шедевр". Этот контрслоган чаще на устах у избирателей и легче транслируется в массах. Такая же участь постигла листовку "Ткаченко. Він знає, він зможе, він переможе". Контрответ: "Ткаченко зможе, якщо Віагра допоможе". И во втором туре: "Симоненко зможе, якщо Ткаченко допоможе. Віагра: традиційний спонсор лівих кандидатів"

3. Рейтинг – технологии: использование искажений. Человек всегда подсознательно ставит на победителя. Но эффективность этого метода в наше время невысока.

4. Запуск и организация слухов. Запуск слухов "в поле" и в СМИ. Программирование агрессивности слухов. Влияние на скорость распространения. Особенное значение слухи имеют на региональных выборах.

Основные направления использования слухов [234]:

- создание определенного имиджа личности, организации, фирмы, манипуляция общественным мнением;
- привлечение внимания к определенному событию, личности;
- реклама товаров, услуг;
- информационно-психологическое обеспечение какой-либо деятельности;
- противодействие какому-либо информационному сообщению (воздействию) или другому слуху, т.е. создание контрслуха;
- использование слуха как способа изучения неформальной системы коммуникации и связей в группе.

Противодействие слухам [234]:

- подавление слуха фактами, а не выделение его для прямого опровержения;
- выступление официального лица с опровержением;
- встречное распространение противоположной информации (слух);
- дискредитация "возможного автора" слуха;
- объявление о существовании некоего врага, распространяющего слух с целью нанесения определенного ущерба;
- объяснение психологических механизмов возникновения конкретного слуха.

5. Ночная контрагитация. Использование бомжей для акций "от двери к двери – ночью". Ночные звонки с предложениями голосовать за конкурен-

та. Также машины, со звукоусилительными устройствами, активно громко агитирующие с музыкой за конкурента ночью. Особая эффективность этого метода в сельской местности.

Психоманипуляции. К психоманипуляциям, по нашему мнению, относятся: запугивание избирателей, шоки, эмоциональное воздействие, информационное дозирование, прямой подкуп избирателей и конечно применение нейролингвистического программирования (НЛП), приемов блефа и полублефа. Применяют подобные методы в соответствии с этапами изменения психоэмоционального состояния населения во время избирательных кампаний и учитывают каналы восприятия информации человеком [225; 235-236].

1. Запугивание избирателей. Использование рефлексов, основанных на осознанных и подсознательных страхах.

2. Шокирующие сообщения. Прямая ложь и клевета.

3. Эмоциональное воздействие. Пробуждение положительных эмоций у избирателей по отношению к кандидату.

4. Использование информационного дозирования (Чернобыльская катастрофа, "радиоактивная" демонстрация). Также запрещенное замалчивание, способное исправить неверное впечатление о кандидате.

5. Прямой подкуп избирателей. Организация подарков и денежное вознаграждение в надежде на соответствующее голосование.

6. Применение нейролингвистического программирования (НЛП). Метод НЛП был задуман американскими психотерапевтами Джоном Гриндером и Ричардом Бэндлером в 1975 году как удачный бренд, и вошли туда множество психологических и психотерапевтических методов, известных ранее, но не имеющих специальных названий. Данный метод получился настолько грамотно, доступно и удобно составлен и классифицирован, что стал массово использоваться не только в Америке, но и в других странах. В контексте манипулятивных технологий в политике успешно применяются из НЛП:

• Способы "якорения" — установки "якорей" в сознании по типу павловских условных рефлексов Ассоциативные связки (якоря) с заведомо отрицательными, всем противными объектами, событиями. Якорение используется в выработке рефлексов больших масс людей на специально вводимые "в народ" слова: "незалежність, демократія, національна ідея, конституція, державність", это из современных, а уже "укрепленные" во времена СССР: "коммунизм, социализм, светлое будущее, империализм, враг народа, интернациональный долг" и т.д.

- Рефрейминг (изменение контекста, НЛП). Изменение шкалы ценностей.
- Изменение фокуса внимания.
- Использование механизмов блокировки опыта в языке (генерализация, опущение, искажение)
- Использование генераций нового поведения
- Разработка шаблонов восприятия и работы с ними.

- Техники изменения линии времени
- Лингвистические способы создания субъективной реальности. Использование пресуппозиций, встроенных сообщений неоднозначностей и связок.
- Построение и использование метафор
- Идея модальностей, или субмодальностей — представлений, основанных на пяти перцептивных системах (органах чувств)
- Идея метапрограммирования, формирования метапрограмм —"фильтров", через которые человек воспринимает окружающий мир
- Методы построения раппорта, подстройки, присоединения и ведения.
- Формирование различных видов "транса" — состояния сознания, которое облегчает внедрение необходимых установок. Использование в публичных выступлениях, текстах для СМИ, агитбригадами.

7. Использование приемов блефа и полублефа в пропаганде. Блеф (bluff — англ.) — это ложное информирование, причем такое, когда желаемое пытаются выдать за действительное. Блеф представляет собой дезинформацию, при которой на основе обмана убеждают кого-либо в том, что нечто желаемое, но не существующее существует. Блеф эффективен, если удается ввести в заблуждение того, на кого блеф направлен. Таким образом, блеф является искусственным заблуждением [237].

Приемы блефа и полублефа эффективно применялись с высокой эффективностью еще в советские времена. "Верхушка" общества с двойными стандартами применяла блеф практически во всех агитационных мероприятиях. Идеализировались герои войны и труда, формировались искусственные идеалы, которые в действительности были точками подражания, на которых воспитывалось молодое поколение, что является положительным моментом блефа. Примерами могут служить Чапаев, Стаханов и т.д. Блефовали часто во время отчетов по экономическим и другим показателям. Даже термин для этого существовал — очковтирательство, кстати, актуальный и поныне.

Приемы блефа и полублефа:

- Фальсификация (подтасовка)
- Дезориентация (замещение)
- Пустословие (словоблудие)
- Полуправда (иррациональная, рациональная, диалектическая)
- Приемы скрытой рекламы
- Приемы одностороннего и избирательного освещения информации
- Приемы искусственно-организованных писем и жалоб
- Догадки и предположения в форме фактов
- Приемы заказных материалов
- Приемы искусственных скандалов
- Прием навешивания ярлыков
- Прием ярких обобщений и смещений акцентов
- Прием недостоверных и заказных социологических исследований

- Представление материалов прошлого как настоящих
- Цитирование несолидных изданий и решений сомнительных собраний и т.д.

Манипулятивные приемы в бизнесе. Для контроля и захвата рынка Украины используется большое количество манипулятивных технологий. Это и лоббирование интересов больших корпораций путем постановлений Кабинета Министров, законов Верховной Рады, финансовые технологии, интенсивные информационные и ПР-кампании, использование спецприемов в рекламе, негласный запрет продажи в Украину супертехнологического оборудования, препятствие производства в области высоких технологий (история с производством компакт-дисков), организация выезда из страны специалистов ("охота за головами" - head hunting) и т.д.

В настоящее время с большой скоростью развиваются новейшие бизнес-технологии. Среди них можно отметить и мерчендайзинг (merchandising) – систему методов по оформлению торгового зала и расположению товара на полках, побуждающую покупателя совершать максимальное количество покупок в данном месте (P.O.S.-конечных точках продажи) по данной цене.

Среди ключевых инструментов мерчендайзинга можно выделить: дизайн магазина (как внешний, так и внутренний), планирование магазина (точнее, планирование потоков движения покупателей, планирование распределения внимания покупателей), рекламные материалы и инструменты на местах продажи (витрины, гондолы, вымпелы, лайтбоксы, плакаты, информационные модули и т.д.), ассортимент товаров, знаки, символы и цвета, усиливающие желание совершить покупку, ароматический логотип, звуковое воздействие и др.

Использование данных технологий (мерчиндайзинга) повышает продажи на 50-80%. Ведь 30-40% покупок считаются строго запланированными а 60-70% покупок являются импульсивными, т.е. решение об их приобретении принимается непосредственно у прилавка. Поэтому разработки в области психологии поведения потребителей являются базовыми в этой отрасли и манипулятивными по своей сути.

В настоящее время в крупных корпорациях разработано огромное количество визуальных методов специального коммуникативного воздействия на потребителей. Это визуальные спецприемы [238]: упрощение, натурализация, наив, утилитаризм, регрессия, деградация, интроекция, вторжение, прием временной добровольной сдачи личной автономии, прием ложного долга, сублимация, эпатаж, ретрофлексия, проекция, усиление потенциала, вовлечение, ориентировочный рефлекс, эмоциональный резонанс, слияние, провокация и т.д

Анализ и мониторинг манипуляций. Для качественного и адекватного анализа и мониторинга манипулятивных воздействий, после набора исследований и сбора информации, необходимо, по нашему мнению, учитывать и использовать основные составляющие анализа:

- классификацию манипулятивных воздействий и методов;

- объект манипуляции;
- манипулятор или заказчик;
- механизмы действия методов на объекты манипуляций;
- каналы коммуникации;
- адекватные методы анализа и мониторинга этих воздействий.

О классификации манипулятивных методов и механизмах воздействий (1 и 4 пункты) было изложено в предыдущем материале. Остановимся на остальных.

Объект манипуляции. Объектом манипуляции мы можем рассматривать так называемые "целевые группы", в маркетинге - это потенциальные потребители товаров и услуг, в политике – потенциальные избиратели, на международной арене – это страна, как субъект отношений и точка приложения манипуляций.

Манипулятор или заказчик. Манипулятор в большинстве случаев не заинтересован в своей известности, как манипулятора, но в итоге он почти всегда "просматривается" на арене как победитель политических или экономических событий. В случае определения манипулятора или заказчика на начальном этапе развития событий, обычно, довольно просто, определить его цели и возможности, а соответственно можно прогнозировать развитие ситуации с высокой степенью достоверности.

Каналы коммуникации. Среди каналов коммуникации можно отметить следующие: средства массовой информации (СМИ), устные встречи, деловые переговоры и переписка, рекламные материалы и наглядная агитация, специальные события (фестивали, выставки, митинги и т.д.).

Методы анализа и мониторинга. Мониторинг СМИ желательно проводить с учетом параметров: вида (пресса, ТВ, радио, Интернет), степени влияния, тиража, зоны вещания, интенсивности, тональности, креативности, повторяемости сообщения, известности, степени цитируемости в других СМИ, а также интересов владельцев СМИ, степени цензуры. Большое значение имеет количество и влиятельность средств массовой информации стран-заказчиков манипулятивных воздействий в нашей стране.

Для мониторинга психоманипуляций, конечно, нужно знать методы воздействия, иметь инвентаризационный перечень приемов и с помощью системного анализа отслеживать их. Для определения приемов блефа необходимо обеспечение оперативной, качественной информацией и желательно фактического материала для мониторинга или возможного опровержения.

Среди методов анализа на первом этапе стоит контент-анализ. Количественный подход на начальном этапе необходим для отслеживания предпочтений, тональности, тенденций, силы воздействия манипуляции.

Системный и структурный анализ позволяет проследить весь процесс манипуляции от проекта до результатов, т.е. "развертку" во времени, а также увидеть процесс изнутри с актуализацией наполнения, а также сделать выводы, определить стиль и методы работы манипулятора, степень угроз.

Психологический анализ необходим для оценки влияния на психические структуры людей данных приемов с точки зрения исследования поведения как отдельных индивидуумов, так и различных социальных групп (законы и методы воздействия в данных ситуациях значительно отличаются). В некоторых случаях действия разворачиваются по законам психологической войны, и тогда данный вид анализа дает максимально адекватную картину и приобретает особое значение. Также здесь можно отследить тончайшие механизмы манипуляций.

Прогностический анализ делает возможным прогнозировать тенденции, предусматривать действия, что очень важно во время организации противодействия манипуляциям.

И регрессивный анализ позволяет актуализировать все примененные методы за определенный период времени и проанализировать свои ответы, их адекватность и эффективность [239-243].

В последнее время на базе нашего Центра разработано несколько методик экспертной оценки рекламной продукции на наличие манипулятивных технологий, и так называемого "активного программирования". Это психомониторинг визуальной печатной продукции, рекламных видеороликов, экспертная оценка мерчендайзинга. Комплексная экспертная оценка рекламной или PR-кампании.

Антиманипулятивные технологии и информационно-психологическая безопасность. Согласно Конституции Украины [244] "Человек, его жизнь и здоровье, честь и достоинство, неприкосновенность и безопасность признаются в Украине наивысшей социальной ценностью" (ст.3), "никто не может подвергаться вмешательству в его личную и семейную жизнь" (ст.32), "каждому гарантируется право на свободу мысли и слова, на свободное выражение своих взглядов и убеждений" (ст.34), "каждому гарантируется право свободного доступа к информации про состояние окружающей среды, про качество пищевых продуктов и предметов быта, а также право на ее распространение" (ст.50).

Широкое использование манипулятивных технологий, информационных воздействий в рекламе и PR-кампаниях представляет собой реальную угрозу в контексте внутренней информационно-психологической безопасности жителей Украины. Разработка антиманипулятивных технологий является важной задачей для обеспечения конституционных прав и свобод жителей Украины и обеспечения их информационно-психологической безопасности.

Также, согласно Конституции нашей страны "защита суверенитета, территориальной целостности Украины, обеспечение ее экономической и информационной безопасности является важнейшими функциями державы, делом всего Украинского народа" (ст.17), "внешнеполитическая деятельность Украины направлена на обеспечение ее национальных интересов и безопасности путем поддержки мирного и взаимовыгодного сотрудничества с члена-

ми международного сообщества по общепринятым принципам и нормами международного права" (ст.18).

Использование технологий манипуляции на международном уровне представляет опасность в контексте международной безопасности Украины. И антиманипулятивные технологии в этой области приобретают стратегическое значение.

По оценке уровня угроз информационной безопасности Украины, сделанной Центром экономических и политических исследований им. А.Разумкова [245] из одиннадцати предложенных угроз на первое место эксперты поставили "разрушение моральных ценностей, духовного и физического здоровья человека, общества вследствие внешнего информационного воздействия негативного характера (распространение порнографии, насилия, ужасов и т.д.). На втором: "создание негативного имиджа Украины на международной арене вследствие неэффективной информационной политики", затем "негативное воздействие на развитие политической системы Украины (в т.ч. воздействие на результаты выборов) вследствие внутренних и внешних информационных кампаний", "деформирование общественного сознания вследствие негативного информационного воздействия", "разрушение национального информационного пространства вследствие информационной экспансии других стран" и др.

В настоящее время одним из наиболее важных вопросов является сохранение и развитие положительного имиджа Украины, как настоящего и потенциального объекта манипуляций. Имидж нашей державы, конечно, базируется на Концепции национальной безопасности Украины [246] и Концепции национальных интересов Украины [247] . Также важно определить составляющие имиджа Украины для адекватного анализа и возможности разработок антиманипулятивных воздействий и моделей манипуляций. Существует несколько подходов к оценке государства, это показатели, которые можно показать односложно, например, уровни продолжительности жизни, безработицы, бедности, экономические показатели: ликвидность ценных бумаг, платежный баланс, стабильность национальной валюты, инвестиционный климат и сложные показатели – уровни коррупции, прав человека, свободы слова и т.д. Данные рейтинги применяются для аргументации и достижения, совершенно прагматических, к тому же тактических целей. Но важен целостный подход, для стратегических разработок. В таком контексте можно отметить внешние и внутренние составляющие имиджа нашей страны.

Внешние составляющие имиджа Украины:

- *Политические.* Внешняя политика Украины. Уровни политических и экономических договоренностей. Ассоциированное членство в престижных международных организациях на равных правах. Влиятельность страны в мировом сообществе. Степень уважения к представителям нашей страны в различных странах. Уровень компетенции украин-

ских политиков. Смена кадров в правительственных структурах. Непредсказуемость развития политической ситуации. Визовые режимы и транспортные коридоры. Впечатление после пересечения государственной границы Украины. Отношение на таможне.

- *Информационные.* Внешняя и внутренняя информационная политика. Качество и количество, влиятельность и оперативность информационных передач о событиях в Украине, на украинском и особенно на иностранных языках. Степень информационной экспансии и контроля. Уровень усиленной трансляции положительного имиджа страны в СМИ.
- Оперативная реакция на информационные нападения извне. Адекватное ответное освещение данных событий на языках "источников" нападения. Степень отработки стратегии и тактики противодействия негативным информационным воздействиям. Лимиты и квоты иностранных СМИ в информационном пространстве Украины. Свобода слова, степень цензуры.
- *Финансово-экономические.* Международная экономическая политика. Долги. Платежеспособность страны. Уровень отстаивания национальных экономических интересов. Структура отношений с международными финансовыми организациями. Наукоемкость промышленности. Уровень рыночных реформ. Качество и количество товаров, предоставляемых на экспорт. Ассоциативное членство в экономических союзах, ассоциациях и т.д. Влиятельность и значимость. Финансовая помощь другим странам. Зависимость от энергоресурсов. Состояние нефтяных коридоров. Теневая экономика. Международный кредитный рейтинг. Уровень защиты иностранных инвестиций. Экономическая преступность.
- *Военные.* Военный потенциал. Современная система ПРО. Боеспособность, мобильность и оснащенность армии. Возможность создания ядерного и других видов оружия массового поражения. Спутники-разведчики. Авиационно-космический потенциал. Вес на рынках вооружений.
- *Культурные.* Стимуляция разработок в области национальной культуры. Достойное место в рейтингах кино, музыкальных и других достижений на международных фестивалях, конкурсах. Степень транслирования украинских фильмов, видео, аудиопродукции, выступлений художественных коллективов в мире. Книгопечатание украинских авторов на различных языках. Развитие отношений с украинской диаспорой.
- *Научные.* Конкурентоспособность научных исследований и разработок. Разработки в области высоких технологий, самолето- и ракетостроения. Разработки в области ВПК и ИТ. Антарктические исследования. Поддержка и внедрение отечественных разработок. Защита прав интеллектуальной собственности.
- *Психологические.* Национальная пропаганда. Формирование у жителей Украины патриотизма, закрепление культурных традиций путем

воспитательных, образовательных и культурных программ. Трансляция культурных ценностей.

- *Спортивные.* Победы на спортивных соревнованиях, фестивалях, олимпиадах. Отношение к победителям. Отношение государства к рейтинговым в мире видам спорта. Обеспечение развития туризма и туристического бизнеса.
- *Другие.* Экологическая политика государства, степень загрязнения окружающей среды. Решение проблем чернобыльской катастрофы. Уровень коррупции. Защита прав потребителей. Уровни благосостояния, минимальной заработной платы. Демографические показатели. Уровень здоровья населения. Политика государства по другим насущным проблемам, находящимся в фокусе внимания мирового сообщества.

В настоящее время международный имидж Украины является неудовлетворительным. Большинство иностранных экспертов определяют Украину как "малозначительную европейскую страну, которая находится в поисках своего места в мире" [248], с "низким уровнем экономического развития и недостаточными темпами экономических реформ, низким жизненным уровнем значительной части населения и высоким уровнем коррумпированности власти" [248].

Имиджевый потенциал Украины довольно высокий и полностью не используется. Как и научный, экономический, культурный и т.д. Но создание позитивного имиджа Украины должно стать предметом особого внимания правительства, СМИ, политических партий, общественных организаций страны, миллионов граждан.

2.5. Маніпулювання як феномен масової комунікації

Перефразовуючи вислів відомого мислителя, аналіз феномену маніпуляції розпочинається із того найближчого для людини, що залишається найвіддаленішим. Маніпулювання, поза сумнівом — повсякденне явище, оскільки не існує індивіда групи людей чи корпорацій ЗМК, які б ніколи не вдавалися до маніпулювання. З іншого боку, не кожен знає про те, де починається і де закінчується маніпулятивний вплив, а тому частіше стає мовчазною жертвою чи в найкращому випадку спостерігачем в ситуації порушення психологічної безпеки, ініціатор якого залишається за фокусом спостереження.

Віртуальна реальність ЗМК відповідає на сьогодні людині нового типу, яка споживає інформацію і деградує в духовно-інтелектуальному відношенні. Вимоги щодо розвитку аналітичних здібностей стосуються передусім швидкості обробки та сприйняття, а не глибини мислення, тим паче - не творення мисленнєвих форм, які могли б конкурувати із спеціально розробленими лабораторно-студійними персонажами ЗМІ.

Першим кроком дослідження проблеми традиційно є термінологічні конвенції, із яких ми і розпочнемо. Здавалося б, маніпулювання далеко не terra incognita в наукових розробках з психолінгвістики, риторики та психології масових комунікацій. Маніпулятивна мегамашина, заведена на повну потужність в рекламі, маркетинзі, пропаганді, різноманітних виборчих технологіях іноді навіть здається узвичаєною складовою взаємодії в соціумі, оскільки якби люди витрачали час на неманіпулятивне переконання своїх партнерів по комунікації, то предметні результати у вигляді зростання збуту товарів, поширення певної ідеології чи визначеної кількості голосів на виборах були б недосяжними. Таким чином, першою передумовою маніпулювання є дефіцит часу, зумовлений складністю пошуку системи кодування/декодування інформації як для маніпулятора, так і для того, ким маніпулюють. Звичайно, обидві сторони уявляють собі, скільки зусиль їм довелося б витратити на те, щоб дійти до рівня особистого смислоутворення, на якому тільки і стає можливою глибинна неманіпулятивна взаємодія. Означене стосується не лише індивідів, але і соціальних груп, малих і великих. Маніпулятор свідомо або безсвідомо дегуманізує того, ким він маніпулює, а тому не вважає за можливе і необхідне рахуватись із психологічною автономією *"жертви"*. З іншого боку, *"жертва"* також прагне до маніпуляції, оскільки відшуковує полегшений в плані інформаційної складності варіант розв'язання проблеми, а отже, створює зону тяжіння для вторгнення в свій психологічний простір, дегуманізуючи тим самим себе.

Друга передумова маніпулювання – руйнування системи психологічного імунітету, інформаційної фільтрації, представлену установками, переконаннями, цінностями. Маніпулятор має здійснити "підрив" системи фільтрації інформаційних сигналів (радикальний варіант маніпулятивного впливу) або ж обійти її, штучно присиливши бар'єр усвідомлюваного (м'який варіант маніпуляції). Об'єктом маніпулювання виступають всі психічні функції, як раціональні, так і ірраціональні. Але якщо маніпулювання одними функціями (наприклад, емоціями) може мати тимчасовий або ситуативний характер, то маніпулювання переконаннями, цінностями чи установками зорієнтоване на перебудову чи переорієнтацію поведінкової активності чи навіть стратегії життєдіяльності. *"Жертва"* також може здійснити саморуйнування, піддавшись такому стану, який спричиняє незахищеність метапрограми психіки від "вірусного" щеплення маніпулятора.

Щоразу величина зони вторгнення визначається величиною фокусу охоплення, тобто, того простору потенційної інформації, яка проникає в свідомість та безсвідоме. Жорсткі фільтри, сформовані соціалізацією, блокують будь-який інформаційний вплив; занадто широкий фокус охоплення, навпаки, створює контактну зону практично в будь-якій комунікації. Відповідно, меншою інформаційною імунозахищеністю щодо маніпуляції будуть володіти представники двох психологічних полюсів: із занадто вузьким фокусом охоплення, закритим для альтернативної інформації (мішень впливу

– безсвідоме), або ж із занадто широким еластичним фокусом охоплення, орієнтованим на будь-яку інформацію (мішень впливу – свідомість).

Перша група – особи із топосно-прив'язаним психічним світом, вихо-вані в традиційному середовищі із слабкою варіативністю когнітивних, емоційно-ціннісних та регулятивних диспозицій. Свідомість тут працюватиме в режимі циклічного реварію вання первинно засвоєних кодів, а тому її відкритість щодо зовнішньої інформації забезпечується шляхом асиміляції от-риманого в семіотику отримувача. *"Башта із слонової кістки"* топосної психіки гарантує їй повну безпеку доти, доки не виникає потреба в соціальній мобільності, що означає тимчасовий вихід із циклічного режиму, тобто, ар-хаїзацію свідомості. Неможливість реверсії свідомості, її переорієнтація на інтерпретативні коди мобілізує безсвідоме, яке починає руйнування фокусу охоплення, заміщуючи його некерованим потоком психічної енергії. Маніпу-лятор тим самим отримує можливість для належного спрямування цього по-току – свою мішень впливу. Остання обставина виведена з під контролю жертви, оскільки підлаштована під звичний режим регулювання.

"...спостереження психологів, – пише Л.Д. Столяренко, – показали, що в зону ясного усвідомлення в даний момент попадають ті об'єкти, які ство-рюють перепони для продовження звичного режиму регулювання. Утруднен-ня, що виникли, привертають увагу і таким чином усвідомлюються. Усвідо-млення обставин, що ускладнюють регуляцію або розв'язання задачі, сприяє знаходженню нового режиму регулювання або нового способу рішення, але як тільки вони знайдені, управління знову передається в безсвідоме, а свідомість звільняється від розв'язання нововиниклих утруднень" [249].

Друга ситуація має місце із протилежним полюсом. Широкий фокус охоплення означає, що безліч інформаційних джерел бомбардують свідомість, яка намагається інтерпретувати практично всі сигнали, що надходять зовні. І якщо інформація має мозаїчний, а не лінійно-системний характер, і подається у прискорених темпах (а за сучасних умов це абсолютно нормально), відбу-вається перехід свідомості у змінений стан. Останнє також розкриває шлюзи психіки для маніпулятора.

Дві вищезазначені передумови не вичерпують собою перелік факторів маніпулятивної віктимології.

Третя передумова пов'язана із поточним психічним станом. Відомо, що афективно-стресові стани також є сприятливими для різноманітних маніпу-ляцій, оскільки відкрите безсвідоме піддається завантаженню сторонньою інформацією без відома реципієнта. Афект чи стрес означають тимчасове відключення системи фільтрації через виникнення дезадаптивного чинника, щодо якого не опрацьовано алгоритмів реагування. Маніпулятор в принципі і розраховує на те, що такий тимчасовий злам не помічається самою жертвою і робить її беззахисною. Найкращою точкою поразки стає довготривала пам'ять, де встановлюються усталені асоціації між стресором та стресом, і то-му що разове *"натискання"* на аналогічний або подібний стресор запускати-

ме асоціативний ланцюг, кінцевим пунктом якого буде повторюваний контекст стресу, необхідний для маніпулятора.

Перехідні суспільства, перебуваючи в стані своєрідного стресу перед невідомістю майбутнього, також піддаються маніпуляції при відключенні фільтрів соцієтальної психіки, оскільки навіюваність при частковій дезорієнтації та переоцінці цінностей (ситуативній аномії) прирівнюється до чутливості з боку авторитетних сугесторів в сфері міжкультурних комунікацій.

Те ж стосується і неоптимальних емоцій — страху, гніву, надмірної екзальтації тощо.

Четверта передумова корелює із віком. Діти і люди похилого віку заносяться до розряду маніпулятивно-незахищених через позицію онтогенетичної залежності від сугесторів, коло яких є необмеженим у дитинстві або ж надзвичайно обмеженим у похилому віці. Неважко припустити, що і перше, і друге уможливлює тотальний маніпулятивний контроль над свідомістю та поведінкою цих вікових категорій. У одних, оскільки механізми когнітивного опору сугестії ще не сформовані, у інших — через монополію вузького кола сугесторів на доступ до вже стабілізованих світоглядних метапрограм, безальтернативність процесів інформаційної переробки, зумовлену скороченням часової перспективи життя.

Вік існування системи, яка прагне захистити себе від маніпулювання, знаходиться в діапазоні зрілості, коли селекція інформації є достатньо високою для того, щоб уникнути навіювання, і достатньо гнучкою, щоб уникнути ізоляції, а отже, і орієнтації в інформаційному просторі.

П'ята передумова випливає з рівня самооцінки, яка, за формулою Джемса, є прямо пропорційною успіху і зворотно пропорційною домаганням суб'єкта. Отже, занижена самооцінка є похідною від високих домагань та невеликого успіху, а менеджмент цими двома величинами прирівнюється до маніпулювання. Наприклад, маніпулятор, граючи на честолюбстві, визначенні стандартів належного, прирівнюючи себе до ролі арбітра чи експерта в питаннях цінного і значущого контролює самооцінку жертви через механізм провини за невідповідність між рівнем очікувань та домагань (перед собою або ж референтною соціальною групою). За умови контролю над ресурсами оцінки успіху (соціальні норми, образи індустрії мас-мистецтва, громадська думка, різноманітні рейтинги) маніпулятор домагається переорієнтації активності суб'єкта до аттрактивно-позиціонованих "*вершин*", знецінюючи власні версії побудови когнітивно-регулятивних образів. Останнє стосується не лише індивідів, соціальних спільнот в макросоціумі, але і перехідних суспільств, оскільки сама ситуація перехідності із висуненням вимог щодо майбутнього також підриває баланс спільноти між успіхом та самооцінкою і робить неможливим на певний час формування власної орієнтаційної складової соціальної програми.

Шостою передумовою є недоступність оперативної та стратегічної інформації в макротекстових потоках. Під останніми розуміються будь-які інформаційні потоки, орієнтація в яких ускладнена з різних обставин (недо-

ступність джерела інформації або ж надлишкова кількість джерел, неволодіння семіотикою макротексту, розрізненість (мозаїчність) макротексту, недоступність фактів тощо.

Недоступність оперативної інформації (поточних даних) припускає нав'язування позиції, відмову від комунікації через необізнаність реципієнта та інші маніпулятивні прийоми. Але недоступність стратегічної інформації в прямому розумінні прирівнюється до інформаційного рабства. Так, в СРСР бюрократичний апарат продукував безліч підзаконних актів, про існування і зміст яких нікому не було відомо, що завжди давало переваги місцевому чиновнику перед вимогами центру, а отже, зумовлювало правову беззахисність громадян, яким могли завжди нагадати про невиконання невідомих їм обов'язків або ж приховати від них їм же належні і не згадані в процесі візиту до бюрократичної установи права.

Маніпулятор, який бере на себе роль генератора стратегічних програм, займає найвигіднішу позицію в комунікативному просторі, і шанси на привласнення такої ролі зростають там, де сегментація інформаційного поля-простору найвища. Цього можна досягти, наприклад, через спеціалізацію системи освіти, надлишкову пропозицію інформаційних продуктів, вибіркова розстановка позитивних акцентів в ЗМІ (перетворення буденних подій на "сенсації").

І нарешті, сьомою передумовою для маніпулювання є стиль мислення, сформований професійною групою.

Отже, перш ніж перейти до розгляду конкретних маніпулятивних технологій, задовольнимося робочою дефініцією маніпулювання як асиметричного, контрольованого свідомістю комунікативного впливу суб'єкта ***А*** на когнітивну, мотиваційно-енергетичну та регулятивну підсистеми індивідуальної, мікросоціальної чи соцієтальної психіки об'єкта психологічного впливу ***Б*** таким чином, щоб ***Б*** модифікував власну активність в напрямку, бажаному для ***А***, керуючись модифікованою субпрограмою-вірусом, створеною ***А***, як своєю власною.

У зв'язку з вищеозначеним треба відрізняти маніпулювання від імперативних технологій впливу, які зовні впливають на спрямованість активності, але не модифікують її непомітно для об'єкта впливу. Маніпулятор, на відміну від агента імперативних сигналів бажає, щоб в момент реалізації його субпрограми об'єкт впливу тішився ілюзією свободи волі та свідомого вибору. При розгляді конкретних маніпулятивних технологій стане зрозуміло, що маніпуляція в ЗМК має не лише внутрішньосоціальний, але і крос-культурний вимір, дозволяючи здійснювати модифікацію активності цілих суспільств так, щоб вони ініціювали реформи начебто з внутрішніх причин, хоча останні генеруються поза суспільством, в лабораторії психологічних війн маніпулятора.

Типологізація маніпулятивних технологій, запропонована у даному дослідженні, переслідує скоріше мету створення більш розгалужених класифікацій із множиною критеріїв поділу, які, здебільшого, вводяться в кон-

текст аналізу задля формально-логічної коректності. Автор пропонує поділити маніпулятивні технології на ті, що розраховані на свідомість та ті, що розраховані на безсвідоме. Маніпулятивні прийоми, що застосовуються в цих технологіях, даються без поділу, оскільки їх застосування охоплює як першу, так і другу групу технологій.

З числа маніпулятивних технологій, віднесених до впливу на свідомість, розглянемо індоктринацію, спін-доктор та перформанс.

Для розуміння того, в чому полягає природа індоктринальних технологій формування громадської думки, спробуємо розібратися з тим, що являє собою індоктринація.

У самому понятті можна виокремити декілька суттєвих рис, повʼязаних із особливостями взаємодії суб'єкта маніпуляції та акцептора маніпулятивного впливу:

По-перше, індоктринація передбачає експансивну взаємодію (*комунікативну експансію*). Комунікативною експансією ми будемо називати насильницьку (*без згоди на комунікацію з боку об'єкта впливу*) стратегію захоплення смислового простору комунікації для навʼязування іншому учаснику своєї комунікативної стратегії та свого бачення реальності.

Індоктринація має місце також і тоді, коли один з учасників комунікації має стратегію, а інший її не має. В результаті відбувається природне навʼязування цієї стратегії. Чисто логічно можна виділити два кроки індоктринальної комунікативної стратегії:

- захоплення смислового простору;
- утримання комунікації в межах захоплення смислового простору.

Погоджуючись із вищенаведеною думкою, можна специфікувати її стосовно інформаційного простору: маніпуляція з боку агента ЗМК буде мати місце тоді, коли він намагається узурпувати роль смислового центру комунікації і орієнтаційного впливу. Комунікатор, репрезентуючи себе як "розум громадськості", захоплює символічне право на "*промивання мозку*" (brain washing) начебто інфантильним акцепторам впливу.

Обєкту промивання мозку буває важко протестувати індоктринальному впливу що-небудь, оскільки він без стратегії-субпрограми практично не існує. Такий статус певної частини безголосої громадськості зумовлений відсутністю ресурсів впливу в соціальному, економічному та культурно-інформаційному полі-просторі. В принципі, для т.з. нижчих верств є типовим поєднання настанов авторитаризму і патерналізму, з чого випливає їх підлегло-екзекутивна роль у комунікативному просторі суспільства; знедолена "попелюшка" шукає чарівного "принца ідеолога", який одним жестом створить для неї привабливу комунікативну партитуру. Але "принц" не планує зробити "попелюшку" королевою, і тому весь час садить "попелюшку" на голку індоктринації.

По-друге, індоктринація спирається на герметичну ідеологію жорсткої моністично-догматичної спрямованості — різновид деякого закритого знання

для посвячених, щодо якого об'єкт впливу начебто має погодитись із статусом абсолютного реципієнта.

Теоретично можна уявити собі, що в науковій або публіцистичній неманіпулятивній комунікації також можлива індоктринація, але тут вона буде не вписуватися в контекст самої ідеології. Соціальний склад потенційних прихильників такої ідеології передбачатиме статус реципієнта: чим менше його залучатимуть до дискусії, тим краще. Лідери ЗМК не віддають переваги діалогічно-дискусійним формам роботи із масовою свідомістю, оскільки їх аудиторія відзначається безмежною нетерпимістю щодо "пустої балаканини" поза розвагами та сенсаційною шоковою інформацією.

По третє, індоктринація передбачає символічний монополізм партії, яка робить можливим вираження думки громадськості як такої. Тут мається на увазі постійне використання типізуючої символіки, що дозволяє певним соціальним колам ідентифікувати себе з комунікатором. Як відзначають московські політологи О.І.Демідов та А.О. Федосєєв, "... ставлення до явищ, що потрапляють у сферу уваги громадської думки, є далеко не однозначним, інтереси та цінності його носіїв виступають в якості своєрідних детонаторів, що викликають інтерес до тем або тих чи інших проблем, подій. Цей "оптичний ефект" дозволяє сфокусувати громадську думку на жорстко визначеній проблемі, рішення якої має важливість саме в даний момент, в силу чого приводяться в дію пласти соціальної енергії, в повній мірі виявляються перетворюючі можливості людської свідомості"[250].

Зрозуміло, що індоктринація стає можливою лише завдяки зустрічі символів та інтересів-детонаторів, яка зумовлює певне "*відключення*" аудиторії від інших проблем, фактів та подій.

По-четверте, індоктринація передбачає застосування закритих вербальних кодів — своєрідної "мови впізнання", яка гарантує політико-ідеологічну діагностику "своїх" і "чужих".

Будь-який агент ЗМІК, незважаючи на його включеність у боротьбу за лідерство в інформаційному просторі суспільства, працює із певним шаром міфолексем, які не піддаються активному аналізу і приймаються як норма. Вся перевага їх полягає в тому, що вони не є поняттями, які щоразу потребують визначення.

Визначеність сама по собі руйнує індоктринацію як таку, оскільки вириває реципієнта із міфологічного кола узвичаєності. Поки індоктринація здійснюється, міф перебуває поза критикою, забезпечуючи згуртованість і солідарність публіки навколо ідей і символічне відокремлення ворогів, що перебувають поза ідеєю. Однак все в принципі залежить ще і від того, в якому суспільстві діє комунікатор. Іншими словами, є суспільства, громадськість яких може з легкістю "проковтнути" пілюлю індоктринації і навіть подякувати режисерам міфологічних сценаріїв за збереження згоди. Американське суспільство, наприклад, накладає табу на обговорення тем, повязаних із критикою політичних інституцій — конгресу, суду, конституції, оскільки всі вони

виступають сакральними формоелементами, на яких і тримається міф про американську демократію.

Ще однією маніпулятивною технологією серед віднесених до групи впливу на свідомість є спін-доктор. Слово "*спін*" в буквальному перекладі означає *обертання*, тобто, комунікативно-маніпулятивну технологію, спрямовану на управління домінуючою тематикою масової свідомості, своєрідний менеджмент порядком денним соціальних комунікацій. Поняття спін-доктору є похідним від введеного американським журналістом та соціологом У. Ліппманом поняття "***порядку денного***" ЗМІК (agenda setting-англ.). Сам автор мав на увазі менеджмент актуальних тем та проблем, що можуть вноситись в інформаційний простір. Адже політична влада іноді випливає не лише із ресурсів розв'язання проблем, але і з позиціонування певних явищ як проблемних, вартих уваги і значущих. Той, хто формує перелік тем доби, отримує і символічну владу над аудиторіями різних соціальних груп, каналізуючи певним чином пізнавальну активність.

Напрямками маніпулятивного впливу спін-доктора є:

1. Створення актуальних тем-сенсацій і підготовка громадських очікувань до сприйняття певної інформації. Спін-доктор має «розкрутити» тему задля налаштовування публіки на визначене ставлення до політика, громадського діяча, події чи рішення. Для цього застосовується варіативно-контекстне прискорення дискусій, презентацій, конференцій та особистих інтерв'ю, завдяки чому діяч, подія чи рішення потрапляють в сегмент «оперативної пам'яті» масової свідомості, чим робиться реклама з «вуст у вуста», складається відповідний сценарій розвитку подій, що видається пізніше за передісторію нововиявленої зірки із знаком "+" чи "–".
2. Елімінація та деактуалізація тем в інформаційному просторі. Стосується скандальних ситуацій, де існує потреба в скорішій трансформації громадського дискурсу на новий інформаційний потік. Елімінація може здійснюватись шляхом елементарного замовчування або ж через розчинення теми в калейдоскопі інших тем, перетворення сенсації на периферійний епізод, про який згадують як про жарт чи непорозуміння. Для зміщення громадської уваги спін-доктори вдаються також до заміщення однієї шокової теми іншою, що дає можливість тимчасово каналізувати агресію на інший, більш значущий об'єкт.
3. Перетворення політексту в макротекст, і навпаки, макротексту в політекст. Перший варіант застосовується за умови недопущення агентів ЗМК до джерел емпіричної інформації, їх штучної ізоляції від місця сенсаційної події або ж конкретної особи. Це робить можливим зробити монопольно отриману інформацію макротекстом, тобто, єдиним інформаційним потоком, щодо якого всі інші повідомлення матимуть секундарний (вторинний, оціночно-коментаторський) характер, оскільки преса, радіо, телебачення не матимуть доступу до фактів.

4. Перетворення макротексту в політекст здійснюється за зворотнім алгоритмом: в інформаційний простір одноразово вноситься «*вичерпна*» інформація, що породжує множинні суперечливі версії її осмислення, наслідком чого стає формування бар'єру недовіри в масовій свідомості, а отже, втрата темою первинної актуальності.
5. Випереджаюче оперативне інформування (інформаційний менеджмент кризових ситуацій), спрямоване на породження єдино можливої версії інтерпретації сенсаційних фактів. Спін-доктор дозволяє загравати із агентами ЗМК, штучно створюючи атмосферу «плідного співробітництва», що насправді переслідує маніпуляторські наміри, виправдовуючи введення в оману і медіа-центри, і громадську думку.

Перформанс як ритуалізована маніпулятивна технологія в масовій комунікації є символічною декларацією причетності до більшості. Здебільшого влада, розігруючи "сходження в маси", керується сценарієм тимчасової гуманізації власного образу. Якщо маси не мають контакту з владою, тобто, трансцедентна влада перестає бути людинодосяжною, вона втрачає легітимність, оскільки найнестерпнішою образою для егалітарної масової свідомості є олігархічна політика, що робиться за спиною населення.

Перформанс має характер дійства з спільного творення "*політичного космосу*", в якому складна езотерична справа по управлінню суспільством трансформується в свято підтвердження суспільного договору: обидві сторони символічно засвідчують позицію солідарності в анонімній комунікації без адресата. Перформансна комунікація дійсно є безадресною, породжуючись завдяки ефекту символічної узурпації права на представництво волі всіх; ніхто ж не наважиться під час масового заходу провести оперативний моніторинг на тему "*Хто ініціатор*?". Невипадково бюрократичні установи, за словами відомого французького соціолога П. Бурд'є, можуть цілком легітимно маніпулювати суспільними конвенціями, укладачем яких є всі взагалі і ніхто зокрема.

Радянська партноменклатура влаштовувала перформанси як мінітеатри злагоди, що підтверджують міф про щасливе життя і про досконалу державу, де важливим є "*щастя цілого при неважливості щастя окремих частин*" (Платон).

"Зазнавши невдачі, – пише Г. Почепцов, оцінюючи роль перформансів в маніпулюванні процесами легітимації в імперіях, – імперія все одно продовжує своє існування у фіктивному режимі простору і часу. Адже живиться вона все одно, не природними, а вимушеними овоціями, оскільки тільки овації (або так звані "*тривалі аплодисменти*") записані в її кодах в якості основного волевиявлення народу по відношенню до влади. До речі, і всі ці тексти створено саме під канал овацій. Вся імперська система комунікацій будується на *прийом/ передачу* овацій, а не інших емоцій населення. Імперія – це великий театр, де тобі дозволено лише шалено аплодувати від щастя" [251-252].

Не менш цікавими з точки зору теорії і практики є маніпулятивні технології, розраховані на безсвідоме. Саме їм належить провідна роль у масових

комунікаціях інформаційного суспільства, культура якого давно вже набула ознак смислової роздрібненості. Парцеляція культурно-символічної реальності та інформаційного простору утруднює або унеможливлює пошук логоцентру, від якого вибудовується стратегія смислоорієнтації конкретних суб'єктів, а отже іноді функція смислоорієнтації передається безсвідомому. Трансформація суспільства на масове і деперсоналізація індивіда, супроводжуючи загальне налагодження життєвого світу в соціальному відношенні, не перекривають собою тієї деградації, яка відбувається в духовному вимірі. Парадоксальним є те, що у сучасної людини з її релятивізмом та нігілізмом з'являється потреба в ілюзорному, вірніше, в ілюзіоністі, який би непомітно переконав у чомусь значущому. Тому прийнятні для стародавньої культури пророцькі віяння скоріше заподіюють шкоду пророку, ніж будуть мати якийсь ефект. Ілюзіоніст і гіпнотизер оцінюються як справжні професіонали у справі переконання, в чому їм допомагають різноманітні психотехніки гіпнозу.

Гіпноз (грець.- Hypnos сон) — психотехнологія створення стану сну за умови тимчасової втрати свідомістю інтенції. Нормальна свідомість в принципі спрямована на щось, тобто, є інтенціональною. Втрата інтенціональності прирівнюється до гіпнотичного (або ж в послабленому варіанті — до трансового) стану, що досягається через:

- інформаційну ізоляцію чи перевантаження (або ж через штучне створення недостатньо насиченого чи інформаційно перенасиченого середовища);
- руйнування автоматизмів свідомості;
- інтерференцію (розсіювання) свідомості, вплив на яку відбувається через увагу;
- формування рефлексів-асоціацій, що запускають механізми трансового стану.

Перший спосіб пов'язаний із властивістю психіки переходити в автоматичний режим функціонування за відсутності подразників або ж при їх надмірній кількості. Інформаційно-статичне середовище втомлює свідомість, але не безсвідоме, з якого нічого нікуди не зникає. Стійке гальмування активності кори великих півкуль мозку може досягатись за рахунок монотонії будь-якого походження: візуального (*однокольоровий нерухомий фон*), ауділального (*повторювані звуки однієї тональності*), кінестетичного (*циклічні рухи*). Виходить, що на тлі загального притумлення все ж залишається невелика ділянка збудження, контрольована гіпнотизером.

За умови інформаційного перевантаження спрацьовує захисний механізм гальмування, оскільки кількість сигналів перевищує певну граничну величину, що може викликати розбалансування в роботі ЦНС. Введення у транс буде залежати від гіпнабельності та навіюваності як пропускних характеристик нервової системи.

Наприклад, рекламні презентації аферистів, що виступали від імені компанії "*Гербалайф*", досягали ефекту за рахунок підготовчих дій: перед

проведенням презентації у великій залі влаштовувалося щось на зразок дискотеки із гучною музикою, ілюмінацією, аерозольними спецефектами. Сенсорно перевантажуючи аудиторію, шахраї безперешкодно навіювати необхідні для них команди щодо купівлі підробок.

Друга психотехніка застосовується в умовах виконання автоматизованих дій інтелектуального, перцептивного, кінестетичного різновиду, коли звичний режим їх виконання переривається шоковим подразником і діяльність свідомості тимчасово припиняється. В момент шокової затримки маніпулятор отримує можливість для проникнення в безсвідоме і неконтрольованої закладки необхідної для подальшого маніпулятивного ведення інформації. Найпоширенішим варіантом вербальної маніпуляції і наведення трансу є побудова тексту із великою кількістю складнопідрядних та складносурядних синтаксичних конструкцій, оскільки нормальна "*довжина*" речення, для того, щоб воно сприймалось адекватно, не повинна перевищувати 13 слів. Саме в цьому діапазоні речення виражає закінчену думку. Якщо ж думка "*розчиняється*" в масиві смислових конструкцій, то свідомість відмовляється декодувати такий сигнал, і як завжди, на допомогу приходить безсвідоме. Допомога, однак, не є безкоштовною: за неї доводиться "платити" безсвідомим слідуванням команді маніпулятора. "*Руйнування шаблонів*" (О. Кардаш) ілюструється маніпулятивним прийомом "артистів", суть якого зводиться до повідомлення людині шокуючої неправдивої інформації і нав'язування слідом за цим вигідного для маніпулятора рецепту розв'язання проблеми.

У передвиборчих кампаніях наведення трансового стану досягається побудовою промов для зустрічей із виборцями таким чином, щоб промова містила масив псевдотексту великої довжини; псевдотекст при цьому оснащується прикладами, що можуть викликати емоційні реакції. Наприклад, депутат, зустрічаючись із виборцями, повідомляє, що нинішній голова місцевої ради запропонував збільшити розмір оплати за житлово-комунальні послуги, оскільки йому, мовляв, не вистачає коштів на будівництво чотирьохповерхового будинку у передмісті. Після наведення прикладу в текст вставляється сугестивна інформація, що стає доступною для безсвідомого завдяки реакції гніву, спричинену повідомленням.

"Іноді деякі звичні дії виконуються безсвідомо,...автоматично. В ці моменти свідомість загальмовується, ... і безсвідоме стає більш доступним. Простягання руки при зустрічі найчастіше є мимовільною реакцією. І якщо руку різко затримати, смикнувши, створити нестандартну ситуацію, розриваючи тим самим звичний шаблон, то це викличе у людини занепокоєння, достатнє для того, щоб перехопити ініціативу та створити ситуацію, сприятливу для наведення трансу." [253].

На телебаченні прийом застосовується у вигляді шокуючих вставок, що стосується як розважальних передач, так і звичних для всіх рекламних роликів. Наприклад, реклама харчового продукту, супроводжувана появою на екрані казкового мультиплікаційного персонажу, який вигукує рекламні гас-

ла. Тим самим також буде досягатись шокуючий фон, в який за сценарієм рекламіста може бути вбудоване сугестивне повідомлення.

Розсіювання свідомості досягається перевантаженням уваги, діапазон утримання інформації якої, за даними Д. Месмера, складає 7+/-2 елементи. При введенні більшої кількості інформаційних блоків (категорій) залишок інформації буде записуватись в безсвідоме.

Рефлекси-асоціації ще називають якорями. "*Якір*" – "*вузлик на пам'ять*", зав'язаний у безсвідомому і поєднаний здебільшого із емоційно-позитивними подразниками. Ними можуть бути насолода від фуршету, гарної музики, природного пейзажу, спілкування у світському товаристві тощо. Маніпулятор використовує подібні аттрактори, звично асоціюючи з ними перехід свідомості у новий режим зміненого стану. Останній часто-густо імітується спеціально підібраною командою натренованих акторів, які імітують "*захоплення*" і заражають тих, хто ще не встиг захопитися особою маніпулятора.

Однак не виключені і такі ситуації, де вузлик сформується через емоційно-негативне зараження. Наприклад, подібні психологічні рефлекси формуються під час релігійних ініціацій в багатьох модерних сектах, діяльності прозелітів, а також в практиці дисциплінарних санкцій у закритих унінодальних структурах. [254].

Під час перформативних ініціацій сатаністів і масонів вузли, асоційовані зі страхом, спричиняють запуск програми наведення гіпнозу при появі лідера або ж відтворенні атрибутів оточення. Так, сатанинський ритуал "*омолодження*" жриці включає вбивство, після якого учасники обмазують одне одного кров'ю жертви. Практикується також канібалізм, нагадування про який через різні візуалізації (фотознімки, відеозапис, художні полотна чи малюнки) уможливлює гіпнотичний ефект.

Резонансні маніпулятивні технології ґрунтуються на виведенні з безсвідомого потребнісно актуалізованого інформаційного запису із його багатоаспектним розкручуванням (*поліаналізаторною та політематичною текстовою мультиплікацією*). Останній міститься в стереотипах та першообразах колективного безсвідомого (*архетипах*). У стереотипах, де концентруються однобічно-редуковані "*передуявлення*", завжди існує простір додаткової атрибутизації явища, особи, факту. Наприклад, дискредитованого президента США Б. Клінтона можна при бажанні атрибутизувати не лише як людину із поганою моральною репутацією, але і як того, хто дискредитує американців як націю "порядних громадян". Зрозуміло, що останнє буде резонувати із стереотипними конструктами "*порядного громадянина*" і "*порядного американця*", який не дозволяє собі комбінувати справу і секс. Далі додаткова атрибутизація має бути розгорнута у громадське обговорення проблеми, де всі проектують і виплескують агресію на нововиниклий сенсаційний об'єкт, переконуючи себе в тому, що стереотип відповідає дійсності, тобто, американці і насправді такими є. Як тільки обговорення відбулося, розпочинається

етап мультиплікації: М. Левінскі пише книгу про роль і місце в її житті Білла, знімається скандальний міні-фільм про "*закат зірки*" Клінтона під час судових процесів Левінскі-Клінтон-Стар, монтуються радіотексти напівгумористичного плану, на побутовому рівні з'являються багаточисельні анекдоти про Білла і Моніку із смакуванням інтимних подробиць. Непопулярний політичний об'єкт аннігілюється як раз через перенасичення комунікацій наполегливим маразматичним реварюванням скандалу. Телеглядачі вже починають думати про те, що їх збираються переконати в тому, що вони і без того давно вже знають.

Стереотипний резонанс передбачає виведення на поверхню дискусії когнітивної складової стереотипу із пошуком такого об'єкту, який би міг викликати емоції, звично поєднані із когнітивною складовою. Так, російський кінорежисер С. Говорухін вибудовує більшість своїх сценаріїв на резонансі, зачіпаючи хворобливу для Росії тему *злочинної влади*. Оскільки влада щоразу зображується як анонімний колективний злочинець, залишається лише здогадуватись про те, що телеаудиторія буде підкріплювати негатив художньо-естетичними засобами.

Архетиповий резонанс є маніпулятивною технологією більш високого рівня складності. Практика архетипового резонансу в якості методологічної основи має аналітичну психологію К.Г. Юнга. Резонування із архетипами — первообразами колективного безсвідомого — не передбачає безпосереднє *провокування реакції гніву, образи, захоплення* чи відчаю; маніпулятор активізує витіснену або ж соціально-інституалізовану архетипову складову, тобто, складову актуалізованого чи неактуалізованого досвіду, після чого придушена енергія архетипу вивільняється і спричиняє соціальні десинхронізації.

Розглянемо застосування даної психотехнології на конкретному прикладі. Припустимо, в українській культурі існує архетип *Матері-Землі* — синтетичний образ *жінки-годувальниці*, генетичного початку. В архетипі міститься набір асоціацій-оцінок, своєрідний сценарій розгортання життя цього образу (*жінка-мати* приймає долю, не зазіхає на чуже життя, є самодостатньою щодо чоловіків тощо) — це актуалізована частина архетипу. Витісненою частиною архетипового досвіду буде нереалізована маскулінність, оскільки жінка-матір в силу своєї автономії розглядається в архетиповій парадигмі як чоловік в можливості (більш детально див. роботу Юнга "*Про архетип і особливо про поняття Аніма*"). Якщо маніпулятор спиратиметься на художній сценарій, то він або позиціонуватиме тотожній актуалізованому досвіду зміст, і тоді резонанс буде стосуватись посилення нарцисизму, *Его-тотожності*, або ж протилежний актуалізованій фігурі образ (підкреслено-маскулінний), що активізуватиме мотивацію "*сизигії*" (Юнг). І в першому, і в другому випадках досягатиметься модифікація соціальної метапрограми через посилення нарцисичної агресивності, ідеології ксенофобії, або ж через руйнацію селективних фільтрів соцієтальної психіки, посилення доступності культури в плані насадження іншокультурних кодів. Те, що для ар-

хетипового резонансу є найприйнятнішим візуальний канал, говорить сам Юнг: "*Representationes collectives* мають домінуючу силу, тому не дивно, що їх придушення спричиняє самий різкий опір... За батьківською чи любовною парою знаходяться змісти найвищого напруження, які не можуть бути апперцепійовані свідомістю і тому можуть стати помітними лише через проекцію. Те, що такі проекції – справжні події, а не традиційні думки, доводиться історичними документами. Вони вказують саме на те, що подібні сизигії проектуються як повна протилежність традиційному віросповіданню, а саме, у *візіонерській* формі переживння."[255].

Маніпулятивна психотехнологія імпринтингу (зомбування) демонструється в практиці пропаганди релігійних сект, передвиборчих кампаніях, рекламній діяльності. Вона синтезує досягнення НЛП, резонансних психотехнологій, індоктринації. Попри всі відмінності імпринтингу, ця психотехнологія включає деякий алгоритм-мінімум, що складається з таких етапів:

- Досягнення рапорту (контакту із безсвідомим). У НЛП найчастіше використовують т.з. калібровку (калібрування)- підлаштування під безсвідоме через улюблену репрезентативну систему, оптимальну з точки зору декодування аудіальну, візуальну чи кінестетичну семіотику реципієнта. Вписуючись в найприйнятнішу семіотику "жертви", маніпулятор досягає резонансу, стягуючи на себе енергопотік психіки.
- Провокування неоптимального психічного стану, афекту. Найчастіше провакується страх, емоційне захоплення, гнів. Фокус уваги при цьому тимчасово втрачається, безсвідоме стає повністю відкритим для завантаження кодами: "*жертва*" символічно вмирає.
- Етап "*реанімації*", на якому маніпулятор виводить закодовану жертву на рівень усвідомлення того, що з нею відбулася психологічна трансформація. Оскільки жертва не знає про те, який код вона "проковтнула", то маніпулятор пропонує "допомогу" у вигляді наставництва, співробітництва, окремих "*безкорисних*" послуг тощо.
- Етап встановлення якоря-активатора, що може мати будь-яке походження, але має обов'язково викликати звичні асоціації, зв'язуючи по горизонталі спровоковану емоцію, психологічну реанімацію та образ "*рятівника*" – маніпулятора [162; 218; 240; 256-263].

Таким чином, маніпуляція в масових комунікаціях відбувається в просторі впливу на когнітивну, емотивну та регулятивну психічні функції індивіда, соціальних мікрогруп та соціальних метапрограм великих спільнот (*націй, континентальних угруповань*). Останнє випливає з принципу психічної гомологічності індивідуальної та соцієтальної психіки, в рівній мірі як і ролі маніпулятора, яким може бути не лише індивідуалізований суб'єкт, але і анонімні соціальні спільноти, неструктуровані мікрогрупи та натовпи, що маніпулюватимуть кимсь, навіть не маючи цього на меті.

2.6. Практика манипулирования массовым сознанием в СМИ и способы ее нейтрализации

Минувший век, ознаменовавшийся двумя мировыми войнами и беспрерывными социальными катаклизмами, привел ответственных политиков во всем мире к осознанию необходимости целенаправленной работы по защите психики широких масс населения от пагубного влияния экстремистских антисоциальных идей и деструктивных технологий, расцветших на гребне технократизации и информатизации общества. В этой озабоченности следует искать объяснение того внимания, которое уделяют сегодня руководства ведущих стран мира мониторингу масштаба и характера влияния на население основных медиа-информационных центров.

Каковы причины взрывного роста популярности электронных СМИ, отмечаемого со второй половины XX в.? Ученые усматривают в телевидении непревзойденное средство гиперкомпенсации массы - возможность символического, виртуального утоления хронически неутоляемых эмоциональных потребностей и фантазийного бегства от хронически нерешаемых насущных проблем, - некий тотальный "опиум народа".

Это то, что лежит на поверхности. Есть и другие, более глубокие объяснения. В психологии современного человека доминируют две противоположные тенденции, находящиеся между собой в отношениях диалектического единства и борьбы. С одной стороны, тенденция к индивидуализации, способствующая обособлению человека в пространстве частных интересов (собственных и своей семьи); с другой - тенденция к инфляции личности, ее растворению в массовой субкультуре, отказ от индивидуальности в надежде восстановить утраченное чувство социального единства.

Электронные СМИ (телевидение, Интернет) в какой-то мере снимают это противоречие, поддерживая в человеке иллюзию интерсубъективности, уникальных личных отношений с источником информации, при этом все более вовлекая его в процесс массообразования. Человек становится элементом толпы, что называется, не выходя из собственного дома. Одиночество в толпе — центральная проблема экзистенциально-гуманистической философии XX в., - обретает свое новое звучание - ощущение толпы в одиночестве. Самое тревожное в этом то, что ощущение утраты внутренней цельности и самоидентичности перестает восприниматься людьми как нечто ненормальное, противоестественное.

Такое состояние сознания человека, утратившего внутренний стержень для целостного восприятия окружающей его социальной реальности и своего места в ней, получило в психологии название масса. Говоря о состоянии массы, психологи обычно подразумевают специфическую совокупность психических качеств людей, пребывающих в том или ином измененном состоянии сознания. Массообразование всегда сопровождается психологическим регрессом - возвратом к более примитивным, архаическим формам реакций и мировоззрения.

Добиваются этого психологически компетентные политтехнологи разными способами. Во-первых, за счет выстраивания эффективной символики воздействия на массу, символики рекламных, имиджевых подач; во-вторых, за счет адекватного массовым запросам манипулирования, т. е. управления массой, вывода ее на предсказуемые реакции; в-третьих, посредством закрепления архаических, примитивных реакций в неких цивилизованных формах их проявления, начиная с покупки тех или иных товаров и заканчивая "правильным" голосованием на выборах.

Большинство современных концепций массообразования декларирует необходимость развития трех основных форм целенаправленной работы с массой: работы в сфере политической власти; работы в сфере маркетинговых программ; а также работы в сфере организации эффективных имиджевых подач, что, в свою очередь, напрямую связано с эффективностью социального управления массой со стороны конкретных лиц или организаций. Все вышеуказанные формы работы с массой осуществляются в информационном пространстве, главным образом, в сфере действия СМИ.

Стратегии массообразования строятся, исходя из специфики того концептуального и технологического аппарата, который был выбран конкретным политтехнологом в качестве объяснительной и инструментальной модели для проектирования и осуществления манипуляции. В настоящее время основные стратегии манипулирования массовым сознанием разработаны в психофизиологическом, психодинамическом, идеологическом и трансперсональном дискурсах.

Обзор современных манипулятивных стратегий. Психофизиологическая (условно-рефлекторная) стратегия манипулирования массой напоминает хорошо известный еще с советских времен принцип взаимодействия власти и населения по типу "сделал (сказал) - получи". Концептуальная модель, построенная на понимании массовой психики как системы коллективных рефлексов, породила соответствующую стратегию манипулирования массой, основанную на провоцировании рефлекторных реакций с позитивным, а чаще негативным подкреплением. В качестве примера можно привести эпизод с покупкой лотерейных билетов грозным управдомом (Н. Мордюковой) в фильме "Бриллиантовая рука": "Распространите билеты среди жильцов!", - "А если не будут брать?", - "Не будут брать, - отключим газ!".

Этот метод управления массой довольно эффективен, но чересчур громоздок и дорогостоящ. Его громоздкость проистекает из необходимости содержать многочисленный аппарат, способный обеспечить тотальный контроль над массой. Затратность условно-рефлекторной модели обусловлена возникновением эффекта гипертрофированной патерналистской иллюзии массы. Эта иллюзия основана на идентификации себя с малыми детьми, которым к праздникам "партия и правительство дарит подарки", обеспечивая удовлетворение "растущих потребностей".

В своей завершенной форме патерналистская иллюзия порождает самоощущение младенца, присосавшегося к материнской груди, восприятие себя в качестве человека, которого "кормит власть". Такая модель с точки зрения социального контроля не лишена прагматизма: младенец, когда он присосан к груди, в общем-то, удовлетворен. Но, к сожалению, "материнской груди власти" на всех не хватает и очень быстро у сформированной таким образом массы возникает так называемый оральный упрек: "Ты не настоящая мама, ты бросаешь меня; хочу другую, более любящую маму!"

Опыт столкновения властей с оральным упреком масс в условиях затратной модели политики имеется в истории многих стран с колониальным и тоталитарным прошлым. Патерналистские отношения оборачиваются тенденцией к блокированию социальных подключений личности. Личность становится потребляющей и продающей свою политическую волю в условиях потребительского отношения. В рамках такого отношения социальность теряется и человек укореняется на уровне узко групповых и/или индивидуальных ценностей.

Условно-рефлекторная стратегия массообразования широко представлена сегодня в рекламных технологиях манипулирования массовым сознанием: "Это вкусно, с этим не больно", "Купи это и получишь то", "Поучаствуй там-то и выиграешь то-то". Вершиной развития данной манипулятивной стратеги явилась объяснительная модель нейролингвистического программирования, основанная на детальном учете и использовании психофизиологических запросов объекта воздействия.

К условно-рефлекторным технологиям, построенным по типу "если - то" и эксплуатирующим рефлекс страха, часто обращаются военные психотехнологи при планировании и проведении психологических операций (ПсО). Так, во время вторжения вооруженных сил США в Панаму (1989 г.) в тактике американских подразделений ПсО применялся метод так называемых "беспокоящих действий".

На все окруженные панамские группировки проводилось вещание через громкоговорящие установки, затем давалось 15 минут на размышление, по истечении которых в ультимативном порядке предлагалось вывесить белые флаги и сдать оружие. В случае неисполнения требований начиналось "ограниченное применение силы". По вызову командира части, блокирующей гарнизон, прибывал вертолет огневой поддержки, который имитировал нападение на объект, а звуковещательные средства призывали сдать оружие и назначали новое время. Это действие повторялось помногу раз и оказывало сильное психологическое воздействие на личный состав панамских войск: многие опорные пункты сдавались без боя.

Психодинамическая стратегия манипулирования массовыми психическими процессами, разработанная на основе психоаналитической теории З. Фрейда и его последователей, является на сегодняшний день наиболее разработанной в технологическом отношении. Достаточно сказать, что модный

термин PR рожден также в психоаналитическом дискурсе (основоположник современной PR-концепции, Эдвард Бернайз - племянник З. Фрейда) и первоначально означал прикладное психоаналитическое знание о средствах манипулирования коллективным бессознательным с целью эффективного символического воздействия на массовые процессы.

Психоаналитическая теория базируется на постулате о том, что в основе поведения людей лежат неосознаваемые мотивы, которые могут фиксироваться профессионалами и искусственно запускаться в направлении, выгодном для управляющей стороны. Основной потребностью человека, как утверждают современные политтехнологи психоаналитического направления, является неосознаваемая потребность быть маленькими, складывающаяся из множества неутоленных детских ожиданий и травматических детских фиксаций. Именно потребность быть маленьким заставляет взрослого человека искать, кому бы подчиниться, всячески идеализировать власть, наделять ее полномочиями внешней, довлеющей, бесконтрольной силы.

Большинство технологий, разработанных в русле психодинамической стратегии массообразования, представляют собой средства, облегчающие человеку поиск в лице власти идеального родителя. Они символически растолковывают человеку, кому нужно подчиниться, чтобы получить возможность отыграть весь комплекс своих инфантильных пожеланий и фантазий. В бессознательном каждого человека в той или иной степени присутствует запрос на власть. Человек, даже очень развитый, хочет время от времени расслабиться, почувствовать себя маленьким, прощенным, свободным от груза ответственности и за эту возможность он готов расплачиваться любовью, восхищением, трудом, готовностью идти на жертвы. Это то, что, по мнению психоаналитиков, составляет глубинную психологическую основу, канву любых властных отношений по ту сторону идеологий, сознательных целей и ценностей, других составляющих бытия человека, производных от принципа реальности.

Благодаря К. Г. Юнгу мы знаем, что кроме индивидуальных, вытесненных, подавленных форм биографического опыта, в нас жив еще и опыт наших предков, реальные формы психологических процессов и психологических содержаний, которые воздействуют на нас как закон, т. е. чрезвычайно нормативно и строго. Коллективное бессознательное управляет человеком без малейших поблажек к его индивидуальной воле.

Согласно юнгианской традиции, наша сознательная личность - это всегда "задний ум", это всегда рационализация того, что произошло не по нашей воле, а по воле тех структур в психике, которые производны от национальной традиции, языка, истории, от групповой идентичности, связанной с государством и т.д.

В настоящее время существуют очень серьезные технологии выявления наследуемых схем поведения (З. Фрейд), которые запускаются тогда, когда для них возникают адекватные социальные условия. В психологии К. Г. Юнга эти

наследуемые схемы поведения или поведенческие сценарии называются архетипами. Человек разделяется в своей психической организации на два уровня детерминации поступков - личностный и глубинно бессознательный. Глубинно бессознательный уровень всегда "побеждает", иными словами, коллективное бессознательное в конечном итоге всегда определяет направленность действий человека.

Традиция выявления логики коллективного бессознательного существует уже тысячелетия. Обращение к этой логике в обход сознания людей с целью управления ими называется символическим манипулированием. Этот тип манипулирования сознанием предусматривает использование архетипически ориентированных символических форм в рамках наглядной агитации, рекламных кампаний, всего, что обращается к массе и способно подвигнуть ее на определенные действия.

Такой метод манипуляции людьми показал свою исключительную эффективность во время последней президентской кампании в России. Анализ работы политтехнологов по продвижению имиджа В. Путина вскрыл наличие в коллективном бессознательном россиян простых архаических схем, использование которых способно сделать массообразование в стране простым, предсказуемым и мало затратным делом. Примитивность вскрытых бессознательных паттернов реагирования, с одной стороны, испугала российских психологов, с другой стороны, успокоила. Жить в стране, где нет четкого алгоритма манипулирования массой, во-первых, дискомфортно, во-вторых, опасно (если массой не управляют отечественные силы и технологии, ее структурируют иноземные).

Психоаналитическая стратегия предлагает разработанную структуру подобного рода понимания и воздействия на бессознательное, состоящую из пяти основных блоков информации.

Во-первых, это технологии, обеспечивающие возможность выбора для каждого типа социума наиболее адекватного социального мифа. Социальный миф - это форма групповой веры в определенные цели и ценности, в необходимость определенной модели властных отношений и тому подобные социально значимые вещи. В настоящее время к числу наиболее действенных социальных мифов можно отнести: национальный, имперский и демократический мифы. Россия после десяти лет нестабильности и поисков, похоже, сделала выбор в пользу традиционного для нее имперского мифа. Украине еще предстоит определиться в своем выборе консолидирующей идеологии.

Второй блок накопленной информации - это проблема адекватности имиджевых характеристик правителя бессознательному запросу массы. Последний включает в себя как биографический запрос (подачу в виде доброго или злого отца, заботящейся или строгой матери и т. п.), так и запрос архаики коллективной памяти (символику тем или образов из исторического прошлого народа), которые должен удовлетворить данный представитель власти для того, чтобы сформировать позитивную ответную реакцию массы на его

имидж. Эта тема является наиболее разработанной, как в отечественной, так и зарубежной политической психологии.

Третий блок связан с проблемой харизматичности - поиском и поддержкой лидеров, способных управлять массой. В рамках каждого типа массовой психологии существует набор архетипов, которые запускают или персонифицируют групповую массовую идентичность. Человек обретает харизму тогда, когда, как правило, случайно начинает соответствовать тому облику, который оказывается востребованным массой на данном историческом рубеже для решения задач сплочения и защиты интересов массы. Создать харизматического лидера практически невозможно, однако существует возможность, детально изучив коллективную архаику той или иной социальной группы, целенаправленно подбирать для нее харизматических лидеров, способных обеспечивать трансформацию данной социальной группы в требуемом направлении. Такого рода политическое обеспечение (поиск и поддержка харизматических лидеров) особенно необходимо для стран, находящихся на этапе реформирования и вынужденных идти на непопулярные в народе изменения.

Четвертый блок проблем связан с учетом психологических особенностей конкретных типов массы. В психоаналитической концепции любого рода задачи всегда проигрываются на индивидуальной модели психической организации объекта. Следуя традиции Платона, даже целую страну можно смоделировать как отдельного человека: мужчину или женщину, человека с соответствующей формой детского (исторического) опыта, своими особенностями темперамента и характера, своими верованиями и привычками. Для каждой социальной группы, независимо от ее масштаба, можно создать такого рода объяснительную модель для проведения в дальнейшем направленных манипуляций с этой группой. Моделирование психической организации объекта применяется для определения характера коллективной патологии той или социальной группы и ее комплиментарности коллективной патологии других социальных групп, для изучения групповых страхов и групповых ожиданий, устойчивых паттернов реагирования, заложенных в той или иной культуре, а также других подобных исследованиях. На основе этой работы строится соответствующий прогноз массового поведения и подбирается соответствующая технология воздействия на бессознательное массы для удержания ситуации в сфере массообразования под контролем.

Пятый блок накопленного психоаналитиками опыта связан с учетом специфики политической деятельности. Политик — это человек, который в своей деятельности воспроизводит систему власти, олицетворяет тот или иной тип властных отношений. Согласно взглядам психоаналитиков, "проклятье" политика, как знаковой фигуры, состоит в том, что он должен постоянно находиться в позиции взрослого - позиции, означающей необходимость постоянно принимать решения, управлять массой, нести ответственность за свои поступки. Соответственно, глубинно психологическая проблема политического процесса - это еще и проблема обеспечения психологического здо-

ровья и эффективности работы конкретных политиков. Она включает методы создания адекватной запросам политика коммуникативной атмосферы, адекватного стиля принятия решений и отношений с ближайшим окружением, критериальной системы оценок его деятельности руководством, методы психологической разгрузки и другие средства минимизации стрессогенных факторов, порождаемых спецификой политической деятельности. Глубокое понимание специфики политической деятельности и особенностей самочувствия человека, участвующего в политике, облегчает задачу манипулирования конкретным политическим лидером, играя на его человеческих потребностях, состоянии здоровья, ближайшем окружении и т. п.

Таким образом, согласно психоаналитической стратегии основной мишенью для манипулирования является бессознательное человека, а социальная манипуляция - это не зло, которое должно быть преодолено, а, напротив, - необходимое средство поддержания адекватной системы властных отношений в обществе. Человек, подвергшийся манипуляции "на самом деле" не унижен и не использован, а получил то, о чем мечтал всю свою жизнь и, прежде всего, уверенность в том, что он не одинок в своих проблемах, а подключен к общему делу. Даже если для этого дела он должен сегодня пожертвовать своими интересами, отложить на неопределенный срок удовлетворение насущных потребностей. Именно в психодинамической традиции политического анализа утвердился в качестве аксиомы тезис, что только посредством манипуляции, за счет подключения к коллективному бессознательному массы человек может обрести смысл своего существования.

Идеологическая стратегия манипулирования массовым сознанием была доминирующей на протяжении всего XX в. Жестокое противостояние трех ведущих идеологий - коммунистической, корпоративистской и либеральной, - повлекшее за собой неисчислимые беды от двух мировых войн и последовавшей за ними холодной войны, с ее тотальным идеологическим противоборством и гонкой вооружений, завершилось на рубеже тысячелетий торжеством либеральной идеологии.

Система социальных взглядов становится идеологией тогда, когда обретает способность предложить человеку целостную и непротиворечивую картину мира, позволяющую ему адекватно осознавать и реализовывать свои интересы. Принимая ту или иную идеологию, человек начинает пользоваться ей, как топографической картой, использовать ее язык, подключаться к имплицированным в ней ценностям. Так, незаметно для себя, он оказывается во власти иллюзий, наработанных этой идеологической машиной, всецело встраивается в формат ее дискурса.

Идеологические иллюзии в данном контексте можно рассматривать как механизм манипулирования массой. Как утверждают жрецы политтехнологий, человек не может жить вне системы иллюзий -фантастических образов исполнения желаний. Следует отметить, что желания эти в массовом масштабе не исполнимы по определению, это именно иллюзорные, невозможные

ожидания, обретающие видимость возможных благодаря активности идеологов и манипуляторов массовой психикой.

Иллюзия религиозного или национального возрождения, иллюзия заботы власти о народе и т. п. - это на самом деле бессмысленные словосочетания, но если люди в них верят, они обретают смысл и придают людям уверенности в их реальных повседневных заботах.

Иллюзия может творить чудеса. При помощи иллюзии люди нередко обретают смысл своей жизни и за хорошую иллюзию они готовы порой отдать свою жизнь. Достаточно вспомнить коммунистическую иллюзию, столь хорошо идеологически подкрепленную, что она убивала в миллионах людей даже инстинкт самосохранения.

Теории иллюзий не существует. Иллюзии - это ценности, о которых не принято сообщать массе. В своей совокупности иллюзии составляют социальную мифологию той или иной страны, той или иной политической системы. Например, современные либерально-демократические мифы о "равных возможностях", "общечеловеческих ценностях", "незримой руке рынка" или особо циничное словосочетание - "гуманитарная военная операция".

Деконструкция иллюзий - процесс очень болезненный для человека. Поэтому мы можем публично разоблачать иллюзии только тогда, когда они умирают. Так, мы можем сегодня спокойно разбирать коммунистические мифы, говорить какова, с точки зрения психологии, символика серпа и молота, красного знамени, ленинского мавзолея или ленинского бюста, октябрятской звездочки или комсомольского значка. Это мертвая идеология, работающая в настоящее время исключительно на ретроспективе и ностальгических чувствах.

Сегодня в постсоветской психологии очень активно развивается знание об иллюзорных запросах людей. Рост интереса к подобным знаниям связан с тем, что на нынешнем постсоветском пространстве практически нет ни одной страны, где иллюзорные запросы людей совпадали бы с реальной системой власти и реальной идеологией. Явно назрела необходимость в коррекции идеологических постулатов и иллюзорных образов, обращенных к широким слоям населения. Очевидно, что в России раньше других поняли этот социальный запрос, так как процесс создания общенациональной идеологии в этой стране явно получил новый импульс.

Наконец, самая молодая трансперсональная стратегия манипулирования массой предлагает оригинальные классификации и технологии использования так называемых измененных состояний сознания: техники наведения транса, методы продуцирования коллективных и массовых психозов, способы подключения к массообразованию с использованием психоделических средств и т. п. Эта стратегия активно применяется сегодня в молодежной среде, в многоуровневом бизнесе, рекламе, а также при организации массовых политических мероприятий "за" или "против" того или иного политика (политической партии).

Направления и приемы манипуляции массовым сознанием. Сегодня, спустя 15 лет, после того как наша страна обрела независимость и встала на путь демократических преобразований, можно с уверенностью говорить о том, что в Украине сложилась собственная специфическая система подготовки и проведения избирательных кампаний. Многочисленные партии, незаурядные общественные и государственные деятели, активно вовлеченные в политический процесс, не без основания надеются обрести представительство в национальном парламенте. Однако избирательные кампании в Украине имеют свойство преподносить кандидатам в депутаты неожиданные сюрпризы. Как и накануне предыдущих кампаний, ни один аналитик не рискнет с уверенностью предсказать результаты предстоящего голосования.

Одной из причин этой неопределенности является то, что утвердившаяся за последние годы "стабильная нестабильность" украинского общества, социальная и идеологическая неоднородность электората ограничивает возможности применения в стране традиционных избирательных технологий.

К числу распространенных мифов последнего времени относится сведение проблемы ресурсов избирательной кампании к вопросу ее финансирования. Бытующее представление о всевластии денег в избирательной кампании не лишено смысла, однако, многократно преувеличено. К числу основных избирательных ресурсов кандидата относятся: его собственные личные и профессиональные качества; политический вес его опорной общественно-политической структуры (партии); связи кандидата с властью, политическими и общественными организациями; информационные ресурсы (связи со СМИ); интеллектуальные ресурсы его команды; людские ресурсы (количество и качество активистов, привлеченных к проведению кампании) и др.

Особое место в успехе избирательной кампании занимает так называемый манипулятивный ресурс, определяемый наличием в команде кандидата специалистов, обеспечивающих успех избирательной кампании за счет использования современных психотехнологий управления состояниями и поступками людей. В зависимости от качества используемых психотехник манипулятивные технологии подразделяются на грубые и тонкие.

К грубым манипулятивным технологиям относится все то, что с подачи прессы получило название административный ресурс. Этот ресурс включает в себя: прямое административное давление на избирателей, включая подкуп, угрозы и подтасовку голосов; давление на конкурентов и т. п. С чисто электоральной точки зрения эти технологии нельзя признать особо эффективными, особенно в долгосрочном плане. Как показали события осени 2004 года, применение административного ресурса имеет свои пределы и может вызвать взрывной противоположный эффект: становясь достоянием гласности грубые административные манипуляции озлобляют избирателя.

Одной из основных черт, определяющих эффективность манипуляции, является скрытостъ проводимого воздействия. Поэтому тонкие, неявные виды манипуляций, определяющие успех всей избирательной кампании, как правило, остаются в тени, за кадром. В зависимости от избранных манипулято-

ром в качестве основных мишеней воздействия, выделяются следующие направления манипулирования массовым сознанием:

- семантическое манипулирование;
- логическое манипулирование;
- манипулирование эмоциями;
- манипулирование образами;
- манипулирование культурными стереотипами и общественными мифами и т. п.

Для каждого из указанных направлений манипулирования общественным сознанием разработаны специфические технологии манипуляции.

Так, семантическое манипулирование - манипулирование значениями и смыслами слов, - является основным в пропагандистской, рекламной работе, центральным содержанием деятельности всех без исключения современных СМИ. Во французском учебнике по пропаганде 1954 года "Психологическая война" указывается на это содержание деятельности СМИ: "В пропаганде речь идет уже отнюдь не о том, чтобы открыто писать в газете или говорить в радиопередаче, что именно, согласно желанию пропагандиста, индивид должен думать или чему он должен верить. Фактически проблема ставится так: заставить такого-то и такого-то думать то-то или, точнее, заставить определенную группу людей действовать определенным образом. Как этого достигают? Людям не говорят прямо: "Действуйте так, а не иначе", - но находят психологический трюк, который вызывает соответствующую реакцию. Этот психологический трюк называют стимулом. Как видим, пропаганда, таким образом, уже не имеет ничего общего с распространением идей. Речь идет не о том, чтобы распространять идеи, а том, чтобы распространять "стимулы", то есть психологические и психоаналитические трюки, которые вызывают определенные действия, определенные чувства, определенные мистические порывы.

Одним из наиболее перспективных направлений семантического манипулирования, тесно связанных с работой идеологов, является создание собственного языка (дискурса) партийной идеологии и соответственно развенчание (деконструкция) базовых идеологических терминов политических оппонентов. Примером создания эффективного искусственного языка в политике является введение американскими политтехнологами в мировую практику так называемого языка политкорректности.

Работы по созданию этого языка начались в США еще во время вьетнамской войны. Были составлены целые словари (тезаурусы) для обозначения тех или иных явлений и действий, которые производили бы на читателя и зрителя нужное впечатление. Из языка были исключены все слова, вызывающие отрицательные ассоциации: война, наступление, оружие для поражения живой силы противника. Вместо них были введены слова: конфликт, операция, взрывное устройство и т. п. Мертвые зоны, в которых диоксином была уничтожена растительность, были названы "санитарными кордонами", на-

палм - "мягким зарядом", концлагеря для вьетнамцев — "стратегическими селениями". Как заявил тогда президент американского лингвистического общества Д. Болинджер: "Америка - это первое общество, которое добилось настоящего табу на все неприятное".

В настоящее время язык политкорректности - не только способ навязывания США остальному миру своего описания политической реальности, но и мощнейшее средство управления этой реальностью. Нужно отдавать себе отчет, что это чрезвычайно эффективный, хорошо структурированный язык, позволяющих безошибочно опознавать своих и крушить врагов, называть одни бомбардировки справедливым возмездием, другие международным терроризмом, одних политиков со средствами - реформаторами, других - олигархами, одних лидеров - врагами народа, других - спасителями нации.

Большую роль в манипуляции сознанием массы играет так называемое логическое манипулирование - подтасовки значений и смыслов утверждений за счет сознательного манипулятивного пренебрежения законами логики. Логический аргумент нередко подменяется эмоциональной оценкой, а отсутствие смысла сказанного или грубое "передергивание" смысла маскируется лавиной информационного шума.

Раскрытие содержательного ядра логической манипуляции способно не только разрушить начальный замысел манипулятора, но и обратить против него заряд "праведного гнева" обманутых людей. Вот почему крайне желательно наличие в команде политической партии (блока) философов и психологов - специалистов по организации контрманипулятивных действий. Метод психологического анализа текстов с целью выявления логической манипуляции изложен в книге Р. Бэндлера и Дж. Гриндера "Структура магии".

Важнейшим объектом для манипуляции является эмоциональная сфера. Можно сказать, что в политической предвыборной борьбе игра на чувствах избирателя - обязательный этап. Основатель учения о манипуляции сознанием массы Г. Лебон писал: "Массы никогда не впечатляются логикой речи, но их впечатляют чувственные образы, которые рождают определенные слова и ассоциации слов".

Общей принципиальной установкой в манипуляции массовым сознанием является предварительное "раскачивание" эмоциональной сферы. Политик должен предвидеть, какой эмоциональный отклик у людей вызовет то или иное его высказывание, заявление, политический поступок, та или иная партийная акция или пропагандистский жест (новый лозунг, листовка, видеоклип и т. п.). Подобного рода консультацию ему должен предоставить опытный психолог-практик.

Мы уже указывали на то, что своевременное разоблачение манипуляции политического оппонента способно пробудить у людей чувство гнева и возмущения в его адрес. Большим побудительным зарядом обладает эмоция страха - ни одна другая эмоция не оказывает столь сильного влияния на мотивационную сферу человека.

Важнейшая сфера манипуляции сознанием избирателя -манипулирование образами и символами. В каком-то смысле можно говорить, что вся предвыборная борьба происходит в сфере символического. Тот же Г. Лебон писал еще в XIX в.: "Толпа мыслит образами, и вызванный в ее воображении образ в свою очередь вызывает другие, не имеющие никакой логической связи с первым... Толпа способна мыслить только образами, восприимчива только к образам. Только образы могут увлечь ее или породить в ней ужас и сделаться двигателями ее поступков".

Изучение символики образов сегодня прерогатива исследований глубинной психологии, прежде всего психоанализа и аналитической психологии К. Г. Юнга. Психоаналитическая стратегия манипулирования массовыми психическими процессами, разработанная на основе теории З. Фрейда и его последователей, является на сегодняшний день наиболее разработанной в технологическом отношении. Первым психоаналитиком, применившим понятия психоанализа для целей политической рекламы, был Э. Дитрих, психолог из Вены, создавший в США "Американский институт по изучению мотивации поведения" и работавший советником в избирательной кампании Кеннеди. Вслед за институтом Дитриха в США возникли другие центры, изучавшие возможность использования психоанализа в политических целях. На постсоветском пространстве можно выделить группу В. Медведева, специалистов в области политического психоанализа Восточно-европейского института психоанализа в г. Санкт-Петербурге, обеспечившую поддержку Б. Ельцина в президентской кампании 1996 г., а также группу кремлевских политтехнологов Г. Павловского, приведшую к власти команду В. Путина.

Обращение к архетипам коллективного бессознательного в обход сознания людей с целью управления ими, называемое символическим манипулированием, предусматривает использование архетипически ориентированных символов в наглядной агитации, текстах политиков и публичных политических акциях.

Практика манипулирования массой с использованием СМИ. Существуют общие для всех вышеперечисленных стратегий манипуляции массовым сознанием приемы психологического воздействия на массу, обусловленные спецификой основного канала реализации этого воздействия. Таким универсальным каналом массообразования на сегодняшний день являются СМИ, а в качестве основного субстрата, воздействующего на аудиторию, выступает информация. Для достижения конкретных целей в сфере массообразования ни одна из вышеперечисленных манипулятивных традиций не может обойтись без разработки и тиражирования специальных информационно-пропагандистских материалов, требующих соответствующих форм подачи.

Считается общепринятым, что информационно-психологическое воздействие на объект должно осуществляться в два этапа. Первый определяет-

ся как подготовительный. Его назначение - создать атмосферу доверия между источником информации и объектом воздействия. Содержание второго заключается во внедрении информации в бессознательное массы и закрепление ее там в качестве социального интроекта.

Деление на указанные выше этапы является относительным и условным. Его не следует рассматривать так, что сначала идет серия информационных сообщений, решающих лишь задачи первого этапа, а затем следуют пропагандистские материалы в соответствии со вторым этапом. Задачи обоих этапов решаются в процессе практически всех осуществляемых информационно-пропагандистских акций. В определенное время может наблюдаться лишь некоторое преобладание в сообщениях материалов, свойственных для одного из данных этапов.

Источник, вызывающий доверие, считается достоверным, правдивым и компетентным. Эффект подключения к массообразованию чаще возникает у того объекта воздействия, который добровольно обращается к определенному источнику информации.

Для создания доверия к источнику информации используются следующие приемы:

- Создание имиджа "особой осведомленности" о событиях, которые могут замалчиваться в силу различных причин официальными источниками информации. Доверие телезрителя (слушателя, читателя) к источнику информации может создаваться передачей достоверных сведений, точность которых заранее известна объекту воздействия или может быть легко им проверена. К категории такой "убеждающей информации" относятся, в частности, фактические данные: имена, названия улиц, номера домов, огромное количество деталей - точных сведений, в которые упаковываются информационные сообщения.

Такая информация снижает у объекта воздействия естественную критичность по отношению к самому источнику информации. Это одно из важнейших правил суггестии, требующее неукоснительного выполнения. Факты, согласно этому правилу, следует подробно освещать, когда нет необходимости их замалчивать или видоизменять. Если объектом воздействия в предъявленной информации выявлена ложь или передержки, власть источника информации над ним существенно ослабевает.

- Создание имиджа "объективности и независимости" или "альтернативности" официальным источникам информации. Достигается цитированием документов, оценок экспертов, свидетельских показаний, отчетов и всевозможных других материалов с обязательным включением элементов самокритики. Восприятие таких материалов носит кумулятивный характер, создает впечатление убедительности и дает не меньший результат, чем тщательно аргументированное обсуждение какого-либо вопроса.

- Оперативность. Доверие создается также более оперативной информацией о текущих событиях, изменениях обстановки, с преобладанием тематики,

не находящей освещения в других источниках. Сообщения по таким темам нужно делать просто и доступно. Истинность (достоверность) в данном случае не обязательна, так как информация такого рода не поддается перепроверке.

Источник информации, первым сообщивший о событии, будет затем более предпочтительным для аудитории, чем другие. Таким образом, технический вопрос о скорости передачи сообщения перерастает в стратегический в контексте осуществления психологического воздействия на аудиторию.

Для того, чтобы усилить эффект сверхоперативности используется также сенсационность, создается ощущение необычайной важности передаваемого сообщения. Сенсационность используется также как прием привлечения внимания и расширения своей аудитории. Опережение официальных (других конкурирующих) источников информации создает ореол осведомленности, хотя информация может в значительной степени фабриковаться на основе не достоверных материалов и сомнительных источников.

Другой психологический эффект сверхоперативности - это "эффект присутствия", заключающийся в иллюзии повсеместного наличия своих источников информации. Это достигается за счет быстрой передачи информации даже о незначительных событиях, происходящих в различных регионах и населенных пунктах.

Человек, услышавший, прочитавший или увидевший какую-либо информацию раньше другого, подсознательно ощущает себя более значимым, хотя практической пользы из полученной информации он не извлекает. Первое сообщение о том или ином факте, событии оказывает более сильное воздействие на объект, чем последующее. Сообщивший информацию первым создает социальную установку ее восприятия и толкования, всем остальным же приходится ее изменять, что намного сложнее, требует больших усилий и времени.

- Предсказание событий, которые источнику событий были известны заранее. "Голос предсказателя" может ссылаться на события, которые он, якобы, предсказал ранее (и которые, на самом деле, получили развитие, схожее с "предсказанным" в силу объективного развертывания событий, либо в силу случайности).

Интерес к передаваемой информации во многом зависит от потребности в ней, а также от интонации, акцентирования, системы аргументов, подачи информации с использованием просторечного языка и диалекта.

Большая роль отводится эмоциональному оформлению передаваемой информации, которое создается при помощи разнообразных экспрессивных средств подачи, изобилующих в арсенале современных СМИ. Создаваемое настроение должно соответствовать содержанию передаваемой информации. Истоки данного приема теряются в глубине веков - в культовых обрядах и ритуальных мистериях. Воздействию данного приема особенно подвержены молодежь и эмоционально экзальтированные люди с недостаточной критичностью и самостоятельностью мышления.

Достижение конкретных целей осуществляется с помощью приемов внушения и убеждения.

Приемы внушения. Эффект внушающего воздействия определяется в первую очередь не содержанием информации, а ее внешней формой, выразительностью, эмоциональной окраской сообщений, авторитетом и доверием к источнику.

Внушение основано на слабой осознанности и низкой критичности восприятия сообщаемой информации, поэтому приемы внушающего воздействия рассчитаны на снижение активности понимания, развернутого логического анализа и оценки.

В настоящее время к основным приемам внушения, используемым в СМИ, относятся:

- Твердые заявления, преподносимые как факт. Подразумевается, что этот факт является очевидным и не требует дополнительных доказательств. Заявления могут быть как правдивыми, так и ложными.
- Оперирование сравнительными материалами для определения важности, тенденций и масштабности событий и явлений. Суждения при этом подбираются таким образом, чтобы заключение было очевидным.
- Подбор фактов, усиление или ослабление высказываний. Выводы не входят в текст приводимых сообщений. Их должны сделать те, кому предназначена информация. Для предоставления объекту воздействия возможности самостоятельно прийти к нужным выводам в сообщениях часто используется разносторонняя аргументация, освещаются, на первый взгляд, "без акцента", различные мнения, ненавязчиво выносятся суждения, якобы имеющие "объективный характер".

- Дробление и немедленность передачи материалов. Многочисленные не связанные друг с другом сообщения перечисляются подобно автоматической очереди. Ошибочно считать, что подобная практика является "чистым информированием" и не преследует вполне определенных целей. Разнородность передаваемого материала затрудняет оценку информации по ее значимости. Дробление информации облегчает подтасовку материала. При формировании сообщений используются действительные факты, которые связываются с другими, порой не имеющими никакого отношения к основному материалу сообщения. Известно, что даже достоверные сведения, также как и отдельные цитаты, вырванные из контекста, могут быть скомпонованы таким образом и поданы на таком фоне, что будут выражать идеи, совершенно отличные от тех, которые хотели выразить их авторы. Такая подача материала порождает у объекта внушения ощущение непрочности, зыбкости обстановки, собственной беззащитности и неуверенности.

- Дозировка отрицательных и положительных оценок. Для того, чтобы похвала выглядела более правдоподобной, к ней нужно добавить немного критики. Для того, чтобы суждение воспринималось, как достоверное, к нему добавляют некоторые положительные характеристики.

- Многократное повторение внушаемого информационного послания. Каждое внушаемое утверждение должно отвечать интеллектуальному уровню и эмоциональным предпочтениям групп людей, на которые предполагается оказывать воздействие. Зритель (слушатель, читатель) не должен задумываться над значением отдельных слов и правильностью формулировок. Психологический механизм многократного повторения основан на принудительной мобилизации внимания, подсознательном восприятии внедряемой информации и стереотипах восприятия (большинство людей склонны не задумываться над значением знакомых слов).

- Демонстрация позиции активного защитника интересов объекта воздействия. Это один из приемов консолидации недовольства. Формирование недовольства сопровождается внушением объекту воздействия чувства собственной нереализованности, ущемленности законных прав, лишения заслуженных привилегий и других чувств, характерных для "орального упрека".

- Подпороговая подача информации. Известно множество примеров использования техник подпороговых подрисовок в печатной рекламной продукции. Родственный прием в аудио СМИ - смена музыкальной темы в фонограмме в момент, когда в дикторском тексте подается материал, на который необходимо обратить внимание аудитории. Непроизвольная реакция слушателей на смену фона повышает пропускную способность также и смыслового канала.

Немалую роль играет момент подачи информации. Самые известные приемы - показ в наиболее (наименее) удобное для телезрителя время, а также выдача информации в совокупности (в блоке) с другой привлекательной или, наоборот, отвращающей информацией.

В последнее время многие авторы указывают на глобалистские устремления манипуляторов по унификации способов восприятия и реагирования больших масс людей (в перспективе всего человечества). Такие усилия уже приносят свои плоды - ведут к деиндивидуализации и деперсонификации людей, превращению их в податливых объектов манипулирования.

Приемы убеждения. В контексте практики манипулирования общественным сознанием, убедить в чем-либо объект воздействия означает не доказать истинность предлагаемой точки зрения или какого-либо утверждения, а добиться согласия с ними и сформировать готовность защищать их или действовать соответствующим образом. Модель "рационального невежества", заложенная в пропаганде, гласит: важно, чтобы люди думали, что полная достоверная информация им не нужна или, что она опасна, или что она слишком обременительна для них.

Убеждение основано на осознанном и критическом восприятии информации, поэтому в основу приемов убеждающего воздействия положен отбор, логическое упорядочивание фактов и выводов.

В практике манипулирования СМИ общественным сознанием утвердились следующие приемы убеждения:

- отбор и тенденциозное преподнесение только положительных или только отрицательных фактов, а также использование дезинформации и измышлений;
- преподнесение событий или вопросов, способных потенциально вызвать замешательство объекта воздействия и вынудить его эмоционально отреагировать;
- использование оскорбительных эпитетов и метафор, вызывающих негативное эмоциональное отношение, ассоциации с низкими поступками определенных лиц с целью опорочить поведение, подорвать авторитет, дискредитировать стиль руководства и т. п.;
- эксплуатация сакральных для народа понятий и чувств ("патриотизм", "независимость", "свобода", "человеческое достоинство" и т. п.);
- подмена значений (например, искусственное распространение авторитета и престижа того, что ценится и уважается в данной культуре на то, что выгодно манипулятору);
- эксплуатация мнения авторитетных лиц, приведение их высказываний, зачастую вырванных из контекста, в качестве аргументации для навязываемых утверждений;
- подбор фраз, требующих единообразия в поведении, создающих впечатление, будто так делают все (например: "Все нормальные люди понимают, что ...", "Ни один здравомыслящий человек не станет отрицать, что ...");
- сообщение нескольких точек зрения по данному вопросу, но так, чтобы незаметно представить в выгодном свете нужную (создание иллюзии независимого выбора);
- замалчивание, то есть проявление безразличия к какой-либо информации (событию) и, тем самым, косвенное умаление ее значения;
- полуправда - предъявление только части правды, при одновременном утверждении, что это "вся правда", касающаяся данной проблемы;
- карикатуризация, то есть подмена одного названия или образа другим, которое имеет негативную нагрузку и способно вызвать сильную эмоциональную реакцию;
- поддержка и усиление предрассудков (например, возбуждение и поддержание негативного отношения к различным группам людей (представителям различных регионов, национальностей, профессий и т. п.));
- откровенная ложь ради достижения кратковременных целей. Сопровождение лживых фактов мельчайшими подробностями, деталями создает видимость правды. Перемешивание лживых фактов с правдивыми создает дополнительную иллюзию правды и дезориентирует объект воздействия;
- намек или дискредитация в скрытой форме: нужный эффект достигается тем, что человек упоминается рядом с осуждаемыми людьми или дис-

кредитирующими фактами; сообщаемые сведения маскируются слухами, непроверенными данными;

- подмена рационально-логических подходов, рассуждений эмоциональными отношениями с целью создать стереотипы для отрицательного отношения. Отражение действительности в ярких, но заведомо деформированных словесных образах, создает извращенное представление о событиях. Стереотипы сводят ситуацию, образ мышления или отношение к штампам, по поводу которых не возникает вопросов, нет необходимости размышлять. Например, продолжительное и многоканальное разъяснение каких-либо событий только с определенных позиций. Одни стереотипы могут быть направлены на то, чтобы дискредитировать какие-то события, проблемы, другие - отвлечь внимание от конкретных реальностей, скрыть их, перевести внимание объекта воздействия в абстрактную, обобщенную сферу памяти.

Способы противодействия манипулированию массовым сознанием в СМИ. Эффективность противодействия практике психологического манипулирования массовым сознанием в СМИ будет выше, если осуществлять его с учетом следующих психологических рекомендаций:

- Необходимо правильно понять и оценить замысел политтехнологов, реализующих тот или иной сценарий психологического воздействия в СМИ.
- Следует "прочесть" символику психологической операции в языке (дискурсе) ее организаторов.
- Необходимо постоянно следить за изменениями ситуации, связанными с технологией психологического воздействия. Особо следует обращать внимание на следующие явления:

1) дисбаланс в распределении ответственности;
2) деформации в соотношении выигрыш - плата;
3) силовое давление;
4) нарушения сбалансированности элементов ситуации;
5) необычность мишеней воздействия;
6) необычность компоновки и подачи информации;
7) неконгруэнтность в поведении трансляторов информации;
8) стереотипизация поведения потребителей информации.

- Необходимо проводить непрерывный мониторинг характера и механизмов манипулятивного воздействия, фиксирующий:

9) ненормативно частое появление психических автоматизмов в поведении потребителей информации (адресатов воздействия);
10) регресс потребителей информации к инфантильным реакциям - воскрешение неутоленных детских потребностей (в заботе, любви, поддержке, желания что-то выиграть, получить в подарок), детских форм поведения (плача, желания кривляться, нежиться, "строить глазки", выпраши-

вать), а также мучительных чувств (неадекватной агрессии, тоски, тотального чувства одиночества);

11) появление дефицита времени, отпущенного на принятие решения;

12) состояние суженности сознания;

14) синхронность изменений тональности источника информации и психологических реакций потребителей информации.

Оценка степени уязвимости населения информационно-символическому манипулированию может включать:

1) учет национально-культурных особенностей населения данного региона;

2) анализ социально-исторического контекста, включающий раскрытие таких его компонент, как цивилизационная идентификация народа, темы основных исторических противостояний на данной территории, а также характер базовой культурно-исторической травмы исследуемого народа;

3) изучение социально-экономической и социально-политической ситуации в стране, степени удовлетворенности основной массы населения своим социальным и экономическим статусом;

4) анализ состояния общей и психологической культуры в стране (регионе).

Стратегия нейтрализации деструктивных замыслов политтехнологов разрабатывается с максимальным учетом специфики психологического воздействия манипуляторов в данной конкретной ситуации. К числу общих принципов психологического противодействия активности манипуляторов в СМИ относятся следующие:

1) не атаковать без необходимости первым. Позволить нападающей стороне как можно полнее раскрыть свои намерения. Энергию психологической атаки использовать для разрушения этой же атаки;

2) разрушая сценарий психологической операции, дать противостоящей стороне понять, что продолжение операции перестало быть выгодным для нее;

3) найти конструктивную основу в замыслах противоборствующей стороны и заявить о готовности сотрудничать с ней в этой сфере. При этом должны решительно вскрываться и нейтрализоваться деструктивные элементы в действия другой стороны;

4) особый упор при столкновении с манипуляцией нужно делать на придании огласки враждебных действий противоборствующей стороны;

5) при соприкосновении с тонкими видами манипулирования массой (духовным и символическим манипулированием) необходим развернутый анализ задействованных глубинных семантических связей, с целью создания целостной картины манипулятивного воздействия.

Рост влияния и значимости информационной составляющей общества, а также психологических и технических возможностей для манипулирования

массовым сознанием требуют перехода от реагирующей к принципиально иной – прогностической, опережающей модели информационного обеспечения. Такая модель должна предусматривать эффективную защиту от непрерывно совершенствующихся технологий информационно-психологического воздействия, а также удовлетворять растущую потребность общества в получении необходимого объема полезной и качественной информации [216; 218; 264-273].

2.7. Самоцензура-самообман-самоманіпуляція ...

Дослідити взаємозв'язок таких понять, а відповідно і соціально-психологічних явищ як "*цензура*", "*обман*" та "*маніпуляція*", нас спонукають саме питання інформаційної безпеки. На погляд автора, вони мають спільне коріння, походження, а результати їх "діяльності" мають однаково негативні наслідки як для окремої особи, професійного товариства, так і для суспільства в цілому. Одразу хотілося б зазначити, що названі явища існували, існують і, переконаний, будуть існувати, оскільки тісно пов'язані із природою людини, її психологічною будовою, життєвими інтересами. Присутність цих явищ у житті суспільства притаманне як нашому постіндустріальному світові, так і китайському суспільству дві тисячі років тому чи Європі епохи Відродження.

Поняття маніпуляція нині достатньо популярне серед науковців і практиків різних напрямів. Літератури з цього питання написано чимало. Та все ж визначимо її коло, щоб було зрозумілим, чим нас привабило це поняття, які його грані чи наповнення можуть бути використані у процесі практичної діяльності у сфері засобів масової інформації. Головною метою цієї роботи є прагнення провести паралель між поняттями "самоцензура" та "самоманіпуляції", вказати на згубність цих явищ на діяльність людини у такій важливій суспільній сфері як журналістика, а по дотичній і у таких сферах як громадська і політична діяльність.

Найчастіше дослідники цього явища сходяться на тому, що поняття "*маніпулювання*" походить від латинського терміну "*manipulare*", що має цілком позитивне значення - "*управляти*", "*керувати зі знанням справи*", "*надавати допомогу*" [274]. Власне корінь слова "*маніпуляція*" походить від латинського "*manus*" – рука. У словниках сучасних європейських мов це слово найчастіше тлумачиться як дія, спрямована на об'єкти з певними намірами, метою, наприклад, ручне керування засобом пересування, огляд пацієнта лікарем за допомогою рук, здійснення деяких операцій на виробництві чи під час наукових експериментів. Тому переносне значення цього слова у мовній практиці європейця може ще означати - спритне поводження з людьми як із неживими об'єктами чи речами. Сучасний Оксфордський словник англійської мови трактує "маніпуляцію" як "акт впливу на людей або ке-

рування ними зі спритністю, особливо із зневажливим підтекстом, як приховане керування або вплив".

У сучасній науковій літературі під "маніпуляцією" ще часто розуміють мистецтво управління великою кількістю людей з допомогою цілеспрямованого впливу на суспільну психологію, на свідомість та інстинкти людини. Найчастіше у цьому зв'язку дослідники наводять слова німецького соціолога Герберта Франке. Він під маніпулюванням розуміє *"своєрідний психологічний вплив, котрий чиниться таємно..."*. Г. Франке наводить найпростіший приклад такого впливу, як не дивно – це всім відома реклама. Німецькому вченому після чергового перегляду рекламного блоку на одному із телеканалів здалося, що цілком простенька на перший погляд реклама є вже й не такою примітивною. Г. Франке помітив, що від улесливого, вимогливого та благаючого голосу реклами виходить м'який, спокійний тиск, який буває тим ефективнішим, чим ці характеристики менш помітні. Це не тільки спонукає людину, яка перебуває під таким впливом, чинити так, як того бажають інші, але примушує його бажати чинити саме так.

Професор Д. Елвайн пропонує дещо інше бачення цього поняття, формулює його зміст таким чином: "Управління людиною, що здійснюється чи то внаслідок так званого примусу речей, чи то внаслідок організованих класових інтересів, чи то внаслідок відповідної економічної структури... Духовне управління людиною, зумовлене впливом ірраціональних чи емоційних засобів і аргументів: у політиці – звернення до нації, любові до вітчизни, до крові, раси, честі" [274].

Як бачимо, ці автори схиляються до того, що під маніпулюванням слід розуміти специфічну форму духовного впливу, який виявляє себе у формі прихованого, анонімного панування, що здійснюється ненасильницьким чином (Б. Бесонов). Та навряд чи можна погодитися із цим визначенням, хоча воно й звертається до такої безмежної й захоплюючої сфери людського буття, як духовність.

Наведене вище визначення вказує нам лише на одну характеристику маніпуляції: на її прихований, анонімний характер, на її непомітну суть та підступну дію. Коли ж ми говоримо про використання маніпуляційних технологій, чи то протидію їхню, нам важливіше знати, хто здійснює маніпулювання, на кого спрямована дія, яка мета спонукала вдатися до цієї психологічної зброї. З часом маніпуляція набула типових ознак соціальної технології у арсеналі управління і впливу на суспільство з боку урядів розвинених держав, оскільки саме для таких країн все гостріше поставало питання про розробку новітніх засобів керування як окремими особистостями, так і великими групами людей. Найбільше у цьому напрямі просунулися США, як свідчать дослідники із цієї ж країни. На дослідження і розвиток цих технологій працював і досі працює чисельний загін інтелектуалів, учених і навіть військових експертів. Відомий американський фахівець, котрий завжди вирізнявся своєю непримиренно критичною позицією щодо суспільної політики власного уряду,

Г. Шіллер наголошує: «Там, де маніпуляція є основним засобом соціального контролю, як, наприклад у Сполучених Штатах, розробка і вдосконалення методів маніпулювання цінуються набагато більше, ніж решта видів інтелектуальної діяльності" [275]. Коли цей автор у своїй скандальній книзі розвінчував п'ять міфів західного суспільства, він називав найбільшим успіхом маніпуляції, котрий добре простежується на прикладі Сполучених Штатів, вдале використання особливих умов західного розвитку для увічнення як єдино правильного визначення свободи мовою філософії індивідуалізму.

Можна цілком упевнено твердити, що у справі маніпуляції фахівці із США досягли досконалості. Ще один американський вчений, котрий у своїй урядовій критиці не відстає від згадуваного вище колеги, Н. Чомський у роботі "Необхідні ілюзії: контроль над свідомістю у демократичних суспільствах" наголошує, що "протягом 80-х років урядам Рейгана й Буша у США вдавалося провадити цілком праву соціальну та мілітаристичну політику навіть за обставин, коли у суспільній думці простежувався сильний зсув у бік соціал-демократичних принципів" [276]. Під час опитування того періоду переважна більшість американців підтримала введення державних гарантій повної зайнятості, державне медичне обслуговування та будівництво дитячих садків, а співвідношення прихильників і супротивників військових витрат у період підготовки до операції "*Буря в пустелі*" складало 3:1. Майже половина населення США була упевнена, що фраза "від кожного за здібностями, кожному за потребами" – стаття із Конституції США, а не гасло із "*Комуністичного маніфесту*" Маркса".

Однак маніпуляція, як з'ясовується, не ноу-хау сучасних макіавеллі чи суслових. Вище вже зазначалося, що маніпуляція як метод впливу "*живе*" серед людей від часу, коли людство вибудувало основи суспільного життя. Для людини маніпулювати і бути під впливом маніпуляції – є проявом інстинктивної потреби у стабільності навколишнього світу й прагнення пояснити все, виходячи із самого себе. Прикладом цьому можна назвати магічні культи старовини, появу релігій, діяльність шаманів та всіляких знахарів.

Феномен маніпуляції привертав увагу дослідників і практиків різних епох. У Китаї багато віків тому було створено своєрідний банк даних, де об'єднано й класифіковано у формі метафоричних схем метод маніпуляційного впливу і розроблено методичний підхід щодо їх використання у різних ситуаціях. Цей твір отримав назву "*Трактат про 36 стратагем*". Як зазначає дослідник маніпулятивних технологій В. Крисько, власне поняття "*стратагема*" означає стратегічний план, у якому для супротивника криється якась пастка чи хитрість [277]. Розглядаючи семантику зазначеного поняття, В. Мясников звертає увагу на те, що у китайській мові воно означає такий синонімічний ряд як винахідливість, багатоманітність тощо.

У найбільш точному вигляді, у лаконічній і метафоричній формі уперше маніпулятивний підхід описано близько двох з половиною тисяч років тому в "Трактаті про військове мистецтво", автором якого, як вважають дослідники,

є видатний китайський полководець і державний діяч, котрий увійшов в історію під іменем Сунь-цзи. Нині дослідники припускають, що під літературно-філософським псевдонімом Сунь-цзи виступав видатний полководець-"стратагемщик" Сунь Бинь, котрий жив у IV столітті до н. є. [278].

На теренах Європи також здавна цікавилися цією проблемою. Опис прийомів маніпулятивного впливу на людей у процесі їх взаємодії досліджував у античні часи Аристотель (*"Про софістичні спростування"*). Існував напрямок у тодішній науці, який отримав назву софістика. Широкому загалу відомі роботи Н. Макіавеллі, А.Шопенгауера, зокрема, у його роботі *"Еристична діалектика"* перераховується 36 риторичних стратагем, чи то прийомів. У Росії 1918 року вийшла друком робота С.Пивоварніна "Суперечка. Про теорію та практику суперечок", де з критичних позицій аналізуються методи маніпулювання та їх використання у різних ситуаціях обговорень та публічних дискусій. А хто не знайомий із книгами Д. Карнегі, де у популярній формі розповідається про чисельні прийоми міжособистісних контактів, серед яких є й приклади психологічної маніпуляції [279-281].

Та особливий інтерес у зв'язку із заявленою проблемою статті можуть мати для нас навіть не стільки зауваження наших сучасників як то Г.Шіллера чи В.Крисько, а дослідження особливостей індивідуальних, групових і масових психологічних явищ у періоди соціальних криз, що їх здійснив у 30-ті роки минулого століття видатний психолог Е. Фромм. Зрозуміло, чому результати цих досліджень сьогодні також привернули нашу увагу як теоретичний матеріал для аналізу нинішнього стану з маніпулятивним впливом у галузі масової комунікації, зокрема у ЗМІ. Не будемо зупинятися на обгрунтуванні того, що період суспільних трансформацій, які ось вже тривалий час переживає наша країна, має всі ознаки кризи. У результаті аналізу Е.Фромм виявив закономірні історичні аналогії в особливостях психологічної поведінки людей у періоди кризових суспільних змін. Учений порівняв сучасні йому реалії (*"велика депресія"*) з періодом епохи Відродження та Реформації, оскільки саме у ці періоди низка країн Західної Європи переживали перехід до якісно нових суспільних форм життя громадян, ламалися старі й формувалися нові економічні структури, соціальні інститути і суспільні відносини, різко модифікувалася державна ідеологія, а відповідно індивідуальна та суспільна психологія. Справді, як описана картина відповідає сьогоднішньому стану України! Так одразу й задумаєшся, що дійсно суспільний розвиток відбувається по *"спіралі Маркса"*.

Розглядаючи епоху Відродження і відзначаючи її прогресивний характер, Е.Фромм разом з тим змальовує, як у той час виявив себе маніпулятивний підхід у взаємодії між людьми. Наскільки глибоко він вразив і вищі верстви населення, і низи суспільства. Власне перехід до епохи відродження та її розквіт були пов'язані з втратою *"середньовічних оков"* і переходом до нових форм взаємодії між людьми, серед яких з особливою силою виявила себе психологічна маніпуляція, або просто маніпулятивні технології того часового

рівня. Учений пише: "Відродження було культурою багатого й сильного класу, який виявися на гребні хвилі, що її здійняв шторм нових економічних сил. Простий люд, якому не дісталося ні нового багатства, ні нової влади перетворився у безлику масу, що втратила упевненість свого попереднього стану. Цій масі лестили або погрожували, але можновладці завжди маніпулювали нею чи експлуатували її" [282].

Геніальність Е.Фромма тут виявилася у тому, що, пишучи про події кількавікової давнини для читачів першої третини минулого століття, він ніби відтворює картину сьогодення і вже оцінює з завидною влучністю суть теперішнього життя, принаймні у нашій країні. І далі: "Відродження (так і хочеться сказати "*період реформування незалежної держави*" - С.Д.) було культурою не дрібних торговців чи ремісників, а багатих аристократів і бюргерів. Їх економічна діяльність, їх багатство давали їм відчуття свободи й відчуття індивідуальності. Проте і вони також зазнали втрат: вони втратили ту упевненість та відчуття приналежності, яку забезпечувала їх середньовічна соціальна структура. Вони стали більш вільними, але водночас і більш одинокими. Вони користувалися своєю владою і багатством, щоб вичавити із життя всі радощі до останньої краплини, але при цьому їм доводилося використовувати всі засоби, від психологічних маніпуляцій до фізичних тортур, щоб управляти людом і стримувати конкурентів серед свого клану" [283].

Для ученого цілком зрозуміло, що всі людські відносини були сплюндровані й отруєні цією смертельною боротьбою за збереження влади й багатства. Солідарність із побратимами, чи принаймні із членами свого клану, змінилася цинічним відособленням; інші люди розглядалися як "об'єкти" використання й маніпуляцій, або безжально знищувалися, якщо такий крок сприяв досягненню власних цілей. Індивід був охоплений пристрасним егоцентризмом, ненаситною жадобою багатства та влади. Як наслідок, було сплюндровано і відношення успішного індивіду до власної особистості, руйнувалося його відчуття упевненості в собі та безпеки. Він сам перетворювався у такий же об'єкт маніпуляцій, у який раніше перетворилися всі решта. Тема, яка цікавить нас у цьому дослідженні, пролунала з уст відомого вченого. Це дає всі підстави сумніватися, що повноправні господарі капіталізму епохи відродження були не так вже й щасливі й упевнені у собі, як то часто зображає їх мистецтво того часу. Мабуть, нова свобода принесла їм не тільки могутнє почуття сили, але й загрозливу ізоляцію, сумніви, скептицизм і, як результат всього цього, тривогу.

У більшості сучасні дослідники маніпулятивних впливів вбачають у цьому понятті механізм прихованого психологічного примусу. У науковій і популярній літературі останнього десятиліття це поняття набуло два основних значення – прямого й переносного чи метафоричного. У переносному значенні, зауважує В.Крисько, воно має достатньо широку диференціацію, тобто можна говорити про систему понять, для яких маніпуляція є родовим. До системи цих понять відносимо: маніпулювання (зокрема, маніпулювання у політиці, маніпулювання

громадською думкою, громадською свідомістю), міжособистісні маніпуляції, соціально-політичні маніпуляції особою. Під час огляду змісту поняття "маніпуляція" виокремлюються основні ознаки, а вже на їх основі визначаються загальні критерії, що дозволяють сформулювати робочі поняття.

Чи не найбільш повно мереживо критеріїв для визначення поняття "маніпуляція" подано у роботах Є. Доценко [162]. Серед них:

- родова ознака-психологічний вплив;
- ставлення до об'єкта маніпуляції як засобу досягнення власних цілей;
- прагнення отримати односторонній виграш;
- прихований характер впливу (як самого факту впливу, так і його спрямованості);
- використання психологічної сили, гра на слабкостях людини (використання психологічної вразливості);
- спонукання, мотивування (формування "штучних" потреб і мотивів для зміни поведінки в інтересах ініціатора маніпулятивного впливу);
- майстерність та вишкіл у здійсненні маніпулятивної дії.

Додамо, що слід розрізняти прості "одноактні" маніпуляції або окремі акти маніпулятивного впливу, а також складні, які можна умовно позначити як маніпулятивні ігри. Словом, процес маніпуляції може бути поширеним у часі і побудований як багатоступінчата поетапна процедура здійснення маніпулятивного впливу на людину. Цей процес може бути відносно простим, що передбачає одноактний період спілкування із використанням одного або кількох прийомів маніпулятивного впливу, чи то структурно достатньо складним, тобто включати комплекс різноманітних маніпулятивних заходів, дії яких спрямовано на різні психологічні структури особистості, використання різних психологічних механізмів з поетапною реалізацією цих прийомів у певні проміжки часу та у різних ситуаціях взаємодії. Таким чином, складна маніпуляція має свою складну часову, просторову та організаційно-соціальну структуру.

Така історична й теоретична база, яка, на наш погляд, цілком достатня для того, аби довести головну думку цієї розвідки. А саме, що маніпулятивний вплив на ЗМІ є складовою впливу на громадську свідомість, психологію окремого індивіда, а разом з тим руйнує через агресивну природу маніпуляції психологію журналіста та його самоусвідомлення як незалежної особистості, на яку професія покладає особливу соціальну відповідальність. Крім того, цей стан речей, за який несе відповідальність перед суспільством еліта країни, є одним із загроз національній безпеці. Оскільки руйнує психологічне здоров'я суспільства, ставить під загрозу існування в державі принципу свободи слова та професії журналіста.

На державному рівні цілком сформованим є усвідомлення того, що маніпулювання є загрозливим явищем у масштабах країни. У проекті Концепції національної інформаційної політики, що розроблена Державним комітетом інформаційної політики, телебачення й радіомовлення України, за-

значається, що маніпулювання громадською свідомістю є однією із основних загроз інформаційній безпеці держави [283]. При цьому не уточнюється, звідки буде ця загроза надходити: чи то ззовні, чи то зсередини. На наш погляд, це не має особливого значення, оскільки головною діючою субстанцією маніпуляції є інформація, а вона, як відомо, сьогодні майже не знає меж і кордонів. З одного боку, як зазначає німецький дослідник К.Герман "необмежений потік інформації ускладнює маніпулювання людьми та їх думками з боку властей і одночасно сприяє самовиявленню індивіда у відкритому суспільстві" [284], а з іншого боку, саме ЗМІ несуть найбільше навантаження щодо поширення інформації, а отже є "універсальним каналом масоутворення, ... без якого не може обійтися жодна із ... діючих сьогодні маніпулятивних традицій" [285].

Журналіст В. Кіпіані зробив для себе такий висновок, що "найближчих родичів респектабельного піару звуть Провокація, Маніпуляція та Фальсифікація" [286]. Цей автор багато писав про приклади маніпуляції українського ґатунку, який дістав назву "темники". Хоча український досвід тут значно поступається світовим лідерам у мистецтві маніпуляції. Прикладом успішного використання маніпуляції масовою свідомістю шляхом ЗМІ називають розгорнуту США інформаційну кампанію щодо запровадження стратегічної оборонної ініціативи (СОІ). Це сталося за часів президента Р.Рейгана й відбувалося у рамках інформаційної війни двох наддержав - Радянського Союзу та Сполучених Штатів. У 1993 році газета "Нью-Йорк Таймс" поінформувала своїх читачів про те, що американській адміністрації ціною титанічних зусиль вдалося проштовхнути 1984 року "дезу", аби обманути керівництво Радянського Союзу щодо високої ефективності нової протиракетної системи. Спеціалісти Пентагону та ЦРУ із інформаційних кампаній (читай маніпуляцій) сфальсифікували результати наукових випробувань і підтасували різні дані для того, щоб примусити СРСР повірити у серйозність загрози, а отже втягнули Країну Рад у новий виток гонки озброєнь. Це й без того знекровлювало втягнену у афганську війну радянську державу. Хоча й остання достатньо часто й успішно використовувала інформаційну зброю проти свого ідеологічного супротивника. Згадати хоча б сфабриковану контрпропагандистськими органами Радянського Союзу "правдиву" інформацію, буцімто ЦРУ винне у появі СНІДу. Суть інформації, на якій будувалася подальша маніпуляція масовою свідомістю, полягала у тому, що американська розвідка випадково поширила вірус із секретної лабораторії у штаті Мериленд.

Крім того, ми мали можливість спостерігати за вправністю американських спеціалістів із маніпулятивних технологій, коли вони на замовлення уряду прагнули переконати якщо не весь світ, то хоча б власний народ у необхідності військової операції в Іраці. Варто зазначити, що робили це вони вправно. Чого варті лише ролики про необхідність запасатися продуктами харчування та засобами індивідуального захисту на випадок терористичних акцій. Американці, які складно, попри навіть 11 вересня, уявляють жахи

війни (хіба що в кінообразах), оскільки у їхній національній соціальній пам'яті це не могло позначитися, масово скуповували харчі та медикаменти. Отож, маніпуляція цього разу мала не лише соціально-політичний чи міжнародний ефект, але й була цілком пристойним маркетинговим заходом — були розкуплені усі застарілі запаси медичних препаратів та туалетного паперу.

Як наслідок маніпулятивного впливу ми спостерігаємо своєрідну "активну пасивність", яка виявляє себе у безапеляційному виконанні чиєїсь волі, нав'язаної не фізичним впливом, а поширенням у ЗМІ певної інформації. Цей висновок перегукується з твердженням того ж Г. Шіллера про те, що "пасивність — кінцева мета маніпулювання свідомістю". Вчений критично зауважує, що зміст і форма засобів масової інформації Америки — міфи та засоби їх поширення — повністю базуються на маніпуляції. У разі її успішного використання, у чому Г.Шіллер ніколи не сумнівався, вони неминуче спричинюють пасивність індивіда, інертність його стану, що унеможливлює усвідомлену дію. Саме такого стану, робить висновок вчений, прагнуть досягти засоби масової інформації і вся система загалом, оскільки пасивність гарантує збереження статус-кво ініціаторів маніпуляції [287]. Саме цей дослідник прагне наштовхнути нас на думку про те, що найважливішою обставиною і характеристикою маніпуляції є те, що, преса, радіо чи телебачення, пропонуючи слухачам і читачам висловити публічно свою думку, створюють лише ілюзію незалежності, об'єктивності та можливості власного вибору із різних точок зору і опори на думку аудиторії.

Та повернемося до ще одного аспекту заявленої проблеми, що його планувалося розглянути у цій статті. Суть його полягає у тому, що маніпуляція є згубним і небезпечним явищем не лише для тих, хто є об'єктом її впливу, але й для того, хто її ініціює з тієї чи іншої причини. Про причини ми вже говорили, коли цитували роботу Є.Доценко "Психологія маніпуляції". Не можна не погодитися з тим, що, апелюючи до ниць мотивів, маніпулятор мимоволі підіймає їх значущість власне для себе, зокрема, сприймає як дещо важливе та корисне. Деформація або затримка власного соціального й особистісного розвитку для маніпулятора загрожує йому не меншими втратами, ніж для адресату, оскільки у цьому випадку він не жертва, яка може ще й протистояти впливові, а, власне, "сам того бажає". Маніпулятор, особливо якщо він проводить свої операції достатньо вдало, звужує свій арсенал досягнення цілей, зупиняє свій пошук і розвиток, тому згодом йому все складніше вирватися із ним же протоптаної "колії".

На певному етапі маніпулятор починає ніби внутрішньо роздвоюватися, виникає суперечність і антагонізм між поглядами, моральними принципами та необхідністю діяти маніпулятивними засобами. У такий спосіб проявляється так званий *"вроджений гріх"* маніпуляції — руйнівний вплив на особистість людини. Що стосується співробітника ЗМІ, то він, на наш погляд, перебуває у ще складнішій ситуації. Журналіст у маніпулятивних технологіях виступає і як ініціатор маніпуляції, і як її об'єкт. Адже ніхто не буде заперечувати, що у

журналіста немає особистісних причини повсякчас вдаватися до такого методу психологічного тиску чи соціально-культурного управління. Скоріше за все він отримує відповідні завдання, тобто сам спочатку потрапляє на місце жертви. А вже згодом йому доводиться використовувати весь наявний творчий потенціал (як би цинічно не звучало), щоб з його допомогою маніпулювати іншими, виконуючи "*редакційне завдання*" чи дотримуючись умов документа під назвою "*редакційна політика*".

Це перший етап руйнування особистісного "Я" журналіста чи будь-якого іншого працівника ЗМІ. Другий наступає тоді, коли він усвідомлює своє подвійне використання. Це справжній момент істини, коли доводиться приймати рішення, шукати виправдань, або погоджуватися на самоцензуру й самообман. Саме через це час від часу виникають конфлікти між власниками ЗМІ та творчими журналістськими колективами чи окремими працівниками. Однак більшість все ж погоджується на самообман. Одне з анкетних анонімних опитувань засвідчило, що представники державних засобів масової інформації "постійно" самоцензурують (42 % проти 26 % у недержавних ЗМІ), "інколи" самоцензурують, навпаки, 30 % представників державних ЗМІ і 52 % представників недержавних [288]. На наш погляд, самоцензуру можна розглядати як форму самоманіпуляції, згубна сутність якої від цього не зменшується.

І цьому можна знайти пояснення. Це питання слід розглядати у площині дослідження проблеми, яка у спеціальній літературі з психології отримала назву "*мішені маніпулятивного впливу*". Так, зазначається, що впливи такого роду будуються на ниць потребах людини або його агресивних нахилах. Такими прийнято вважати, наприклад, брутальний секс, почуття власності, вороже ставлення до інакомислячих чи відмінних від загалу людей, природна людська слабкість перед спокусою владою, грішми, славою, розкішшю тощо. Дослідники наголошують, що, як правило, маніпулятори експлуатують потяги, які мають діяти безвідмовно: потреба у безпеці, у їжі, у товаристві.

Універсальними психологічними мішенями для маніпуляторів є гордість, прагнення індивіда до задоволення різного роду, комфортного життя, а також бажання мати сімейний затишок, просуватися по службі (кар'єрний ріст), бути популярним. Хоча журналістське й загалом творче середовище складається із людей освічених, що часто претендують на звання духовної еліти суспільства, однак вивчення специфічних потреб цієї соціальної верстви, суперечності та внутрішня боротьба у цьому колі — краща мішень для мисливців на їх душі й розум. Важливо лише визначити пріоритети, актуалізувати потреби, підкинути нові суперечливі ідеї. Далі це середовище саме буде їх плекати, готуючись до самоманіпуляції, щоб на якомусь етапі вже бути цілком залежним і готовим ретранслювати маніпуляцію назовні, відгородившись від світу пеленою самообману. Висловлюючись мовою психології, замовники маніпуляцій прагнуть регресу спочатку у продуцентів інформації у напрямі інфантильних реакцій на зразок нереалізованих дитячих фантазій і

потреб — в любові, турботі, бажанні мати щось особливе, отримати винагороду чи подарунки до свят, потішити власні творчі амбіції.

Згодом у журналістів простежуються дитячі форми поведінки — бажання ніжитися (літати літаками еліти чи можновладців, відпочивати у тих же санаторіях, що і "сильні світу цього"), кривлятися (участь у ток-шоу, висвітлення поїздок знаних осіб, що претендують на звання еліти, а є скоріше квазіелітою, котра сама провокує й сплачує маніпулювання), випрошувати щось приємне (подарунки від можновладців, нові посади та знову ж таки квазізвання у так званих рейтингових акціях). Коли працівники ЗМІК відчувають власний психологічний регрес як наслідок маніпулятивного впливу, виникають руйнівні інфантильні почуття — неадекватна реакція, сум, тотальне почуття самотності, безвиході. Особиста трагедія засновника інформаційної агенції "Українські новини" є жорстоким підтвердженням цих цілком наукових припущень. Журналісти більше ніж інша професійна група піддається впливу маніпулятивних технологій, оскільки жодна із існуючих сьогодні маніпулятивних традицій, за свідченням науковців, не може обійтися без розробки і тиражування спеціальних інформаційних, іміджевих, пропагандистських чи рекламних матеріалів, для масового поширення яких потрібні у першу чергу канали ЗМІК. Через це працівники ЗМІК, хоча й таврують у своїх виступах некоректні форми політичної чи економічної боротьби національної еліти, та вкрай боляче і неохоче відмовляються від привитої їм інфантильності. Вони страждають, морально деградують, розглядають світ у чорно-білих кольорах, але не можуть вийти із зачарованого кола вже самоманіпуляції. У такій ситуації самоцензура стає необхідною умовою їх творчої діяльності. Людина опускається від вершини до підніжжя "*піраміди потреб А. Маслоу*", залишивши як непотріб потребу в творчості, самоактуалізації та самореалізації. Далі не варто аналізувати, який наслідок це має для всього суспільства. Водночас ті, хто не зрадив власним аутентичним життєвим цілям та принципам, журналістським середовищем виштовхується на маргінальне поле існування. Минула й сучасна історія вітчизняних засобів масової інформації знає багато таких імен.

З іншого боку ті, на чиє замовлення розробляється і готується маніпулятивна стратегія, добре усвідомлюють роль ЗМІК у реалізації своїх планів. Звернімося знову до досвіду США, оскільки український тут не такий ефектний, хоча не менш ефективний. Отож, один із президентів Сполучених Штатів Р. Ніксон якось підмітив, що успіх президентства полягає в умінні маніпулювати пресою. Та досвідчений політик миттю зауважує, що не дай вам Бог продемонструвати пресі, що ви нею маніпулюєте. Свого лідера підтримали колеги-журналісти. Фахівці Інформаційного агентства Сполучених Штатів додали: "Нам краще обробити одного журналіста, ніж десять домогосподарок. Ми працюємо не з людьми, а з каналами". Працівник ЗМІК тут виступає як "*лідер думки*". Це вже досить зручно для маніпулювання і помітно посилює ефективність діяльності маніпуляторів. Оскільки за твердженням фахівців,

число лідерів думок складає від 10 до 20 відсотків населення, куди ми відносимо, безперечно, й журналістів. Але маніпулювання чи, принаймні, вплив на частину цієї групи дозволяє поширювати далі свій вплив з найменшими матеріальними та інтелектуальними витратами.

Пропагандистська та маніпулятивна функції засобів масової інформації приваблюють еліти до цього суспільного феномену особливого засобу впливу на нееліту. Послуговуючись ЗМІ нові еліти декларують свої претензії на політичні та економічні права [289]. Для втілення своїх задумів вони найчастіше використовують владу у різних її формах. Цитований нами Е. Фромм із цього приводу зазначає, що ті, хто володіє символами влади і прагне мати з цього вигоду, мають перш за все придушити здатність до реалістичного, критичного мислення у підлеглих і примусити їх вірити у вигадки. "Кожному відомі махінації пропаганди і методи, за допомогою яких придушується критичне мислення, – волає до світу учений-гуманіст. – Відомо, яким покірним і керованим стає розум, поглинутий шаблонними фразами, і якими німими стають люди, втрачаючи незалежність, здатність вірити лише власним очам і покладатися лише на власну думку. Захопившись вигадками, вони більше не сприймають дійсність у її істинній суті [290]. Це можна назвати механізмом психологічної руйнації.

Психологи дають загалом невтішні прогнози щодо використання у майбутньому психо-маніпулятивних технологій, оскільки "*суспільство саме створює необхідні умови для маніпуляції*", бо "*людству для розвитку потрібні відповідальні натури*". Це їх "обраних (і недоторканних) навантажують відповідальністю за всіх, наділяючи владою, дозволяючи їм ставити цілі й пропонуючи себе у якості засобів здійснення задуму лідерів чи лідера" [162].

Журналісти також частина суспільства, не так часто вони потрапляють до "*обраних і недоторканних*", а отже вони також пропонують себе у якості засобів здійснення задуму лідерів, частіше політичних чи громадських діячів. Тут починають діяти психологічні механізми, які керують нашими думками та вчинками, однак часто залишаються незрозумілими. У цьому зв'язку приходить на думку відомий експеримент, описаний у багатьох наукових виданнях та навіть журналістських матеріалах, що його здійснив західний психолог Мілграм. Як це традиційно буває, він знаходив серед вулиці випадкових людей, які за невелику платню зголошувалися взяти участь у нескладному на перший погляд дослідженні. Все, що вимагалося від таких добровольців в ім'я науки, так це зіграти роль вимогливого "*учителя*" – зачитувати на прохання вченого завдання "*учневі*" й оцінювати його відповіді. Хто в житті не виконував таку роль? У разі неправильної відповіді необхідно було натискати на кнопку, наказуючи "учня" розрядом електричного струму. Сила електричного удару з кожною наступною неправильною відповіддю збільшувалася на *15 W*. Перед "учителем", аби йому було все зрозуміло й він відповідав за свої дії, встановлювалася приборна дошка із шкалою, на якій вказувалося і напруга, і

рівень її безпеки для "учня". А саме: 15 — 60 W - "легкий шок", 195 - 240 W - "*сильний шок*" і так аж до того рівня, що загрожує життю людини. "*Учня*" розміщували за склом так, щоб піддослідний "учитель" між спостерігати за ним і чув свого "підлеглого". Перед тим, як власне розпочинався експеримент, "*учителю*" давали спробувати на собі невеликий розряд у 60 W. Цього було цілком достатньо для "легкого шоку" та відчуття болю й страху. Далі на очах в "учителя" до усміхненого й довірливого "учня", а його, зрозуміло, грав професійний актор, підключали електроди і змазували тіло у місцях дотику зубною пастою, щоб не було опіків. Актор —"учень" починає грати свою роль: зображає тривогу, звертається вже до "учителя" з проханням не забути, що у нього хворе серце, слабкі нерви, він страждає на високий тиск і взагалі не радий, що згодився на роль "учня". Головне, щоб "учитель" відчув, що несе відповідальність за іншого, що він може стати не лише причиною страждань, але й смерті іншої людини.

Розпочинається експеримент. "*Учень*" традиційно виявляється малоосвіченим, робить багато помилок, що змушує "*учителя*" з кожним разом посилювати струм. "*Учень*" вже не кричить від болю, а волає помилувати його. І розпочинається головна стадія експерименту, зміст якого нам цікавий саме з точки зору висловленого вище припущення, як журналісти потрапляють у залежність від обраних і лідерів. Коли "*учитель*" хоче припинити експеримент, поруч з'являється той, хто наймав його для цього, хто платив йому хай мізерні, але гроші — суворий та невблаганний експериментатор і на спробу "*учителя*" припинити дослід вимагає: "Не зупиняйтеся. Це вкрай важливо й відповідально. Ви повинні продовжити". І "*учитель*"... продовжував. Як твердить сам Мілграм, сорок його колег, сорок досвідчених психіатрів до експерименту були переконані, що до смертельних 450 W може дійти хіба що один із тисячі, та й той із садистськими нахилами. Однак за підсумками експерименту максимальний струм призначили на вимогу "*лідера*" 65 відсотків учасників. А серед ліберально налаштованих студентів, котрі до цього демонстрували своєю поведінкою та зовнішнім виглядом цілковиту незалежність, виявилося 85 відсотків тих, хто уповні виконав інструкції експериментатора.

Психолог Мілграм зробив той висновок, що "*учителя*" йшли на поступки експериментатора лише тому, що він був у їх очах наділений владою, саме особистість із владними ознаками визначала їх поведінку, хоча вони й усвідомлювали, що чинять погано щодо людини, яку й не знають, проте добре чують і бачать. А що говорити про журналістів, якщо їх аудиторія для них безлика, а її стенань чи проклять вони не чують. Піддослідні "учителі" чимось нагадували дітей (виявляли інфантильну поведінку), коли малеча прагне діяти правильно за розумінням батьків і не викликати з боку дорослих немилості. "Учителя" прагнули діяти правильно й уникнути соціальної немилості, навіть наперекір своїм власним бажанням, перебуваючи у повній підпорядкованості авторитету — експериментатору. Виказуючи найвищий рівень напруги, прак-

тично усі "учителя", йдеться далі в описі експерименту, висловлювали протест (плакали, дрижали, кусали губи), але продовжували тиснути на кнопку. У нестандартних ситуаціях значна кількість людей виявлялися нездатними на самостійний моральний вчинок чи вибір, котрий йде у розріз авторитетному чи може авторитарному "Ви маєте!". У такій ситуації журналісти також обирають традиційний для цього експерименту шлях, а самообман допомагає їм зняти із себе вантаж відповідальності за скоєне.

На причини появи передумов маніпуляції вказував також відомий культурфілософ, естетик, представник іспанського екзистенціалізму, культуртрегер і публіцист Х. Ортега-і-Гассет. У такій ситуації він знаходить справжнє виправдання для ініціаторів маніпулятивних технологій. Мислитель виводить феномен "маніпулювання" із фатальної необхідності духовної диктатури у всі історичні епохи, що їх знало людство. Справді, його думка збігається з поглядами цитованого Е. Фромма чи Н.Макіавеллі. "Більшість людей, – твердить він, - не мають власної думки". Народ, чи як звичніше звучить у термінології Х.Ортега-і-Гассет маси, не здатні володіти теоретичним розумінням буття речей, маса здатна лише на оціночні судження. Народ ніколи не мав ідей про щонебудь, а лише віру, емпіричний досвід, приказки та міфи. Непридатність до теоретичного розмірковування заважає масі приймати усвідомленні рішення і формувати правильні думки. Але без думок людське суспільство було б хаосом, навіть більше – "історичним ніщо". Тому, переконаний цитований автор, "думку слід втиснути в людей під тиском ззовні, як мастило в автомобіль".

Таке нав'язування громадської думки полегшується тим, що масі загалом притаманна вроджена психічна функція відтворення, інстинкт слухняності і прагнення наслідування якогось прикладу. Водночас Х. Ортега-і-Гассет визнає, що нав'язування громадської думки – відверте насилля, завдяки чому у суспільстві виникає панування. Але без духовної влади, без того, хто втілює панування, без маніпулювання думкою і людьми у суспільстві склалася б анархія, яка врешті зруйнувала б суспільство. Тим паче маніпуляція потрібна в сучасну епоху, веде далі автор "*Бунту юрби*". Адже нині "маси", "*народ*", претендують на управління суспільством, не маючи на це відповідного досвіду й уміння. Сучасна "масова людина" не здатна мислити, переконаний Х. Ортега-і-Гассет. Тому формування громадської думки є загальним законом тяжіння політичної історії. "Словом, там, де відсутня меншість, що впливає на маси, і немає маси, котра готова підкоритися меншості, там суспільство або відсутнє, або перебуває на межі загибелі" [291].

Коли цитований автор говорить про меншість, він має на увазі політичну, підприємницьку та культурну еліту з чітко визначеними ціннісними та метафізичними принципами та нормами. І коли мова зайшла про цю суспільну групу, досить обмежену, закриту й консервативну, то варто одразу зауважити, що саме її принципи можуть бути засобом протидії масовим психологічним маніпулятивним технологіям, спрямованим на ЗМІ та журналістський корпус. За твердженням українського дослідника О. Бахтіярова, відсутність її (еліти)

робить завдання побудови контрманіпулятивних програм не на приватному, а на державному рівні, як того вимагає логіка суспільного розвитку, заздалегідь безнадійною справою [292]. Саме цей прошарок суспільства має демонструвати стан активної рефлексії й особливі стани об'ємної свідомості, які дозволяють одночасно бачити кілька альтернативних картин світу і підходів до вирішення актуальних проблем. Тоді він матиме моральне та історичне право називатися не політичними лідерами чи діючими політиками, а державними діячами. Проте, як писав вище Е.Фромм, у часи суспільних катаклізмів навіть найбільш досвідчена й обдарована частина суспільства зазнає розбрату й конфлікту інтересів. На допомогу національній еліті у захисті розвитку українського суспільства на основі автентичних принципів і норм від традиційно агресивних масових маніпулятивних технологій могли б прийти напрацьовані вітчизняним вченими контрманіпулятивні технології. Серед решти завдань ці технології мають передбачати і психологічний захист чи реанімацію такої інтенції, котра була б спрямована на зміцнення самоповаги, незалежності, цілісного ставлення до подій, конструктивного співробітництва та міжнародної інтеграції.

2.8. Медіа-маніпулювання масовою свідомістю як інструмент управління міжнародними кризами

У сучасному світі інформація виступає важливим стратегічним ресурсом не лише окремих країн, а й міжнародного співтовариства в цілому. В таких життєво важливих сферах діяльності держав як обстоювання національних інтересів, захист національної безпеки, формування позитивного іміджу держави у світі управління інформаційними потоками набуває вирішального значення. Досягнення цих цілей передбачає розробку і реалізацію комплексу заходів із впливу на внутрішню та зовнішню аудиторії. Адже успішність зовнішньополітичної стратегії держави значною мірою залежить від її сприйняття цільовою аудиторією. Для формування сприятливого інформаційного середовища та здобуття підтримки світової громадськості розвинені держави вдаються до засобів маніпулювання масовою свідомістю, починаючи від використання прийомів реклами і закінчуючи зовнішньополітичним ПР (*публічною дипломатією*).

Особливого значення технології впливу на світову громадськість набувають у кризових умовах, оскільки кризи у розвиткові конфліктних ситуацій викликають підвищений інтерес громадськості як всередині країни, так і за її межами.

У даній роботі висвітлено основні прийоми маніпуляції свідомістю та здійснено аналіз особливостей маніпулятивного впливу на світову громадськість на прикладі Іракської кризи 2002-2003 років. Використано промови президента США Дж.Буша та прем'єр-міністра Великої Британії Тоні Блера з офіційних сайтів Білого Дому та Даунінг Стріт.

Публічна дипломатія як "мистецтво" маніпулювання свідомістю.

Публічна дипломатія – це мистецтво завоювання думок та сердець за допомогою інформаційних впливів та двосторонньої комунікації. Головною метою публічної дипломатії є здобуття підтримки, сприятливого ставлення світової громадськості до зовнішньополітичної стратегії країни.

За визначенням USIA, публічна дипломатія спрямована на просування національних інтересів та національної безпеки через розуміння, інформування та здійснення впливу на зарубіжні аудиторії, а також розширення діалогу з іншими націями [293].

Інформування та розуміння означає поширення інформації про внутрішню та зовнішню політику країни через усі можливі канали комунікації, враховуючи особливості сприйняття та культури цільової аудиторії. Основним принципом є націленість на отримувача інформації: важливим є не стільки те, що сказано, а як це сприйнято аудиторією [294]. Підтримання діалогу з іншими націями здійснюється шляхом реалізації програм обміну як на освітньому, так і на урядовому рівнях. Важливою умовою ефективності здійснення публічної дипломатії є переконливість поширюваних повідомлень, їх послідовність та правдивість [295].

Сутність американської публічної дипломатії розкривається через її гасло: "Розповісти Американську історію всьому світові" [296].

Публічна дипломатія відрізняється від традиційної тим, що охоплює не лише взаємодію між урядами країн, але і встановлення співробітництва з неурядовими організаціями, громадськими угрупованнями.

У словниках термін "маніпуляція" трактується як поводження з обєктами з певними цілями, для яких потрібні спритність та вправність.

Зазвичай, це поняття вживається у переносному значенні і означає програмування думок та установок мас, їх настроїв і навіть психологічного стану для забезпечення поведінки, вигідної власникам засобів маніпуляції [275].

До особливих ознак маніпулювання відносяться:

- прихований психологічний вплив, здійснення якого потребує майстерності та знань;
- технологія здійснення влади, а не звичайний вплив на поведінку партнера;
- використання засобів переконання, заснованих на умисному введенні в оману;
- створення у об'єкта впливу ілюзії самостійності прийняття рішень та вибору дій [162; 274].

Маніпулятивному впливові підлягають як емоційна, так і раціональна сфери людської свідомості, а головним засобом є створення або використання кризи, аномальної ситуації, здатної вплинути на почуття. З метою маніпуляції використовуються як негативні, так і позитивні почуття, але ці емоції мають бути "актуалізовані" у суспільстві.

Одним з найпоширеніших об'єктів маніпуляції є почуття страху. Розрізняють два типи страху: істинний (реакція на реальну небезпеку) та ілюзорний (формується в уявленні людини, у світі символів). Різновидом ілюзорного страху є маніакальний страх внаслідок перебільшення небезпеки та могутності "*ворога*" [240].

Оскільки почуття тісно пов'язані з уявленнями, то ефективне управління народними масами передбачає здійснення впливу на їх уявлення через виклад інформації таким чином аби сформувати яскраву й цілісну картину реальності. Як творча здібність, уявлення має високий рівень уразливості до зовнішнього впливу. Максимальний ефект досягається за умови поєднання емоцій з уявленням. Одним з яскравих прикладів такого впливу на масову свідомість є тероризм у поєднанні з впливами телебачення.

Цінність уявлення як об'єкту маніпулювання пояснюється тим, що уявлення дає загальне враження від предмету, пов'язане з імітацією, — уявленням себе на місці іншого.

Активне уявлення, пов'язане з прогнозуванням ситуації чи плану дій, спрямоване на майбутнє і розташовує образи у певні, досить чіткі часові координати. Це дозволяє переконати людей у тому, що подія відбудеться рано чи пізно й тим самим приспати пильність або, навпаки, спровокувати передчасні дії.

Поряд з емоціями та уявленням важливими об'єктами маніпуляції є увага та пам'ять. Основна мета маніпулятора полягає у переконуванні людей шляхом привернення та утримання уваги на тих чи інших повідомленнях, темах тощо. Людина повинна не лише звернути увагу на повідомлення, а й запам'ятати "*потрібну*" інформацію.

Запам'ятовування інформації досягається за допомогою частих повторень та поширення повідомлень з високим рівнем емоційності. Як правило, людина запам'ятовує те, що її вразило. Для посилення ефекту маніпуляції емоційний вплив підкріплюється аргументами, доказами та іншими доводами. До головних об'єктів маніпулювання на раціональному рівні відносяться знакові системи, особливо мова, а також метафори, асоціації та стереотипи.

Мова як система понять, за допомогою яких людина сприймає світ та суспільство, є головним засобом підкорення. Сила мови як засобу маніпулювання посилюється тим, що слова здатні викликати певні образи в уявленні людини. Маніпуляція на цьому рівні передбачає подвійний вплив: поряд з відкрито надісланим повідомленням маніпулятор надсилає адресату «закодований» сигнал, сподіваючись викликати у його свідомості потрібні образи. Цей прихований вплив спирається на здатність адресата створювати в уяві образи, які впливають на його почуття, думки та поведінку. Значну роль у програмуванні поведінки людини відіграють асоціації та метафори.

Серед знакових систем не менш важливу роль, аніж слова, відіграють числа. На відміну від слова, число створює враження точності та неупередженості, а отже правдивості. До того ж число є сильним засобом сугестії: як-

що людина сприйняла якесь кількісне твердження, навіть абсурдне, його вже практично неможливо витіснити не лише логікою, але й кількісними аргументами.

Людина аби діяти у власних інтересах має реалістично визначити три речі: сьогоднішній стан, бажаний стан у майбутньому та шлях переходу від теперішнього до майбутнього стану. Але замість вивчення та осмислення цих речей, людина вдається до асоціацій та аналогій, тобто вживає метафори, які відсилають її до інших, вже звичних станів. Але у дійсності зрозумілість станів є ілюзорною. Саме на створення таких ілюзій спрямоване маніпулювання свідомістю. Для впливу використовуються короткі яскраві чи виразні лозунги, алегорії, порівняння тощо.

Одним з найсильніших засобів впливу на масову свідомість є стереотипізація. Соціальні стереотипи допомагають людині швидко сприймати і оцінювати дійсність і є невід'ємними складовими масової свідомості. Вони являють собою стійку сукупність уявлень що формується на основі особистого досвіду і різноманітних джерел інформації та включають емоційне ставлення людини до об'єктів та явищ.

Маніпуляція передбачає не лише використання вже існуючих у суспільстві стереотипів, але й створення ілюзорних стереотипів, тобто нав'язування тих чи інших, часто неправдивих ідей та пояснень у такий спосіб, що вони стають звичними й очевидними. Прикладом є антикомуністичний стереотип, що формувався США у часи існування СРСР.

Одним з складних стереотипів є імідж глави держави, політичного лідера або громадського діяча. У міжнародній політиці на формування іміджу лідера країни або нації в цілому впливають такі фактори, як державні інтереси, історичний досвід, тобто сприйняття іншого на основі минулих стереотипів, когнітивний фактор (потреба у диференції відносно інших), а також подібність культури та цінностей іншої нації тощо [297].

Особливості використання зазначених маніпулятивних технологій у зовнішньополітичній стратегії можна прослідкувати на прикладі американо-британської інформаційної стратегії проти Іраку наприкінці 2002 – на початку 2003 років.

Антіракська інформаційна стратегія "завоювання думок та сердець". Іракська криза є типовим прикладом спричинених [298]. Спричинені кризи є навмисними та ініціюються державою, яка прагне спровокувати збройний конфлікт. Шукаючи привід для початку війни держава-агресор діє таким чином, щоб перетворити свого невинного "супротивника" на головного призвідника кризи та подальшої війни. Держава вдається до різного роду засобів, хитрощів та дипломатичних прийомів аби ізолювати свого супротивника й водночас здобути собі підтримку громадської думки як країни-жертви, так й міжнародного співтовариства в цілому. Особливістю спричинених криз є те, що держава–провокатор прагне не до угоди чи компромісу, а лише до абсолютної перемоги.

У даному випадку ініціатором кризи виступили США за підтримки Великобританії, жертвою – Ірак. Керівництво США та Великобританії сконцентрувало свої зусилля на переконуванні світової громадськості у необхідності застосування радикальних заходів щодо Іраку, який становить неабияку загрозу міжнародній спільноті. Головна мета – роззброєння Іраку заради збереження миру та безпеки у світі.

В основу "кризової" стратегії США було покладено використання страху для емоційного впливу на громадськість. Підкреслюючи уразливість Америки після терактів 11 вересня 2001 року Президент США Дж. Буш попереджав, що небезпека з боку Іраку є значно більшою й може призвести до більш жахливих наслідків [299].

Основний акцент було зроблено на *"демонізації"* іракського лідера Саддама Хусейна та його режиму. Саддам Хусейн позиціонувався як *"кровожерливий тиран"*, *"найжорстокіший диктатор у світі"*, *"безжалісний, агресивний диктатор"*, *"учень Сталіна"* тощо [300-301]. За словами Прем'єр-міністра Великої Британії, ці характеристики обумовлюють специфіку дипломатичної стратегії щодо Іраку: Саддам Хусейн має усвідомлювати, що дипломатичні заходи можуть бути підкріплені силою [302].

Обґрунтування небезпечності іракського режиму й особливо його лідера включало декілька аспектів.

По-перше, Саддам Хусейн розв'язав дві війни, атакував сусідні країни без попередження, заохочував виробництво зброї масового знищення. За його наказами були здійснені хімічні атаки не лише на сусідні країни й на іракський народ, катування дітей, жорстокі репресії проти політичних опонентів [301].

Для більшої переконливості керівництва США та Великобританії наводили кількісні показники, які демонструють масштабність жертв політики іракського режиму та арсеналу зброї масового знищення Іраку [302]. Зокрема, у промові Президента США Дж.Буша наводиться цифра 20 000 людей, які загинули внаслідок хімічних атак, ініційованих Саддамом Хусейном. Зверталася увага, що цей показник у 6 разів перевищує число жертв від терактів 11 вересня 2001 року у США. [301].

По-друге, наголошувалося на тому, що іракське керівництво підтримує тісні зв'язки з міжнародними терористичними угрупованнями, у тому числі з членами Аль Каїди. Саддам Хусейн надає всіляку допомогу терористам й на території Іраку розташовані бази підготовки терористів. Підкреслюючи ворожість й ненависть Хусейна до США, Дж.Буш мимохідь зазначив, що іракський лідер не приховував задоволення, дізнавшись про теракти 11 вересня.

По-третє, акцентувалася ворожа непримиренність Саддама Хусейна до світового співтовариства. Впродовж 11 років Саддам Хусейн порушував резолюції Ради Безпеки ООН, які зобов'язували його повністю знищити зброю масового знищення. За словами Дж. Буша, "весь світ був свідком 11-річної історії непідкорення, обману та віроломності з боку Іраку" [301].

Особливо алармістською була постійно відтворювана інформація про те, що, незважаючи на економічну блокаду та ізоляцію країни від цивілізованого світу, Саддам Хусейн розвивав і продовжує розвивати програму з розробки зброї масового знищення. Відповідно одного дня іракський лідер може застосувати страшну зброю проти будь-якої країни [303]. Звідси нав'язувався однозначний висновок: оскільки існує значна ймовірність "найгіршого випадку", подальші зволікання та бездіяльність є найбільш ризикованим варіантом поведінки. Така політика лише дасть можливість Саддаму Хусейну зміцнити свої позиції й тримати весь світ у постійному напруженні.

Для більшої переконливості пропагандисти вдавалися до прийому використання історичних аналогій. У даному разі, - аналогії із мюнхенським умиротворенням 1938 р., яке відкрило шлях Гітлеру до розв'язання II Світової війни.

Особливістю американо-британської медіа-інформаційної кампанії проти Іраку полягає у її націленості на конкретну особистість. У своїх промовах Дж.Буш і Тоні Блер неодноразово наголошували, що їх ворогом є Саддам Хусейн, а не іракський народ. США та Великобританія прагнуть звільнити іракський народ від тирана та диктатора, а отже від пригнічення, злиденності, страждань, та забезпечити вільний розвиток і процвітання нації [304].

Паралельно з формуванням гіпертрофованого образу ворога в особі Саддама Хусейна, США позиціонували себе як країну, покликану захищати мир й боротися зі злом не лише всередині країни, але й на світовій арені [305].

Починаючи з лютого 2003 року, медіа-стратегія керівництва США та Великобританії була сфокусована на переконуванні світової та, власне, американської й британської громадськості у небажанні іракського лідера забезпечити повноцінне співробітництво з інспекторами міжнародної організації й виконати вимоги ООН [306].

Непідкорення Саддама Хусейна розцінювалося як вираз зневаги до міжнародного співтовариства, яке впродовж 12 років проявляло терпимість й намагалося обмежитися лише мирними засобами. До того ж подальші ухиляння іракського лідера свідчать про неефективність такої політики стримування. За цих умов країни змушені вжити силові методи для роззброєння Іраку. Дж. Буш підкреслив, що Саддам Хусейн знехтував останнім шансом й свідомо зробив вибір – роззброєння силовими методами [307].

Мотивуючи доцільність ліквідації режиму Саддама Хусейна американський президент виділив декілька позитивних змін на міжнародній арені:

- встановлення довготривалої безпеки та стабільності у світі;
- створення умов для демократичного розвитку та процвітання Іраку;
- зрушення у відновленні миру на Близькому Сході;
- послаблення терористичних організацій [308].

Звертає на себе увагу також роль, що надається ООН. У промовах американського президента справа Іраку постає як своєрідне випробування на ефективність чи здатність ООН протистояти викликам сьогодення. Доцільно

навести один уривок з промови Дж. Буша від 26 лютого 2003 року: "Якщо Рада [Безпеки] відповість на непідкорення Іраку черговими зволіканнями, якщо її влада нічим не буде підкріплена, то ООН як джерело стабільності та порядку буде сильно послаблена". (*"If the council [the Security Council] responds to Iraq's defiance with more excuses and delays, if all its authority proves to be empty, the United Nations will be severely weakened as a source of stability and order"*) [308].

Маніпулятивні прийоми, використані під час іракської кризи, зведені у таблиці.

Таблиця

Об'єкти та прийоми маніпулювання у період Іракської кампанії

Об'єкти маніпуляції	Маніпулятивні прийоми
Емоції	Формування страху перед ймовірністю повернення жахів 11 вересня 2001 року, але у більш страшній формі
Уявлення	Створення цілісного образу ворога шляхом "демонізації" іракського лідера
	Переконання у ймовірності несподіваного застосування Іраком зброї масового знищення проти будь-якої нації
Пам'ять	Постійне повторення інформації про жорстокість Саддама Хусейна
	Невиконання ним міжнародних зобов'язань
	Нагадування про постійні ухиляння іракського диктатора від контролю міжнародного співтовариства, введення ним в оману світової громадськості
	Акцентування зв'язків Саддама Хусейна з терористами
Знакові системи	Використання кількісних показників, які свідчать про чисельність жертв політики іракського керівництва та значні запаси зброї масового знищення
Асоціації та стереотипи	Побудова асоціативного ряду: Ірак - Саддам Хусейн – небезпечний тиран, зброя масового знищення – тероризм – жахливе майбутнє
	США – поборник міжнародного миру, безпеки, прав і свобод людини – визволитель іракського народу

Таким чином, під час антиіракської кампанії був задіяний практично весь спектр маніпулятивних прийомів. Емоційний вплив на громадськість здійснювався шляхом формування ілюзорного страху перед *"ворогом"*. Посилення ефекту досягалося логічним викладом історичних фактів, доказів, включаючи числові показники, та формулюванням висновків щодо найгіршого варіанту розвитку подій. Інформаційна кампанія була націлена головно на демонізацію супротивника. Негативний образ іракського лідера будувався шляхом орієнтації сприйняття громадськості на минулі стереотипи та екстраполяції минулого на сьогодення й майбутнє. Для акцентування небезпечності

ворога здійснено диференціацію:

- керівництва Іраку й іракського народу: ворогом є Саддам Хусейна, а не весь іракський народ;
- Іраку й решти світу: Ірак як антипод "*нормальних*" країн, в якому не визнаються загальнолюдські цінності й панує терор і страх.

Втім результати Іракської кризи свідчать про неефективне здійснення даної кампанії публічної дипломатії, завдяки якій так і не вдалося здобути підтримки світової громадськості. Інакше кажучи, не було досягнуто головної мети публічної дипломатії – переконати міжнародну спільноту у правильності зовнішньополітичної стратегії держави. США вдалося переконати лише внутрішню американську аудиторію. За інформацією CBS більше половини громадян США схвалювали стратегію Дж. Буша й вірили у високий рівень загрози з боку Іраку та необхідність рішучої боротьби проти диктаторського режиму [309].

Водночас, за даними Pew Research Center for the People and the Press, антиіракська кампанія призвела до посилення антиамериканських настроїв у світі, а рейтинг схвалення зовнішньої політики США в європейських країнах суттєво знизився. До того ж, існує переконання щодо негативного впливу американської політики на європейські держави й щодо особистої відповідальності за це Дж.Буша, а не США в цілому [310].

Причини погіршення міжнародного іміджу США містяться в самій американській зовнішньополітичній стратегії: проголосивши головною метою боротьбу з тероризмом, США зарезервували за собою право не лише самостійно визначати терористів та держав, які підтримують тероризм, але і вдаватися до превентивних військових операцій проти цих країн в односторонньому порядку без санкцій Ради Безпеки ООН [311].

Така політика продемонструвала розбіжність між ідеалами, що проголошуються, та реальною політикою. Виступаючи за захист прав та свобод людини, за справедливість, повагу до суверенітету інших країн, за дотримання міжнародно-правових норм й суворе покарання порушників, за збереження миру та безпеки, США тимчасом з чисто імперських позицій єдиної у світі наддержави втручаються у внутрішні справи інших держав й, ігноруючи думку світової громадськості, розв'язують війну без санкцій ООН.

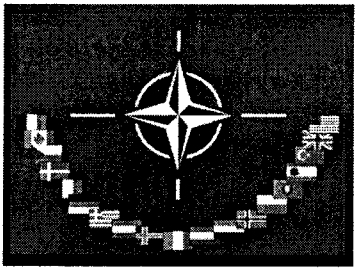
Істотною помилкою публічної дипломатії США та важливим чинником зростання ворожості з боку мусульманських країн було неврахування особливостей культури та комунікацій цільової аудиторії. Американське керівництво фактично здійснювало однобічну публічну дипломатію, засновану на американському стилі комунікацій. Публічна дипломатія США базувалася на поширенні великого обсягу фактів та аргументів, спиралася на ЗМІ як основний канал комунікації. В арабських країнах такі стратегії не спрацьовують, оскільки мас-медіа не користуються популярністю і довірою серед населення, перевага надається міжособистісній комунікації та емоційно забарвленим повідомленням (метафори, аналогії є більш переконливими, ніж звичайні докази) [312].

Антиіракська кампанія негативно позначилася на іміджі американського президента Дж.Буша та британського прем'єр-міністра Тоні Блера. За даними опитування американських громадян, у вересні 2003 року рейтинг схвалення зовнішньої політики Дж. Буша досяг найнижчого за період іракської кризи показника (45 %). У жовтні цей показник зріс до 53%, у той час як на початку війни в Іраку -у квітні цього року - він становив 66 % [313].

Тоні Блер був звинувачений у фальсифікації інформації про іракську зброю масового знищення. За результатами опитування більшість громадян Великобританії (67%) вважають, що уряд Тоні Блера вводив їх в оману. До того ж суттєво знизився рівень довіри до урядових джерел інформації (6% громадян) [314].

РОЗДІЛ 3

ІНФОРМАЦІЙНА БЕЗПЕКА В РЕГІОНАЛЬНИХ ТА НАЦІОНАЛЬНИХ ДОКТРИНАХ



3.1. Регіональна інформаційна безпека: європейська та євроатлантична практика

Процеси світової глобалізації, тенденції зрощування глобальних і регіональних проблем вплинули на можливості суверенних держав визначати напрями і стратегії політичних змін як всередині країни, так і в світі в цілому, обумовили необхідність створення потужного механізму міжнародних інститутів на регіональному рівні для розв'язання глобальних проблем міжнародного співробітництва. Характерною рисою європейської інформаційної політики в галузі безпеки та превентивної дипломатії є включення у систему прийняття рішень регіональних міжурядових інститутів ЄС, ОБСЄ та НАТО. Діяльність регіональних міжурядових організацій в галузі інформаційної безпеки та міжнародного обміну інформацією суттєво вплинула на міжнародні відносини, виявила диспропорції і нерівність європейських країн в інформаційному розвитку, сформувала нові контури регіональної безпеки.

Концепція регіональної політики інформаційної безпеки зумовила позиції країн ЄС, НАТО та ОБСЄ щодо інформаційного виміру європейської безпеки, сприяє взаєморозумінню і пошуку спільних рішень щодо протидії інформаційним та комунікаційним загрозам, визначає пріоритетами політики безпекових інституцій – забезпечення сталого миру в регіоні, становлення інформаційного суспільства, нової економіки та міжкультурних відносин.

Вирішення проблеми інформаційної безпеки у програмах Європейського Союзу передбачає вироблення загальної стратегії європейської інформаційної безпеки, протидії кібервійнам, інформаційному тероризму та боротьбу з інформаційною злочинністю. Інформаційна безпека в рамках НАТО охоплює стратегії інформаційної політики та інформаційного протиборства в контексті переосмислення стратегії безпеки у XXI ст., створення системи регіональної інформаційної безпеки, сприяння розвитку кадрового потенціалу з інформаційної безпеки, здійснення спеціальних інформаційних операцій, роз'яснення цілей діяльності НАТО для громадськості. Компетенція ОБСЄ в сфері інформаційної безпеки полягає у визначенні загальних підходів до прогнозування конфліктів, у моніторингу кризових ситуацій, в ухваленні документів з інформаційної безпеки та застосуванні заходів превентивної дипломатії.

Взаємодія держав європейського регіону в процесі освоєння та застосування ІКТ(інформаційно комунікаційні технологій) стала однією з найдинамічніших та багатообіцяючих сфер міжнародного співробітництва. В зв'язку з цим в доктрині зовнішньої політики ЄС з'являються нові положення, а в дипломатичній діяльності – нові задачі, пов'язані з забезпеченням інформаційної безпеки в регіоні. Важливо враховувати той факт, що вдосконалення інформаційних технологій сприяє не лише зміцненню суспільних зв'язків, а й веде до появи невідомих раніше джерел ризику та небезпеки.

Нові виклики інформаційно-комунікаційних технологій зумовили загострення багатьох проблем: збільшення цифрового розриву між розвинутими країнами і країнами, що розвиваються; організація та контроль глобальних процесів на користь еволюційного розвитку суспільства; забезпечення регіональної та світової інформаційної безпеки.

Так економіка і обороноздатність провідних держав світу все більшою мірою залежать від нормального функціонування глобальних комп'ютерних мереж. Порушення їх працездатності може спричинити серйозні наслідки, а національні і міжнародні правові інститути і організаційні структури практично не готові до адекватної протидії новим загрозам.

Разом із позитивними, розвиток ІКТ та Інтернет спричиняють і негативні наслідки. Прихованість та знеособленість підключення до телекомунікаційних мереж створюють можливості для несанкціонованого, в тому числі і транскордонного, збору інформації та контролю за особою, здійснення в міжнародному масштабі різного роду незаконної діяльності (тероризм, кримінал), експорту ідей, культури та моральних цінностей, які несуть руйнівний вплив на національне суспільство в інших державах. Тобто людство, використовуючи нові можливості, водночас переносить у віртуальний простір свої проблеми, які можуть набувати там всесвітніх масштабів, впливати на реальність і навіть формувати її, оскільки світова спільнота не встигла встановити бар'єри та правила регулювання в цьому новому, глобальному електронному середовищі.

Всесвітня мережа є ідеальним середовищем для діяльності терористів, оскільки до неї існує легкий доступ, в ній легко забезпечити анонімність користувачів, вона ніким не управляється і не контролюється, в ній не діють закони і не існує поліції. На сьогоднішній день в мережі представлені абсолютно всі відомі терористичні групи, які публікують свої матеріали, щонайменше, на 40 різних мовах. Терористичні групи створюють і багатомовні сайти, щоб забезпечити вплив на людей, які безпосередньо не залучені в конфлікт.

Прямий політичний наслідок інформаційно-комунікаційної революції — прискорення процесу трансформації міжнародних відносин, яка проявляється у наступних напрямках:

- Розмивається традиційна концепція національного суверенітету. Існує теорія, згідно якої глобальне електронне середовище є непідконтрольним національним урядам. Транспарентність та проникність національних кордонів для інформаційних потоків ведуть до того, що національні уряди не можуть повністю контролювати нові інформаційні послуги та види діяльності, які здійснюються через інфомережі. По-перше, проти цього виступає значна частина світової спільноти, яка дбає про права та свободу особи. По-друге, для такого контролю ще немає суттєвої правової бази — ні національної, ні міжнародної, — розвиток якої відстає від розвитку віртуальної реальності і практики. По-третє, для його введення потребуються значні фінансові, технологічні та кадрові ресурси.

- Ставиться під сумнів відповідність змісту поняття «територія» новим умовам.
- Національний суверенітет «стискається» у зв'язку з тим, що з'являються нові учасники міжнародних відносин — транснаціональні корпорації і транснаціональні банки, а також неурядові організації.
- Принципово новою у зв'язку з розповсюдженням ІКТ стає проблема забезпечення європейської інформаційної безпеки. Вона доповнюється інформаційно-комунікаційною складовою. Імплементація цих технологій призводить як до збільшення могутності держави, так і до її вразливості з точки зору інформаційно-електронного впливу [315].

В сучасних умовах вся сукупність інформаційних ресурсів держав стає одночасно і об'єктом ворожого впливу, і могутнішою зброєю в інформаційних війнах. Виникає загроза застосування надзвичайного потенціалу ІКТ в інтересах забезпечення військово-політичної переваги, силового протиборства, шантажу на міжнародній арені. Нового змісту набуває поняття агресії. Держави залучаються у процес створення у себе потенціалу для міжнародного хакерства, інфопіратства.

Новою транснаціональною загрозою є проблема міжнародної інфо- та кіберзлочинності, відповідних проявів міжнародного тероризму.

В інформаційному просторі існують і використовуються різні прийоми кібертероризму:

- завдання збитку окремим фізичним елементам інформаційного простору, наприклад, руйнування мереж електроживлення, наведення перешкод;
- використання спеціальних програм, стимулюючих руйнування апаратних засобів, а також біологічних і хімічних засобів для руйнування елементної бази та ін.;
- крадіжка або знищення інформаційного, програмного і технічного ресурсів, що мають суспільну значущість, шляхом подолання систем захисту, впровадження вірусів, програмних закладок і т. п.;
- дія на програмне забезпечення й інформацію з метою їх спотворення або модифікації в інформаційних системах і системах управління;
- розкриття і загроза публікації або сама публікація закритої інформації про функціонування інформаційної інфраструктури держави, суспільно значущих і військових інформаційних систем, кодах шифрування, принципах роботи систем шифрування, успішному досвіді ведення інформаційного тероризму та ін.;
- захоплення каналів ЗМІ з метою розповсюдження дезінформації, чуток, демонстрації потужності терористичної організації і оголошення своїх вимог;
- знищення ліній зв'язку, неправильна адресація, штучне перевантаження вузлів комутації;
- проведення інформаційних і психологічних операцій і ін.[316]

Розвиток глобальних інформаційних мереж, в першу чергу загальнодоступного Інтернету, значно полегшило організацію діяльності терористичних організацій, спростивши рекрутування бойовиків та політичних прихильників, організацію управління ними, закупівлі зброї та оплату проведених операцій, пропагування ними своїх ідей та проведення інформаційних кампаній проти офіційної влади. Інфомережі — це також зручний та доступний об'єкт для проведення диверсій.

ІКТ впливають на всю економічну діяльність держав. Зростаюча процесорна міць, падіння вартості інформації і мережева взаємодія сприяють підвищенню продуктивності праці, електронна комерція та Інтернет-банкінг стимулюють інновації і подальші технічні зміни у всіх секторах, включаючи високотехнологічні і традиційні. Європейська Комісія надає великого значення індустрії ІКТ і вказує три головних напрямки її розвитку:

- доступний, швидкий і безпечний Інтернет;
- інвестиції в людські ресурси;
- стимулювання масового використання Інтернету [317].

Але взаємопов'язаність та успіх Інтернет одночасно створюють нову залежність, а залежність спричиняє вразливість. Тому відкрита архітектура Інтернет — це не лише його найбільша перевага, але й відкриті двері до протизаконного його використання.

Вплив Інтернету на дійсність часто недооцінюється. Можна говорити про зміни в структурі суспільної свідомості, пов'язані із знищенням моралі (розповсюдження порнографії), права (спори за доменні імена, вірусні ліцензії, електронний підпис, копірайт), політики (пропаганда, створення компромату), міжнародних відносин (відсутність в мережі державного суверенітету). Боротьба з кіберзлочинністю та кібертероризмом — найважливіший фактор, який впливає на політику держав і є викликом у забезпеченні інформаційної безпеки. Інтернет призвів до появи нових форм злочинності, серед яких злочини, пов'язані зі зломом, підробкою та використанням кредитних карток [318].

Інтернет надає злочинцям виняткові можливості. Він служить для них джерелом легкого (і без привертання зайвої уваги) отримання практично будь-яких необхідних відомостей: від пропозицій потенційних постачальників зброї і необхідних технічних засобів до інструкцій про створення бомб. З його допомогою можна переказати необхідні фінансові кошти або отримати їх, збираючи пожертвування або зламуючи банки, можна вербувати найманців і здійснювати пропаганду і, нарешті за допомогою Глобальної Мережі можливо швидко і з мінімальними витратами порушити нормальне функціонування будь-якого об'єкту цивільної або військової інфраструктури. І все це при виключно високому рівні захищеності від втручання держави в потоки відповідної інформації, а, отже, при збереженні основної характеристики і умови злочинної чи терористичної діяльності — її секретності.

В результаті, багатофункціональні можливості й постійно зростаюча важливість Інтернету піднімають тепер серйозні питання про безпеку:

- Постійна загроза вірусів. Кількість вірусів набула вибухового росту за останні декілька років, вони стали складнішими та «ефективнішими», призвели до великих економічних збитків. В 2004 році, наприклад, лише три віруси Bagle, MyDoom та NetSky разом завдали шкоди більш ніж у 100 мільярдів $ по всьому світі.
- Розповсюдження незаконної чи небезпечної інформації через вебсайти. *Вебсайти - ідеальні інструменти для того, щоб поширювати інформацію* і дезінформацію у глобальному масштабі. Тому терористичні групи усе більше використовую їх для своєї пропаганди, а їх методи стають все більш професійними. Для терористичних груп вебсайти надають багато переваг: легкі у створенні та використанні, доступні, дешеві, забезпечують анонімність.
- Злочинне використання електронної пошти.
- Шпіонаж за конфіденційною інформацією. Кожна комп'ютерна система, яка пов'язана з мережею, вразлива до вторгнення, і вся цифрова інформація може бути використана зловмисниками. Чи то шпіонаж здійснений діловим конкурентом, чи іноземною секретною службою, чи терористом або лише «звичайними» хакерами, у більшості випадків жертва не буде навіть розуміти, що інформація з її комп'ютера була скопійована третьою особою або, коли вона здогадається чи помітить, вже буде занадто пізно реагувати. Всі переміщення даних через Інтернет ризикують бути перехопленими.
- Виведення з ладу суспільно важливих інформаційних систем та інфраструктур. Відповідно до визначення Європейської Комісії, суспільно важливі інформаційні системи та інфраструктура складаються із тих фізичних та інформаційних засобів обслуговування технологій, мереж, послуг та активів, порушення або зупинення яких мало б суттєвий вплив на здоров'я, безпеку, економічний добробут громадян або ефективне функціонування уряду в державах-членах [318].

В Європі мета політики інформаційної безпеки полягає у тому, щоб захистити інформацію (цілісність) та інформаційні системи, гарантувати належні умови її обігу (доступність, конфіденційність) та цінність. Ці завдання необхідні для того, щоб гарантувати незалежне здійснення державної політики та надійне використання інформаційно-комунікаційних технологій у важливих соціальних та економічних галузях (електронне врядування, торгівля, освіта, медицина і т.д.)

Три види суб'єктів можуть бути причетними для виконання вищезазначених цілей забезпечення інформаційної безпеки в європейському регіоні:

- громадяни, які пов'язані з захистом інформації та даних;

- компанії, дії та успіх яких тісно пов'язані з захистом їх ноу-хау, повагою до прав інтелектуальної власності, чесної конкуренції та діяльності, заснованої на використанні складних інформаційних систем;

- державний апарат, відповідальний за захист та безпеку безперервної роботи установ та інфраструктури, які є життєво важливими для соціально-економічного життя [318].

Отже, інформаційні загрози надають цілий ряд серйозних викликів громадськості. По-перше, через їх внутрішній характер комп'ютерні атаки практично неможливо прогнозувати або прослідкувати в реальному часі. Тому атака може у будь-який час, в країні або за кордоном, і стояти за нею можуть спраглі гострих відчуттів молоді люди, вороже налаштовані країни, злочинці, шпигуни і терористи; потрібно буде витратити значні ресурси, щоб з високою мірою ймовірності визначити, хто несе за це відповідальність. Технологічно, як прогнозується, не буде можливим в найближчому майбутньому вирішити цю проблему. По-друге, із-за складності законів, що діють у всьому світі, збір доказів в таких обставинах, коли могли бути використані Інтернет або інші електронні засоби, а також переслідування згідно із законом, пошук, захоплення і видача окремих осіб представляються проблематичними. Вказані проблеми актуалізують необхідність осмислення механізмів, що існують, і вироблення нових міжнародно-правових механізмів боротьби з кібертероризмом.

У кожній із цих сфер ціль полягає у тому, щоб захистити інформацію та інформаційні системи чи мережі завдяки низці технічних та законодавчих заходів, які покликані врахувати потреби забезпечення прав та свобод особистості та потенційний розвиток кримінальних злочинів.

Формування нової європейської системи безпеки здобуває реальних характеристик на підставі основних загальноприйнятих принципів, а саме:

- чіткого усвідомлення факторів, що впливають на рівень національної безпеки: політичні, економічні, військові, етнічні, екологічні, інформаційні та інші фактори, розвитку демократичних процесів, формуванні взаємовигідних міждержавних відносин;
- необхідності створення механізмів колективного реагування на нові загрози, що набули трансконтинентального характеру: міжнародний тероризм, поширення зброї масового ураження і обігу наркотиків, організована злочинність тощо;
- визначення фундаментальних вимог до системи колективної європейської безпеки – неподільності безпеки та її всеохоплюючого і комплексного характеру [319].

Наявність досить великої кількості різноманітних європейських і трансатлантичних інститутів і організацій, які приймають участь в процесі забезпечення безпеки в Європі потребує найшвидшого рішення питання про розподіл відповідальності і координації діяльності.

ОБСЄ – одна з провідних структур із підтримання безпеки та стабільності у регіоні, що охоплює всю Європу, Північну Америку (США, Канада) та центральноазіатські республіки колишнього СРСР. Як єдиний форум ОБСЄ є ключовим компонентом європейської архітектури безпеки. Вона являє собою комплексну основу для співпраці в галузях прав людини, фундаментальних свобод, демократії, верховенства права, економіки та безпеки.

Нова модель безпеки, спираючись на Гельсінські принципи і Кодекси поведінки держав, повинна сприяти закріпленню безпеки всіх держав—учасників ОБСЄ без виключення. Саме на саміті у Гельсінках у 1992 р. уперше поняття «безпека» було розширене таким чином, що із суто військово-політичного, тобто такого, як було раніше, воно перетворилося на багатомірне, включаючи у себе ще й інформаційні, торгово-економічні, екологічні та гуманітарні відносини. Необхідно уникнути включення у нову модель безпеки *тих елементів, які могли б забезпечувати безпеку одних учасників за розвиток* інших. В цьому плані особливого значення набуває розвиток засобів довіри.

Починаючи з саміту ОБСЄ у Будапешті в грудні 1994 р., ця організація була задіяна до глибокого комплексного обговорення усіх аспектів безпеки, спрямованого на розробку концепції безпеки XXI сторіччя.

У грудні 1996 року, у прийнятій на Лісабонському саміті Декларації про систему загальної та всеосяжної безпеки у Європі XXI сторіччя, глави держав і урядів країн – членів ОБСЄ ще раз підтвердили, що європейська безпека потребує якнайширшої співпраці та координації зусиль між державами-учасницями й іншими європейськими та трансатлантичними організаціями. Вони також заявили про свій намір розвивати співпрацю з іншими організаціями безпеки [320]

Розглядаючи шляхи підвищення ролі ОБСЄ в забезпеченні інформаційної безпеки у Європі, слід враховувати обмежені можливості цієї Організації самостійно протистояти сучасним викликам і загрозам. Це робить необхідною практичну реалізацію схваленої в рамках Хартії європейської безпеки (1999 р.) *Платформи безпеки, що ґрунтується на співробітництві*, яке передбачає зміцнення і розвиток співпраці ОБСЄ з ООН, ЄС, Радою Європи і НАТО на засадах взаємозміцнення, взаємодоповнення і рівноправності. У цьому зв'язку стає актуальним налагодження конкретних механізмів взаємодії між зазначеними організаціями, зокрема у вирішенні загроз, пов'язаних з розвитком ІКТ.

У своїй Декларації з питань євроатлантичної безпеки й співробітництва, прийнятій в Мадриді у 1997 році, глави держав та урядів країн НАТО визнали ОБСЄ як організацію європейської безпеки, що має найширше представництво. Вони підкреслили ключову роль ОБСЄ у забезпеченні миру, стабільності та безпеки в Європі і наголосили на важливості принципів та зобов'язань, прийнятих цією організацією, за основу для розвитку структур всеосяжної європейської безпеки, що базується на співпраці [321]

У Мадриді НАТО також висловило свою подальшу підтримку зусиллям ОБСЄ, спрямованим на розбудову загальної та всеосяжної системи безпеки Європи XXI сторіччя та ідеї розробки Хартії європейської безпеки відповідно до *рішень, ухвалених у 1996 році на саміті ОБСЄ в Лісабоні.*

Головною метою НАТО є захист свободи і безпеки всіх її членів політичними та військовими засобами. З моменту утворення Альянс працює над установленням справедливого і тривалого мирного порядку в Європі на засадах

загальних демократичних цінностей, прав людини та верховенства права. Для досягнення своєї головної мети Альянс виконує такі основні завдання в галузі безпеки: закладає необхідне підґрунтя для стабільного клімату безпеки в Європі на основі зміцнення демократичних інститутів і прагнення до розв'язання суперечок мирним шляхом. Він намагається створити такі умови, за яких жодна країна не могла б вдаватись до залякування чи тиску, спрямованих проти будь-якої іншої держави, через загрозу застосування, або застосування сили.

На в квітні 1999 року держави-члени НАТО, ухвалили стратегію реагування Альянсу на виклики і можливості XXI століття, яка вказуватиме шлях майбутнього політичного і військового розвитку. забезпечує загальні напрями розробки детальних політичних та військових планів. У ній описані мета і завдання Альянсу і розглядаються його стратегічні перспективи у світлі змін у стратегічному середовищі та загрозах і ризиках для безпеки. У Концепції визначається підхід Альянсу до безпеки у XXI столітті, підтверджується важливість збереження трансатлантичного зв'язку та забезпечення необхідної військової потуги. В ній вивчається роль інших важливих елементів широкого підходу Альянсу до стабільності та безпеки, зокрема, власне .

У концепції відзначено, що останнім часом ситуація характеризується тривалими і в цілому позитивними перемінами і що Альянс відіграє важливу роль у посиленні євро – атлантичної безпеки, яке має місце по закінченні холодної війни. Що стосується ризиків, в документі підтверджується висновок, який був зроблений у Стратегічній концепції 1991 року про те, що загрози загальної війни в Європі практично вже не існує, але залишились інші ризики і нестабільність, з якими стикаються країни - члени Альянсу та інші держави євро - атлантичного регіону. Серед них: етнічні конфлікти, порушення прав людини, політична нестабільність, економічна вразливість, а також поширення ядерної, біологічної та хімічної зброї та засобів її доставки.

Альянс вважає за необхідне посилити свій європейських елемент через розвиток ефективної власне Європейської системи безпеки і оборони (ESDI), яка могла б задовольнити вимоги європейців і водночас підсилила безпеку Альянсу. Відповідно на зустрічі у у квітні 1999 року глави держав та урядів країн - членів Альянсу схвалили роботу з подальшого розвитку власне Європейської системи безпеки і оборони. Було розпочато обговорення ряду специфічних питань, а саме:

- засоби забезпечення ефективних взаємних консультацій, співпраці і гласності між Європейським Союзом ( ) і Альянсом, які ґрунтувались би на механізмах, що існують між НАТО і Західноєвропейським Союзом ( );
- участь європейських членів Альянсу, які не входять до ЄС;
- практичні можливості доступу ЄС до планувальних можливостей НАТО, а також до ресурсів і потужностей Альянсу [321].

Посилення власне Європейської системи безпеки та оборони (ESDI) стало невід'ємною частиною адаптації політичних та військових структур НА-

ТО. Водночас вона є важливим елементом розвитку Європейського Союзу (ЄС). Обидва процеси відбуваються на ґрунті Маастрихтського, 1991 р., та , 1997 р., договорів Європейського Союзу та відповідних декларацій Західноєвропейського Союзу, а також рішень, прийнятих Альянсом на Лондонському, 1990 р., 1994 р., , 1997 р., Вашингтонському, 1999 р. самітах, а також на засіданнях міністрів країн – членів НАТО.

З середини 2000 року спільні спеціальні робочі групи НАТО – ЄС проводять засідання для обговорення питань безпеки (наприклад, процедури обміну секретною, включно з розвідувальною, інформацією); умови доступу ЄС до ресурсів і сил НАТО; цілі розвитку спроможності (включно з питаннями системи оборонного планування Альянсу) та організація постійних консультацій.

14 березня 2003 р. НАТО та ЄС підписали спільну домовленість з політики інформаційної безпеки. З того часу, НАТО та ЄС почали переговори з метою встановлення взаємного визнання з оцінювання та схвалення криптографічного обладнання, яке використовується для захисту інформації, включаючи гриф «секретно».

Європейський Союз, як економічна міжнародна організація, підтримує доктрину європейської інформаційної економіки, впровадження нових технологій у традиційні сектори економіки, спрямовує розвиток "інтелектуальної" торгівлі для зростання економічної стабільності і конкурентоспроможності Європи на міжнародних ринках.

Нова економіка й Інтернет стоять на першому місці в програмі ЄС з часу Лісабонського Саміту (березень 2000р.) Тоді лідерами ЄС була визначена нова і досить амбіційна мета – перетворити Європу в регіон з найбільш конкурентоспроможною і динамічною економікою, заснованою на високих технологіях. Для досягнення цієї мети Європейська Комісія розробила всеосяжну стратегію, відому як план «Електронна Європа 2002» (e-Europe 2002 Action Plan) [319].

Ініціативи «Електронна Європа» (e-Europe) і «Лісабонська стратегія» («Lisbon strategy») ставлять за мету створити до 2010 року в Європейському союзі найдинамічнішу і конкурентоспроможну інформаційну економіку з більш високим рівнем зайнятості і суспільної згоди.

Процес законодавчої боротьби з кіберзлочинністю надзвичайно складний. Але деякі кроки в цьому напрямку вже зроблені. 23 листопада 1995 р. всіма державами ЄС в рамках проекту TREVI (Text Retrieval and Enrichment for Vital Information) була схвалена система тотального спостереження, яка створена для «прослуховування» та аналізу телекомунікаційних каналів держав Європейського Союзу. При цьому ЄС прийняв рішення направити листи різним міжнародним організаціям, які займаються питаннями телекомунікації (наприклад, ISO та ITU), з рекомендацією врахування положень проекту TREVI при розробці вимог до телекомунікаційного обладнання та послуг[322]. У грудні 1997 на зустрічі міністрів внутрішніх справ та юстиції дер-

жав «вісімки» було підписано документ «*Принципи та план дій по боротьбі з високотехнологічними злочинами*». У травні 2002 року в Парижі була досягнута домовленість про прийняття державами «вісімки» аналогічних законів по боротьбі з кіберзлочинністю на національному рівні. А у листопаді 2001 року на конференції в Будапешті представниками 30 держав (в тому числі 26 держав-членів РЄ) була підписана Конвенція з кіберзлочинності. Згідно з документом, повинен бути створений спеціальний міждержавний орган, який покликаний працювати в цілодобовому режимі і мати повноваження по вилученню матеріалів без залежності від фізичного місцезнаходження Інтернет-ресурсу. Узгоджували національні законодавства, режим розшукових заходів, передбачалась розробка системи покарання злочинців. Фактично документ передбачав створення міжнародної кіберполіції з найширшими правами. Ратифікація угоди затяглася, і на даний момент він не набрав чинності.

У Великій Британії вступив у дію закон про тероризм, який ставить комп'ютерних хакерів в один ряд з бойовиками Ірландської республіканської армії. Даний нормативний акт покликаний посилити боротьбу з різними угрупуваннями, які використовують територію Об'єднаного Королівства для своєї діяльності. Відповідно до нього, у разі злому хакерами комп'ютерної системи, що забезпечує національну безпеку країни, а також спроб з їх боку чинити дію на державні структури або загрожувати суспільству, вони можуть бути звинувачені в тероризмі зі всіма наслідками [323].

У країнах континентальної Європи йдуть аналогічні процеси. До розряду пріоритетних висувається питання правових і організаційних механізмів регулювання використання комп'ютерних мереж Першою міжнародною угодою по юридичних і процедурних аспектах розслідування і кримінального переслідування кіберзлочинів стала Конвенція з кіберзлочинності, прийнята Радою Європи 23 листопада 2001 р. Конвенцією передбачаються скоординовані на національному і міждержавному рівнях дії, спрямовані на недопущення несанкціонованого втручання в роботу комп'ютерних систем.

Очевидно, що жодна держава сьогодні не в змозі протистояти цьому злу самостійно. Боротьба з комп'ютерним тероризмом, як втім, і з тероризмом взагалі, не може бути долею окремо взятих держав, тому необхідно забезпечити взаємодію спецслужб, включаючи національні служби безпеки і спеціальні підрозділи по боротьбі з тероризмом на національному, регіональному і міжнародному рівнях.

Необхідне опрацьовування і коректування законодавчих, нормативних і правових документів відносно цього виду злочину, зокрема, що регламентують міжнародну діяльність. Найважливіше значення мають наукові роботи в області створення сучасних технологій виявлення і запобігання мережевим атакам і нейтралізації кримінальних і терористичних дій на інформаційні ресурси. Очевидно, що все це неможливо без вдосконалення багаторівневої системи підготовки кадрів в області інформаційної безпеки.

Інформаційна безпека закладає необхідне підґрунтя для стабільного клімату безпеки в Європі.

Особливості європейської безпеки – комплекс взаємопов'язаних принципів і норм, який відображає риси функціонування системи підтримання миру і безпеки в Європі та її взаємозв'язок як регіональної системи безпеки з універсальною системою забезпечення миру і безпеки.

Існування і діяльність регіональних систем безпеки не суперечать існуванню і діяльності універсальної системи і з необхідністю передбачає наявність регіональних систем, які діють для виконання тих задач, що і універсальна система. Існування універсальної системи безпеки передбачає наявність між ними юридично оформлених зв'язків і узгодження діяльності на основі правильного зваженого розподілу компетенцій.

У процесі забезпечення європейської безпеки разом з загальноєвропейськими організаціями (ОБСЄ, РЄ) беруть участь ряд субрегіональних організацій (Рада держав Балтійського моря, Рада Баренцового моря).

Для регіональних організацій, які включені в процес забезпечення європейської безпеки, притаманна свого роду «спеціалізація» по певній проблематиці, пов'язаною з певними аспектами безпеки. Наприклад, РЄ займається правами людини і гуманітарним співробітництвом. ЄС бере участь у вирішенні економічних проблем; лише ОБСЄ займається всім комплексом питань, пов'язаних з забезпеченням безпеки в Європі.

Інформація потребує до себе серйозного ставлення, оскільки є інтелектуальним багатством країни та її громадян, ресурсом суспільства, який не повинен витрачатися неефективно. Залучення інформаційних технологій створило нові можливості для ефективного розвитку економіки, політики, суспільства, громадянина. А інформаційний вплив на державу, суспільство, громадян сьогодні є ефективнішим ніж політичний, економічний і, навіть, військовий.

3.2. Європейська стратегія боротьби з інформаційним тероризмом

Європейський Союз, як найвпливовіша інтеграційна структура на європейському континенті, відіграє важливу роль в забезпеченні європейської безпеки. Після Другої світової війни Європа отримала неповторний історичний досвід створення та розвитку наднаціональних органів і єдиного правосуддя. Пізніше ЄС набув повноважень і засобів забезпечення безпеки у багатьох невійськових сферах, але дуже чутливих до нових загроз, зокрема співробітництво у сфері юстиції і внутрішніх справ, спрямоване на боротьбу з тероризмом.

У міжнародних відносинах тероризм становить гостру загрозу міжнародній безпеці, дестабілізує відносини між державами і групами держав та провокує міжнародні конфлікти. Тероризм виступає як інструмент втручання

у внутрішні справи держави, грубо порушує права людини, міжнародний правопорядок. Принципово нові загрози міжнародній стабільності виникли з розробкою, використанням і розповсюдженням інформаційної зброї, що уможливлює інформаційні війни та інформаційний тероризм [10; 41; 263; 324-330].

У зв'язку з рівнем інформаційно-технічного розвитку Євросоюзу, особливого значення в діяльності ЄС набула проблема забезпечення інформаційної безпеки. Спільна позиція країн-членів Європейського Союзу щодо змісту поняття «інформаційна безпека» була висловлена представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН, згідно з якою інформаційна та мережева безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці.

Позиція з приводу інформаційної безпеки відзначається раціоналізмом, адже предметом безпеки називаються конкретні поняття різних видів інформації. Крім того, простежується досить чітке розмежування особливостей. У рамках інформаційного забезпечення національної безпеки, захисту особистої інформації є боротьба з кіберзлочинністю, оскільки це особливо актуальна проблема для країн Європи.

Глобалізація сучасної економіки, її насиченість новітніми інформаційно-телекомунікаційними технологіями, інформатизація таких життєвоважливих сфер діяльності суспільства, як зв'язок, енергетика, транспорт, системи зберігання газу та нафти, фінансова та банківська система, оборона та національна безпека, структури забезпечення стабільної роботи міністерств та відомств, перехід на методи електронного врядування створюють умови для розповсюдження кібертероризму. Сучасні війни ведуться насамперед в інформаційній сфері, яка випереджає і безперервно супроводжує так званий "прямий контакт" протиборчих сторін. Спецслужби ведуть свої війни безпосередньо в Інтернеті. Як повідомлялося, для боротьби з потенціальним супротивником в експортне мережеве обладнання США встановлюються чіпи з логічними вірусами, які можуть бути активізовані в потрібний момент. Для боротьби з певними людьми є комп'ютерні програми обнуління банківських рахунків та багато чого іншого. За даними аналітичних центрів США, розробки нової інформаційної зброї відбуваються у 120 країнах світу.

Велику занепокоєність експертів-аналітиків викликає той факт, що терористичні організації більш гнучкі, аніж державні інституції щодо застосування технічних інновацій [331-332]. Відповідно вони мають суттєві переваги

у проведенні добре координованих операцій. А високий ступіть організації та реалізації останніх резонансних терористичних актів свідчить, на думку деяких експертів, про те, що за злочинами стояли інтереси різних держав.

З цією метою терористи використовують технічні засоби, які знаходяться у вільному продажу та об'єкти інфраструктури країни перебування. Простежується також їх зв'язок з великими потоками нелегальних, в першу чергу кримінальних грошей. На шостому засіданні Робочої групи зі співробітництва правоохоронних органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю (Монстер, 28-30 серпня 2000 р.) оприлюднили дані Інтерполу про те, що прибутки комп'ютерних злочинців у світі посідають третє місце після прибутків наркодилерів та нелегальних постачальників зброї.

Інтенсивність кібератак в сучасному світі невпинно зростає. У 2002 р. радник президента США по технологіям Ричард Кларк оголосив список країн – потенційних носіїв кібертероризму. До нього потрапили Ірак, Ірак, Південна Корея, Китай та Росія. За переконаннями Кларка в цих країнах є спеціалісти, здатні порушити безпеку США через Інтернет [325; 333]. Проте, за даними фірми Riptech, кібератаки з небезпечних для США країн становлять 1%, а найбільша кількість атак - 40% зафіксована за самими США. Далі за кількістю нападів йдуть Німеччина та Південна Корея. Зазначимо, що нині США мають 42% світових комп'ютерних ресурсів та 60% ресурсів Інтернету, Китай – 1%, Росія – 1%, а Україна – менше 1%.

Кібертероризм є частиною такого явища, як інформаційний тероризм. У середині 1980-х рр. Беррі Коллін, співробітник американського Інституту безпеки і розвідки, ввів термін „кібертероризм „ для визначення терористичних дій у віртуальному просторі. Автор терміну зазначив, що про реальний кібертероризм можна говорити не раніше, як у першому десятилітті XXI ст. Проте вже у 1990 р. було зафіксовано перші серйозні кібератаки. А згодом Пентагон наказав Агентству супутникових телекомунікацій розробити стратегію ведення кібервійни (OPLAN 3600), яка передбачає «безпрецедентне об'єднання комерційних і державних структур країни». До її розробки залучається і ФБР, оскільки ситуація вимагає рішучого об'єднання усіх зусиль для протидії можливим атакам через Інтернет. Уряди європейських країн теж розпочали розробку своїх стратегій ведення інформаційної війни.

Термін „кібертероризм" означає дії з дезорганізації інформаційних систем (несанкціоноване втручання в комп'ютерні мережі, перепрограмування, порушення роботи серверів та інше), що становлять небезпеку для життя людей, призводять до значних майнових збитків, або інших суспільно небезпечних наслідків, якщо їх здійснено з метою порушення громадської безпеки, залякування населення або впливу на прийняття рішення органами влади, а також загроза здійснення зазначених дій. Головне в тактиці інформаційного тероризму полягає в тому, що терористичний акт мав небезпечні наслідки, був широко відомий населенню і викликав потужний резонанс у суспільстві. Ви-

моги терористів супроводжуються погрозами повторення акту без зазначення конкретного об'єкту. Таким чином, характерною особливістю кібертероризму є те, що на відміну від кіберзлочинності, умови терориста широко висвітлюються в інформаційній мережі.

Діяльність кібертерористів виявляється в загрозі насильства, підтримці стану залякування з метою досягнення політичних та інших цілей, примусі до певних дій, притягненні уваги до особи терориста та терористичної організації, яку він репрезентує. Використання злочинними елементами новітніх інформаційно-комунікаційних технологій надзвичайно небезпечно. Вони радикально змінюють методи терористичної діяльності, сприяють екстремістським елементам у формуванні гнучких та ефективних мережевих організаційних структур, що об'єднують окремі групи у транснаціональні терористичні угрупування, які дуже важко виявити до здійснення терористичного акту. За багатьма ознаками мережеві організації подібні до стільникової структури, що складається з декількох груп, які мають різних лідерів або різну спрямованість. Водночас вони здатні об'єднуватися для вирішення спільних завдань. Зазначена структура може існувати тільки в умовах інформаційно-розвиненого суспільства.

Кібертероризм ще не призводив до людських втрат, але спричиняв суттєві фінансові збитки та впливав на психологічний клімат у суспільстві.

Таким чином, кібертероризм є одним з сучасних викликів високотехнологічним державам світу. Фахівці вирізняють наступні засоби тероризму у кіберпросторі для досягнення терористичних цілей:

- завдання збитків окремим фізичним елементами кіберпростору, зокрема, знищення мереж електроживлення, використання спеціальних програм, що стимулюють руйнування апаратних засобів, а також біологічних та хімічних засобів для порушення елементарної бази;
- знищення або крадіжка інформаційного, програмного та технічного ресурсів кіберпростору, що мають значення для суспільства в цілому, шляхом порушення систем захисту, встановлення вірусів, програмних закладок та інше;
- вплив на програмне забезпечення та інформацію з метою їх викривлення та модифікації в інформаційних системах та системах управління;
- розкриття та загроза оприлюднення або оприлюднення закритої інформації про функціонування інформаційної інфраструктури держави, принципів роботи системи шифрування, успішного досвіду проведення актів інформаційного тероризму;
- загрози здійснення терористичного акта у кіберпросторі, що викликають серйозні економічні наслідки;порушення ліній зв'язку, неправильне адресування, штучне перевантаження вузлів комутації та інше;
- вплив на операторів, розробників, експлуатаційників інформаційних та телекомунікаційних систем шляхом насильства або загрози насильства, шантаж, підкуп, введення наркотичних засобів, використання гіпнозу, засобів створення ілюзій, мультимедійних засобів та інше;

— проведення інформаційно-психологічних операцій [41].

Основною формою кібертероризму серед вищезазначених є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури. Здійснення кібератак призводить до втручання в систему, перехоплення управління, або блокування засобів обміну в мережі та інше. Війна проти Югославії стала першою в історії інтерактивною війною — всі, хто мав доступ до Інтернет, в будь-який момент часу мали можливість спостерігати за розвитком збройного конфлікту. Вперше в історії збройних конфліктів хакери використали мережу проти ведення військових дій як Югославії, так і НАТО, шляхом порушення роботи урядових комп'ютерів та встановлення контролю над сайтами.

Втручання в мережі, обладнані комплексами захисту, надзвичайно складне завдання, яке не під силу здійснити самим терористам, що не мають необхідних знань та кваліфікації. Проте, маючи відповідні фінансові кошти, вони в змозі найняти для цього хакерів. Хакерством називають експлуатацію комп'ютерів витонченими засобами за допомогою спеціального програмного забезпечення. Небезпека кібертероризму в тому, що він не має національних меж і терористичні акти можуть відбуватися з будь-якої частини світу. Терориста дуже важко виявити, тому що він діє через один або декілька підставних комп'ютерів.

Цілі, що переслідують для своїх атак терористи, відповідають в цілому складовим національної інфраструктури: обладнання, в тому числі комп'ютери, периферійне, комунікаційне, теле-, відео-, та аудіо обладнання; програмне забезпечення; мережеві стандарти та коди передачі даних; інформація як така, що може бути представлена у вигляді баз даних, аудіо-, відеозаписів, архівів та інше; люди, які діють в інформаційній сфері. Групи цілей (мішені) кібертерористів — це міжнародні організації (цілі кібератак учасників антиглобалістського, антивійськового рухів та учасників різних військових конфліктів), вищі органи виконавчої та законодавчої влади, установи економічного блоку та університети окремих держав (цілі суб'єктів політичного, соціального та інших форм протесту), громадські організації (цілі носіїв релігійної, національної та інших форм ворожості) та банківські і фінансові структури (цілі суб'єктів кримінальної діяльності).

Незважаючи на те, що здійснення таких атак вимагає високої кваліфікації від їх виконавців, інколи кібертерористичні дії можуть виявитися зручнішими для її замовників, ніж акти звичайного тероризму. Адже проведення кібератак забезпечить високу ступинь анонімності і вимагає більше часу на реагування. Подекуди атаки через інформаційні системи залишаються непізнаними як терористичний акт — їх сприймають як випадковий збій у системі.

Інформаційні атаки високого рівня, що кваліфікують, як акти кібертероризму, можна розподілити на дві категорії. Це виведення з ладу інформаційних систем та руйнівні атаки. Кожна категорія виокремлюється, але

чітких меж між ними немає. Одна особа, або терористична група може здійснювати одночасно весь спектр дій. Діяльність кібертерористів аналізуються виходячи з міркувань її небезпеки для суспільства. Найбільшу загрозу становлять дії, спрямовані проти об'єктів критичної інфраструктури – командних пунктів ядерних сил, систем управління АЕС, промислових підприємств, транспорту. Порушення, чи блокування їх роботи може установити миттєву загрозу для життя багатьох людей.

У контексті даної статті переважно розглядаються політично мотивовані атаки на інформацію, що обробляється комп'ютером, комп'ютерні системи та мережі, що становить небезпеку для життя та здоров'я людей, здійснені з метою порушення стабільності у суспільстві, залякування населення, провокації військового конфлікту . Наведені приклади діяльності терористів в інформаційному просторі показують широкий діапазон використання електронних засобів впливу, різні цілі, гравців та географічні діапазони [334-337].

1. Виведення з ладу інформаційних систем.

Хакерські атаки цього типу є найбільш поширеними; вони спрямовані на тимчасове виведення з ладу окремих Інтернет-служб, переадресацію інформації. Вони зазвичай проводяться *„тимчасовими терористами"* – приватними особами, які не пов'язані напряму з терористичними організаціями, але поділяють опозиційні ідеї.

Існує багато способів, за допомогою яких певна особа може порушити, або припинити роботу Інтернет-серверів (в основному це DOS-документи). Белградські хакери в період війни в Косово організовували атаки проти серверів НАТО. Вони бомбардували сервери командами, які перевіряли, чи працює сервер і чи пов'язаний він з Інтернетом. Очікуваним ефектом таких атак було перевантаження лінії сервера – мішені. Косовські хакери, як засіб віртуального протесту, використовували бомбардування електронної пошти. Вони надсилали політикам тисячі листів одночасно за допомогою автоматизованих інструментів, що часто призводило до блокування електронної скриньки і вона припиняла роботу. Американські засоби масової інформації писали, що Косовський конфлікт перетворив кіберпростір в нематеріальну військову зону, де військові зіткнення відбуваються через електронні зображення, групові поштові відправлення та хакерські атаки.

На думку Дороті Денінг, автора дослідження „Активність, хактивізм та кібертероризм: Інтернет як засіб впливу на зовнішню політику", Інтернет вплинув на політичний діалог, тому що активно експлуатувався активістами, які мали на меті тиснути на осіб, відповідальних за прийняття політичних рішень[338].

2. Руйнівні атаки.

Насамперед, це інформаційні (хакерські) операції проти об'єктів, які здатні знищити інформаційний ресурс, лінії комунікації, або викликати фізичне знищення структур, що включають інформаційні системи. Якщо системи діють у критичних інфраструктурах, то при найгіршому розвитку подій мере-

жеві інформаційні атаки можуть мати масштабні наслідки з людськими жертвами, як і традиційні терористичні акти.

Саме такі кібератаки були організовані в трагічний день 11 вересня 2001 р., що уможливило на деякий час «засліпити» операторів авіарейсів, баз ВПС тощо. Вони не оголосили своєчасної тривоги лише тому, що «картинка» на екранах їх комп'ютерів відповідала «нормі», хоча й не мала нічого спільного з тим, що відбувалося насправді. Близькою за формою до військової була атака на цілу низку серверів державних установ США, яку здійснили китайські хакери в період війни в Югославії.

У 1999 р. відбулося бомбардування силами НАТО китайського посольства в Белграді, були жертви. Після цієї події розлючені китайські хакери зламали декілька американських урядових сайтів. На сайті американського посольства в Пекіні було вміщено гасло, в якому американці називалися варварами. Водночас на сайті департаменту внутрішніх справ хакери розмістили фотокартки трьох вбитих під час бомбардування журналістів, пекінських демонстрацій проти війни та зображення китайського прапора. Газета "*Washington Post*" опублікувала заяву представника департаменту внутрішніх справ США, в якій зазначалося, що експертам вдалося знайти слід хакера, що вів до Китаю. Газета писала про заяву, розміщену на сайті міністерства енергетики США: "Протестуємо проти нацистських діянь США! Дайте відсіч нелюдським діянням! Ми, китайські хакери, не причетні до політики. Але ми не можемо спокійно споглядати вбитих китайських репортерів — вам відомо ким."

Після трагічного випадку Китай призупинив військові контакти з США на вищому рівні. НАТО не припинив військові дії в Югославії. Уряд США офіційно вибачився за дії військових, виправдовуючи їх помилковою інформацією розвідки, використанням старих карт, в результаті чого переплутали споруду з військовим об'єктом. Бомбардування вплинуло на зовнішню політику більше, ніж атаки хакерів. Але кібертерористи вирішили своє завдання, а саме — порушили роботу державних установ та здійснили інформаційний вплив на політичну еліту, користувачів мережі Інтернет всіх країн світу, що є ціллю будь-якого тероризму, зокрема інформаційного.

Хакерський рух в Китаї організовано на державному рівні. Зокрема, Китай дозволив своїм кібертерористам об'єднатися в Honker Union of China (*honker* — гібрид англійського «*hacker*» і китайського «*hong*» — червоний).

Є багато прикладів кібератак, що наочно демонструють потенційні можливості тероризму в інформаційному просторі, практично не відрізняються за можливими наслідками від дій звичайних терористів. Так, на Ігналінській АЕС у 1995 р. програміст змінив програмне забезпечення системи безпеки одного з реакторів з метою шантажу. Тільки завдяки організації співробітниками станції вдалої протидії вдалося запобігти трагедії у густонаселеному районі Європи. В атомній енергетиці зміна інформації або блокування інформаційних центрів може призвести до ядерної катастрофи .

Ядерний шантаж – специфічна форма кібертероризму, яка дестабілізує суспільство. На початку 1999 р. через мережу Інтернет на адресу урядів 20 країн світу було відправлено лист від офіцерів російської ракетної військової частини, яка розташована в м. Козельськ Калузької області і має на озброєнні стратегічні ракети шахтного базування. В листах зазначалося, що офіцери незадоволені принизливим становищем Росії та погрожували здійснити запуски ракет по цілях, розташованих в столицях та великих центрах західних країн. Крім того, аноніми вимагали виплати великої грошової компенсації. Уряди низки країн звернулися до МЗС Росії, висловили своє занепокоєння та прохання знайти шантажистів. Через певний час анонімів знайшли та притягнули до суду. Вони були мешканцями Калуги, до того ж не військовослужбовцями. Суд визнав їх дії, як заздалегідь неправдиве повідомлення про акт тероризму.

Системи супутникового зв'язку та глобальні мережі дають можливість здійснювати атаки практично в будь-якій частині планети. За повідомленнями британських ЗМІ, на початку 1999р. хакерам вдалося захопити управління військовим телекомунікаційним супутником серії „Скайнет" та змінити його орбіту. Стало відомо, що спеціальний підрозділ поліції розпочав розслідування у зв'язку з вимогою виплати певної грошової винагороди в обмін на те, щоб хакери припинили втручатися в управління супутником.

У комерційній сфері серед масштабних зломів комп'ютерних мереж був злом системи захисту та привласнення санкт-петербурзьким хакером Володимиром Лєвіним з нью-йоркського банку „Сітібенк" 10 мільйонів доларів. За даними експертів Ради Європи, тільки афери з кредитними картками щорічно становлять 400 млн. доларів. Збитки від вірусів складають 12 млрд., а порушення прав власності становить 250 млрд. доларів збитків. За оцінками Інтерполу, оголошеними на шостому засіданні робочої групи по співробітництву правоохоронних органів країн Центральної та Східної Європи (м. Мюнстер, 28–30 серпня 2000 р.) з питань боротьби з комп'ютерною злочинністю, прибутки комп'ютерних злочинців у світі посідають третє місце після доходів наркодилерів та нелегальних постачальників зброї.

Комп'ютерні віруси, або черви хакери використовують для поширення гасел протесту або для виведення з ладу комп'ютерних систем. Обидві форми порушують роботу комп'ютера та поширюються по мережі. Віруси з великим руйнівним потенціалом є потужним інструментом в руках кібертерористів. Перша кібератака з використанням черв'яка відбулася у 1989 р. в мережі адміністрації національної аеронавтики і космонавтики США. Вчені побачили на комп'ютерах центру управління польотами НАСА у Грінбелт, штаті Мериленд, вітання :"Черви проти ядерних вбивць. Ви говорите про час миру для всіх, а одночасно готуєтеся до війни". Хакери здійснили спроби призупинити запуск космічного човна, що мав на борту обладнання, яке живилося від радіоактивного плутонію на Юпітер. Джон Макмахон, менеджер НАСА, оцінив втрати від руйнівного черв'яка у півмільйона доларів, марно витраче-

них на ресурси та роботу команди фахівців. Тоді хакери не зупинили запуск. Джерело нападу не було знайдено, але є припущення, що це були австралійські кібертерористи.

Комп'ютерні віруси використовували для поширення політичних заяв і подекуди це мало руйнівні наслідки. В лютому 1999 ізраїльський підліток, який заявив про знищення ним іракського урядового сайту, став національним героєм. Чотирнадцятирічний Нір Зігдон за допомогою спеціального програмного забезпечення відстежив сервер сайту в одній з країн Персидської затоки. За його словами, цей сайт вміщував брехню про США, Велику Британію та Ізраїль. Тель-Авівський хакер відіслав на сайт комп'ютерний вірус в додатку до електронної пошти. Упродовж години сайт було знищено. В період війни в Югославії комерційні структури, громадські організації, академічні інститути країн-членів НАТО отримували електронну пошту з вірусами. Збитки адресати таких листів мали від додатків, зокрема в антинатівському мультику. При цьому реальну загрозу сербські хакери представляли для комерційних установ, а не для краще підготовлених військових мереж.

Комерційній організації складно боротися проти вірусу, тому що користувачі відкривають додатки з вірусами та поширюють їх серед колег. Незважаючи на те, що антивірусні програми виявляють та знищують віруси, їх необхідно підтримувати на високому рівні, постійно поновлювати та правильно користуватися. Віруси у листах з політичним змістом здаються на перший погляд не дуже складною проблемою, але робота організації через вірус може призупинитися. Приватні компанії США володіють 80% критичної інфраструктури в США і більшість з них не забезпечує необхідний рівень захисту своїх систем.

Незважаючи на заяви офіційних осіб США про перебільшення загрози кібератак, американці розуміють, що вона реально існує. Ще 7 січня 2000 р. президент США підписав „Національний план захисту інформаційних систем", відповідно до якого було визначено 10 програм:

- визначення критично важливих ресурсів інфраструктури, їх взаємозв'язків та загроз щодо них;
- виявлення нападів та несанкціонованих вторгнень;
- розвідувальне забезпечення та розробка правових актів , спрямованих на захист критичних інформаційних систем;
- своєчасний обмін інформацією про напади;
- створення засобів реагування та поновлення;
- активізація науково-дослідної роботи в цій галузі;
- підготовка кадрів фахівців в сфері інформаційної безпеки;
- внесення необхідних змін та доповнень до національного законодавства;
- забезпечення захисту громадянських свобод.

У результаті було створено широку систему управління критичними об'єктами інфраструктури США. 16 жовтня 2001 р. розпочала діяльність Рада з захисту критичної інфраструктури США, а 14 лютого 2003 р. підписано

розроблену за розпорядженням президента Буша Національну стратегію з підтримки безпеки кіберпростору. Вона базується на усвідомленні того, що з поширенням інформаційних технологій критичні інфраструктури залежать від ефективної роботи мережі, порушення якої може мати непередбачені наслідки.

У стратегії передусім розглядаються питання технічного забезпечення американськими користувачами безпеки своїх ділянок мережі, тобто тих ресурсів, якими вони володіють або користуються. Йдеться про комп'ютерні антивірусні програми, системи захисту *„Файр-уолл"*, підвищення якості освіти. Проте не визначено норми, що регулюють взаємодію учасників у зазначеній галузі (уряд, промисловість, неурядові та інші організації та приватні користувачі). Відсутність таких норм, на думку фахівців, призведе до того, що на практиці стратегія виявиться неефективною. Автор статті погоджується з зазначеними оцінками, враховуючи той факт, що нині жодна держава неспроможна самостійно протистояти глобальним загрозам. Важко підтримувати безпеку національних мереж та відповідну інфраструктуру за умов безконтрольного поширення інформаційної зброї.

Американські стратеги в умовах відсутності всезагального міжнародного підходу до проблеми забезпечення міжнародної інформаційної безпеки і існуючих загроз інформаційного протистояння готують грунт для нанесення контрудару у відповідь на інформаційну агресію. Відповідно до стратегії, США залишають за собою право адекватно реагувати на кібератаки. На думку експертів-аналітиків, існує небезпека, що прагнення розширеного тлумачення поняття тероризму створює загрозу використання тези боротьби з тероризмом, кібертероризмом, зокрема, для збільшення власної військової та інформаційної присутності у світі. Згідно офіційних осіб, США вже сьогодні готові вести інформаційну війну, якщо на країну буде здійснений інформаційний напад.

Викликає занепокоєність те, що в зазначеній стратегії питання міжнародної співпраці не деталізуються та не конкретизуються. У відповідному розділі зазначається, що США планують працювати в рамках міжнародних організацій, щоб просувати, так звану, культуру безпеки, сприяти розслідуванню кіберзлочинів та притягненню до відповідальності винних у їх скоєнні, брати участь у створенні міжнародної мережі для нагляду та оприлюднення відомостей про загрози кібератак або про факти їх здійснення. Щодо розробки будь-якого міжнародного документу в цій сфері, навіть на перспективу, не йдеться.

Європейці також вирішують питання про неправомірне використання інформаційних засобів. Злочини у галузі високих технологій у центрі уваги Ради Європи з 1980-х років. У 1995 р. було прийнято Рекомендації для боротьби проти кіберзлочинності, які закликають налагодити міжнародне співробітництво з зазначених питань. У 1997 р. в рамках Ради Європи було утворено Комітет експертів зі злочинів у кіберпросторі. Комітет досліджував

доцільність та можливості уніфікації і гармонізації законодавств держав-членів ЄС, зокрема, щодо кіберзлочинності. В результаті цієї роботи було підготовлено проект Конвенції Ради Європи *„Про кіберзлочинність"*, який було ухвалено 23 листопада 2001 р. в Будапешті [339-340]. Нині разом з європейськими державами до конвенції приєдналися Канада, Японія, ЮАР та США.

23 листопада 2001 року Україна підписала разом з іншими країнами Європейську Конвенцію про кіберзлочинність. 7 вересня 2005р. Верховна Рада України ратифікувала, а 25 вересня 2005 р. Президент України підписав закон про ратифікацію Конвенції про кіберзлочинність. Конвенція відкрита для підпису іншими державами світу та набула чинності 1 липня 2004 року, після ратифікації документа Литвою.

Конвенцію прийнято у зв'язку із занепокоєнням країн тим, що комп'ютерні мережі та електронна інформація можуть бути використані при кримінальних правопорушеннях. А докази, пов'язані з такими правопорушеннями, можуть зберігатися та передаватися по цих мережах. Крім комп'ютерного хакерства та вірусів, положення Конвенції регламентують (віртуальну) дитячу порнографію і здійснене за посередництвом комп'ютерів шахрайство. Правоохоронні органи країн, які ратифікують Конвенцію, отримають нові повноваження щодо заволодіння даними, перехоплення комунікацій.

Отже, відповідно до цієї Конвенції комп'ютерні правопорушення класифіковані на певні групи. *Перша група* передбачає кримінальну відповідальність за вчинення правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а саме:

- незаконний доступ;
- нелегальне перехоплення;
- втручання у дані;
- 4)втручання у систему;
- зловживання пристроями.

Друга група передбачає відповідальність за правопорушення, пов'язані з комп'ютерами, а саме:

- підробка, пов'язана з комп'ютерами;
- шахрайство, пов'язане з комп'ютерами.

Третя група - правопорушення, пов'язані зі змістом інформації, а саме правопорушення, пов'язані з дитячою порнографією:

- вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
- пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
- розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
- набуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;

- володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

Четверта група включає правопорушення, пов'язані з порушенням авторських та суміжних прав.

Багато з положень Конвенції не обов'язково мають бути імплементовані в повному обсязі. Наприклад, у країнах може виникнути ситуація, коли комп'ютерне хакерство буде здійснюватись шляхом порушення заходів захисту. Проте також можна визнавати хакерством злочин, якщо він здійснюється без зламування системи захисту (наприклад, якщо задіяний комп'ютер не мав системи захисту).

На початку 90-х років XX століття зазначеній проблематиці приділяється значна увага в багатьох державах. Окреслені проблеми перебувають і у полі зору Президента України, Верховної Ради та Уряду України. Стимулом цього виступають також взяті Україною зобов'язання щодо інтеграції у світове співтовариство, у тому числі згідно з Програмою інтеграції України до Європейського Союзу (розділ 13 – "Інформаційне суспільство").

6 грудня 2001 року Президент України підписав Указ № 1193/2001, який передбачає внесення змін у законодавство, що регулює питання боротьби з кіберзлочинами.

З метою організації протидії "*комп'ютерному тероризму*", в тому числі поширенню через глобальні та національні мережі зв'язку ідеології тероризму, пропаганди насильства, війни і геноциду Постановою Кабінету Міністрів України від 14 грудня 2001 р. було розроблено із урахуванням рекомендацій Парламентської Асамблеї Ради Європи заходи щодо боротьби з міжнародним тероризмом. Вони передбачали проекти Законів України "*Про моніторинг телекомунікацій*", "Про захист інформації в мережах передачі даних", "Про регулювання українського сегменту мережі Інтернет". Однак, спроби силових структур (зокрема, – СБУ) напрацювати проекти відповідного законодавства та провести ці законопроекти в Верховній Раді наштовхнулися із-за низки об'єктивних та суб'єктивних причин на опір тих народних депутатів, які вбачають у цьому законодавстві замах на невід'ємні свободи та права людини.

Положення Конвенції Ради Європи „Про кіберзлочинність" знайшли своє відображення в Законі України «*Про внесення змін до Кримінального та Кримінально-процесуального кодексів України*» від 23.12.2004 року, відповідно до якого в розділі 16 «*Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*», викладені у новій редакції статті 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ст. 362 (Несанкціоновані дії з інформацією, яка обробляється в електронно– обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації,

вчиненні особою, яка має право доступу до неї), ст. 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється) Кримінального кодексу України та передбачена кримінальна відповідальність за статтями 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається на комп'ютерах, комп'ютерних мережах або на носіях такої інформації) та 363-1 (Перешкоджання роботі комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку).

Актуальність проблем комп'ютерного тероризму для України подвійна: з одного боку, держава фінансово неспроможна переобладнати свої критичні об'єкти — управління атомними електростанціями, підприємствами хімічної промисловості тощо, з метою їх недосяжності для інтелектуальних диверсантів.

З іншого боку, інформаційна структура, яка нині формується, потребує постійної уваги. З точки зору національної безпеки України в цій галузі існує також негативна тенденція, пов'язана із зростанням технічної та технологічної залежності нашої держави. Практично не розвивається вітчизняне виробництво конкурентоспроможних засобів інформатизації та зв'язку. Інформатизація як державних, так і комерційних структур відбувається переважно на базі західної технології і комп'ютерної техніки.

В Україні інформаційна діяльність поки що не набула належного розвитку. Отже потребують значної уваги проблеми захисту національного інформаційного ресурсу та формування системи протидій терористичної діяльності проти України. Одним з найважливіших аспектів інформаційної безпеки є забезпечення безпеки інформаційного обміну як у спеціальних системах зв'язку, так і в системах зв'язку загального користування. Нині в Україні спеціальні телекомунікаційні системи створені і діють у понад 19 міністерствах і відомствах. Серед них МО України, МВС України, МНС України.

Основою інфраструктури інформаційної безпеки є Державна система урядового зв'язку, що забезпечує надійним безперебійним захищеним зв'язком понад 1000 абонентів урядового міжміського зв'язку та біля 2,5 тисяч абонентів урядового міського та спеціального міського зв'язку. Разом з тим на цей час спеціальні телекомунікаційні системи використовують морально та фізично застаріле обладнання, понад 80 % обладнання майже вдвічі перевищило встановлені строки експлуатації та потребує заміни. Вимагає значного розширення і комплекс телекомунікаційних послуг, що забезпечуються цими системами. Зокрема, швидко зростає потреба органів державної влади і управління у послугах захищеного факсимільного та комп'ютерного зв'язку, пе-

редачі даних. За сучасних умов посилення інформаційного протиборства потребує подальшого удосконалення система захисту інформації у спеціальних телекомунікаційних системах, насамперед переведення їх на апаратуру технічного та криптографічного захисту вітчизняного виробництва. пеціальні Спеціальні телекомунікаційні системи України використовують засоби криптографічного захисту інформації виключно розробки колишнього СРСР (РФ) та переважно виробництва РФ.

Таким чином головні загрози є не внутрішніми, а зовнішніми. Вони створюються іноземними державами, міжнародними терористичними організаціями та іншими угрупуваннями, що користуються нерозвиненістю відповідних державних структур та законодавчої бази. На жаль, відсутня належна державна підтримка фундаментальних та прикладних вітчизняних досліджень у сфері упередження та боротьби з кібертероризмом. Це створює проблеми для України, яка прагне на рівноправній основі увійти до світової інформаційної системи.

Ефективна боротьба з транснаціональною комп'ютерною злочинністю та кібертероризмом – важливий елемент міжнародної безпеки, реальна протидія новим формам тероризму та організованої злочинності.

З огляду на викладене, з урахуванням стратегічного напрямку розвитку України – членства в Європейському Союзі, з метою підвищення ефективності боротьби з кібертероризмом Україні доцільно здійснити наступну систему заходів.

1. Організувати ефективне співробітництво з державами світу, їх правоохоронними органами, а також міжнародними організаціями.

2. Ініціювати підписання регіональних угод як одного з найефективніших інструментів по боротьбі з кібертероризмом.

3. Розробити державну стратегію, концепцію і доктрину по боротьбі з тероризмом.

4. Необхідно мати національний підрозділ для боротьби з кіберзлочинністю та міжнародний контактний пункт для допомоги в умовах здійснення або попередження кібератаки.

5. У відповідності до існуючих законів про боротьбу з кіберзлочинністю та кібертероризмом та згідно діючим міжнародним стандартам і Конвенції Ради Європи про боротьбу з кіберзлочинністю Україні необхідно ухвалити закони про електронну безпеку.

Проблема загальносвітової протидії загрозам інформаційної безпеки поглиблюється у зв'язку з тим, що тероризм повністю перейшов в сферу міжнародних відносин. Відповідно, шляхи створення ефективних систем протидії також знаходяться в компетенції міжнародного права. Створено міжнародно-правовий базис, але, як свідчить практика, ще не досягнуто задовільних результатів. Важливо розвивати національні антитерористичні законодавства та водночас гармонізувати законодавчі системи всіх членів світового співтовариства з урахуванням нових форм тероризму та нових умов . Те-

ристам не треба залишати ніде в світі території правової безвідповідальності. Зокрема, важливо встановити в усіх країнах обмеження щодо неконтрольованого поширення нових інформаційних технологій, шифрувальних кодів, використання яких терористами, як вже зазначалося , призводить до вдосконалення їх організаційної структури та засобів здійснення терористичної діяльності. Важливо не тільки звернути увагу на питання політичного, правового вирішення проблеми, але й здійснити заходи з метою усунення соціально-економічних причин здійснення кіберзлочинів. У наших спільних інтересах шукати шляхи подолання негативних наслідків глобалізації, зокрема, цифрового розриву.

3.3. Культурна ідентичність як чинник інформаційної безпеки розширеної Європи

Глобалізаційні процеси охоплюють усі сфери суспільного життя, зокрема й культуру. Вони постають зовнішніми чинниками, що мають значний вплив на характер та напрями культурних процесів в окремому суспільстві. Ці чинники характеризуються значними деструктивними тенденціями уніфікації культурного простору, порушуючи тим самим перед національною державою проблему збереження власної культурної самобутності на міжнародній арені та підтримки культурної багатоманітності у суспільстві. Дедалі більше поширюються тенденції стандартизації способу існування людини, її матеріальних потреб та духовних пріоритетів, так звана „масова культура". Саме тому актуальним завданням культурної політики на національному та міждержавному рівнях стає спрямування впливу процесів глобалізації на збільшення можливостей розвитку національних культур, що і зумовило зростання уваги до питань культурного розвитку людства. Водночас утверджується усвідомлення культури як вагомого чинника внутрішньосуспільного розвитку, характеру його суспільно-політичних процесів та творчого потенціалу становлення загалом.

Глобалізаційні загрози інформаційній безпеці як складовій національної безпеки держави зумовлені розмиванням уявлення різних прошарків світової спільноти про власну ідентичність щодо етносу, нації чи культурно-цивілізаційної приналежності. Саме ціннісна система є соціокультурною основою сфери безпеки суспільства, що виконує стабілізуючу, інтегруючу та консолідуючу функції.

Одним з основних консолідуючих та інтегруючих суспільство чинників дослідниками визначається культурна ідентичність. Як і визначення специфіки інформаційної безпеки, що ґрунтується на існуванні певного набору світоглядно-ціннісних орієнтацій, цей чинник передусім актуалізує проблему збереження та розвитку культурної самобутності націй. Нині існують два взаємовиключні підходи до оцінки глобалізаційних процесів та проблеми збереження національних культур. З одного боку, глобалізація оцінюється як не-

гативне явище (Т. Адорно, С. Хантінгтон, Дж. Гейтс та інші), що становить загрозу національній самобутності культур під тиском масової комерціалізованої культури, з іншого (А. Перотті, Джагдиш Бхагвати та інші) – сприяє збагаченню культур, міжкультурному діалогу та становленню полікультурних суспільств.

Таким чином, культурна самобутність певного суспільства містить у собі принаймні дві складові динаміки культурних процесів. Внутрішня складова сформувалася під впливом полікультурності та самобутності певного суспільства. В державній культурній політиці це обумовлює необхідність взаємоузгодження державних інтересів консолідації суспільства та культурної диференціації суспільного життя. Зовнішня – включеність у динаміку тенденцій світової культури. Державна культурна політика у цьому напрямі є гарантом безпеки від деструктивних впливів. Отже, культура виступає важливим чинником у системі національної безпеки кожної держави. Проте водночас такий характер розвитку культурного життя актуалізує проблему збереження культурної самобутності націй.

Оскільки поняття „культурна самобутність" вже давно є одним з основних пріоритетів культурної політики міжнародних організацій, то метою даної статті є виявлення взаємообумовленості цього поняття та інформаційної безпеки розширеної Європи.

На Всесвітній конференції ЮНЕСКО з політики у сфері культури (Мехіко, 1982 р.) культурна самобутність визначається як сукупність неповторних і незамінних цінностей, традицій і форм вираження народу, за допомогою яких він репрезентує себе у світовому співтоваристві. Культурна самобутність не лише розширює можливості для всебічного розвитку людини, а й „мобілізуючи кожний народ, кожну групу, спонукає їх черпати сили у своєму минулому, засвоювати елементи інших культур, які сумісні з їхнім характером, і цим самим продовжувати процес творення себе". З вищенаведеного випливає, що процес збереження національної культурної самобутності неможливий без актуалізації творчого потенціалу та адаптивного процесу в актуальному часі. Зокрема, ще у 1981 році у своєму виступі на Всесвітньому симпозіумі з питань науки та культури тогочасний Генеральний директор ЮНЕСКО Амаду-Махтар М'Боу зазначав, що утвердження національної самобутності має вести до довгострокової творчості та „мобілізації животворчих сил традиції з метою підпорядкування сприятливих умов сучасності".

Подальшому визнанню культури як вагомого чинника безпеки нації сприяли програмні матеріали Всесвітньої конференції у Мехіко, де, зокрема, *проголошено культурну автономію невід'ємною складовою національного* суверенітету, а повага, збереження і розвиток національної культурної самобутності було визначено як питання першочергової ваги, оскільки воно відображає спільне прагнення країн, що розвиваються.

Незважаючи на дедалі потужнішу популяризацію ідей демократії та лібералізму — підвалин забезпечення національної безпеки західної держа-

ви, а відповідно, і зміни парадигми культурної політики у бік обмеження повноважень держави у динаміці суспільних процесів, загрози, які несе глобалізація, нині знову актуалізують дискурс щодо функції держави як основного суб'єкта національної культурної політики, її конструктивної ролі у збереженні гуманістичного виміру культури кожного народу як етносоціальної спільноти.

Саме держава є основним гарантом безпеки людини у просторі культури, чим взаємообумовлюється як взаємозалежність безпека держави, суспільства та людини. Усвідомлення культурної самобутності, національної спадщини, історичних коренів та творчого потенціалу суспільства є рушійною силою розвитку держави. Дії держави як суб'єкта культурної політики мають спрямовуватися на збереження, відтворення та творення культурної самобутності нації.

Політика культурного різноманіття відповідає Статуту ООН – головного міжнародного форуму з розвитку культури миру та демократії на основі фундаментальних принципів Організації. На 60-й сесії ГА ООН (14 – 16 вересня 2005 року) було підтверджено зобов'язання підтримувати зусилля міжнародного співтовариства, спрямовані на забезпечення суверенної рівності всіх держав та ефективного міжнародного співробітництва у вирішенні міжнародних проблем економічного, соціального, культурного або гуманітарного характеру. Організація Об'єднаних Націй закликала державичлени визнати різноманітність світу та різноманітність культур і цивілізацій, які збагачують спільну культурну спадщину людства. Ініціативи ООН також спрямовані на забезпечення толерантності, діалогу різних культур, цивілізацій та народів з метою становлення мирного, прогресивного і демократичного світу на основі Декларації та Програми дій у галузі культури миру, Глобального порядку денного для діалогу цивілізацій та його Програми дій, в яких підкреслюється необхідність діалогу між культурами та цивілізаціями, включаючи міжконфесійне співробітництво. Проблема формування культури миру та демократичного управління в полікультурному та багатоетнічному суспільстві також відображені в ініціативі *„Альянс цивілізацій"*, проголошеної Генеральним секретарем ООН 14 липня 2005 року ГА ООН підтвердила, що демократія – це універсальна цінність, вираження вільного волевиявлення народу, який визначає свої політичні, економічні, соціальні та культурні системи, що відрізняються національними особливостями моделей демократії.

До критеріїв демократичного управління в полікультурному та багатоетнічному суспільстві відносять такі чинники як:

- культурне різноманіття як загальна спадщина людства;
- права людини як гарантія культурного різноманіття;
- демократизація управління як чинник співробітництва самобутніх культур та цивілізацій;
- міжконфесійний мир;
- мультикультуралізм та підтримка ідентичності у багатоетнічному суспільстві.

Асиметричний розвиток світу породжує різноманітні виклики для визнання релігійного і культурного різноманіття у глобальних масштабах. Так, культурна самобутність та багатоманітність може стати причиною гострого національного та етнічного протистояння, збройних конфліктів та соціальної напруженості. Зокрема, їх причиною може стати вибір офіційної мови (нова конституція Афганістану), відносини між державою та конфесіями або релігійними віруваннями (суніти та шиїти в Іраку), державна підтримка традиційної демократії (мусульмани у Франції), протести корінного населення проти забруднення довкілля (басейн річки Амазонки в Бразилії), політика імміграції (Велика Британія) або процедура отримання громадянства (ФРН), етнічна війна (Руанда, колишня Югославія). Зважаючи на вплив глобалізації, національні держави, етнічні групи та корінні народи висловлюються проти дискримінаційного міжнародного співробітництва, яке обмежує культурну різноманітність. Викликами для світової спільноти є поширення упереджених політичних "міфів" у міжкультурному середовищі:

- суттєві диспропорції демократичного та культурного розвитку;
- конфліктогенність культурної різноманітності на основі відмінностей культурних;
- культурна різноманітність перешкоджає розвитку глобального суспільства.

Тому, в рамках ООН, представники країн, що розвиваються вимагають поваги до своєї культурної самобутності (історії, видатних осіб, релігійної культури та самобутніх традицій), забезпечення соціальної справедливості, розширення політичної участі країн світу у становленні нового світопорядку без домінування однієї держави, форми політичної системи чи культури. Диспропорції цивілізаційного розвитку, загроза знищення самобутності та ідентичності змушує країни, що розвиваються, висловлювати застереження проти глобальної інтеграції, модернізації та вестернізації.

За статистикою ООН, у 200 багатоетнічних державах нараховується 5 тисяч етнічних та релігійних груп, які в 2/3 країн складають близько 10 відсотків населення. Глобалізація прискорила міжнародну міграцію, наслідки якої особливо виявилися у США, Канаді, Західній Європі, Росії та Латинській Америці тощо.

У міжнародному співтоваристві існують різні підходи до поєднання політики мультикультуралізму та політики однорідної культурної ідентичності національних держав на основі усвідомлення ідеї єдиної загальнонаціональної ідентичності, заснованої на відчутті спільності історії, цінностей, переконань усіх етносів та народів національної спільноти. Визнання етнокультурного різноманіття щодо організованих, політично активних і диференційованих в культурному відношенні груп і меншин розглядалось як загроза державній, політичній та соціальній єдності багатоетнічного суспільства. З одного боку необхідність виборчого виокремлення етнічних груп, резервування для етнічних меншин місць в парламентах, в органах місцевої влади, спеціальні

пільги при працевлаштуванні чи надання права на традиції релігійної етнічної символіки розглядались як порушення принципу рівноправності у суспільстві. З іншого боку більшість держав змогли врахувати інтереси різних етнічних груп і розширити їх культурні свободи без втрат для своєї єдності та територіальної цілісності.

Одним із напрямів політики демократичного управління в полікультурному суспільстві виступає федералізм – система політичної організації, що заснована на гарантованому конституцією балансі між державним управлінням та самоврядністю, має, як правило, два рівні управління – центральну владу та владу територіальних утворень, які користуються автономією в межах своєї компетенції, визначеної конституцією. Ступінь та масштаби автономії коливаються в широких межах: найширші повноваження передбачає демократична система Швейцарії, централізоване управління у федеративній державі практикують Бельгія та Іспанія. Єдину національну ідентичність проголошують Австрія, Німеччина, множинну ідентичність конституційно визнала Швейцарія.

Інші держави поєднують єдину та множинну ідентичність, проголошуючи як національну самобутність, так і плюралістичний характер багатоетнічних суспільств (Іспанія). Здійснюється цілий ряд вражаючих ініціатив по наданню автономії і самоврядування, коли один і той же народ живе по різні сторони національних кордонів (Рада по співробітництву з проблем народу саамі, створена спільно Фінляндією, Норвегією та Швецією).

Федералізм виявляється у симетричних чи асиметричних повноваженнях окремих територіальних утворень щодо центрального уряду.

Політичні заходи, в рамках впровадження концепції федералізму, спрямовані на зменшення ризику політичних конфліктів на грунті захисту культурної самобутності, сприяли попередженню або врегулюванню гострих зіткнень у багатьох країнах та регіонах світу. Політика мультикультуралізму, окрім того, зміцнювала потенціал держав та сприяла соціальній гармонії, посилювала розвиток та збереження різноманітних та взаємодоповнюючих самобутніх культур.

Визнання полікультурності входить до національних, регіональних та глобальних стратегій людського розвитку, які охоплюють:

- забезпечення, участі полікультурних груп в політичному житті;
- політику в галузі релігії та релігійної практики;
- політику в галузі національного права та правового плюралізму;
- політику багатомовності;
- політику подолання соціально-економічної винятковості.

Об'єктивна реальність свідчить, що більшість меншин та інших маргіналізованих груп відсторонені від реальної політичної влади і відчувають свою відчуженість від держави. В деяких випадках така винятковість зумовлена відсутністю в країні демократії або ж обмеженням політичних прав. Навіть в умовах мультикультурної демократії члени таких груп були недостатньо

представлені в органах влади чи обмежені на виборах, що породжує політичну недовіру та соціальну напруженість у суспільстві та прояви агресивного сепаратизму. Водночас моделі полікультурної федеративної демократії можна вважати ефективними механізмами "участі у владі" етнічних груп та самобутніх культурних спільнот. Така форма "участі у владі" забезпечує права полікультурних груп та запобігає порушенню цих прав з боку більшості чи правлячої еліти.

Пропонується дві категорії демократичних механізмів, у рамках яких полікультурні групи та меншини, можуть брати реальну участь в політичному процесі та діяльності державних інститутів:

- передбачає реальну "участь у владі" на територіальному рівні на основі різних форм федералізму. Вони включають створення в державі адміністративно-територіальних одиниць, де меншини користуються значною автономією. Така форма "участі у владі" доречна там, де меншини проживають компактно та мають традиції самоврядування, від яких не бажають відмовлятися;

- передбачає "участь у владі" на основі консоціації, яка забезпечує участь в політичному процесі полікультурних груп, представники яких не проживають компактно або ж не виступають з вимогами автономії чи самоврядування. Консоціація базується на принципі пропорційності: етнічні або культурні спільноти представлені в інститутах держави пропорційно їх відсотку в населенні країни. Досягнення пропорційності вимагає застосування специфічних механізмів і політичних заходів, щоб відобразити інтереси всіх груп, резервування місць та виділення квот в органах виконавчої та законодавчої влади, як це передбачено, наприклад, в Хорватії – для угорців, італійців, німців та інших меншин. Практика участі у владі, ведення переговорів про квоти та місця, що резервуються, може призвести до конфліктів.

Поділ влади за принципом федерації чи консоціації широко практикується у всьому світі: існують приклади успішного застосування як першого, так і другого механізмів. Федералізм створює практичні можливості для вирішення конфліктів в мультикультурних суспільствах на основі інститутів демократичного представництва та збереження культурного різноманіття шляхом відкритого визнання політики різноманітності та полікультурності.

Участь забезпечується у виконавчій, законодавчій і, як правило, в судовій гілках влади. В Бельгії Асамблея й Сенат розділені за мовним принципом – голландська та франкомовна групи, німецькомовна ж група визначена як частина франкомовної. Ключові питання вирішуються більшістю голосів в кожній групі та загальною більшістю в дві третини голосів: у мажоритарних демократіях управляє більшість, а в демократіях консоціативних – більшість всіх груп, що бере участь у владі.

В "асиметричних" федеративних системах влада, що надається окремим територіальним утворенням, виявляється по-різному: деякі регіони мають автономію в одній сфері, деякі – в іншій. Таким чином, федеративні держави мо-

жуть включати в себе низку територіальних утворень на основі визнання своєрідності їх політичних, адміністративних та економічних структур.

Так, майже кожна мирна довготривала та етнічно різноманітна демократія має не тільки федеративний, а й асиметричний характер. Бельгія ділиться на три регіони: Валлонію, Фландрію та район столиці — Брюсселя; два з них були створені за мовною ознакою (Валлонія — для населення, що розмовляє французькою та німецькою мовами, а Фландрія — голландською мовою). Швейцарська федерація також включає різні мовні та культурні групи.

В Іспанії Країна Басків, Каталонія, Галісія та ще 14 районів отримали статус "автономних спільнот" (comunadades autonomas), які володіють широким та різноманітним спектром владних функцій у таких сферах, як культура, освіта, мова та економіка. Для цих трьох історичних регіонів визначені чіткі межі автономії та самоврядування. Баскським общинам у Наваррі надані більші, порівняно з іншими "автономними спільнотами", владні повноваження в галузі податків та витрат. Намагання Іспанії задовольнити вимоги регіонів, які відрізняються один від одного, допомогло пом'якшити конфлікти та стримати сепаратистські рухи, сприяли поширенню у суспільній свідомості розуміння різноманітної ідентичності.

Однак більшість багатоетнічних федерацій, складові частини яких були об'єднані примусово, а управління здійснювалось на основі несправедливого розподілу політичної та економічної влади між ключовими етнічними групами, зазнали краху. Закінчилися провалом спроби створити етнічно "чисті", моноетнічні суб'єкти федерацій (Югославія), оскільки федеративні відносини не мали демократичного характеру, не виражали багатоманітну самобутність, що створило передумови зростанню сепаратизму та політичної дезінтеграції.

Успіх федеративних відносин залежить від чинного законодавства та політичної волі, спрямованої на удосконалення демократичного управління. Важливо, щоб федеральні принципи сприяли врегулюванню основних розбіжностей та одночасно зміцнювали національну лояльність. Наприклад, федеративні структури, які лише задовольняють вимоги створення ексклюзивних моноетнічних "батьківщин" для етнічних груп, можуть негативно впливати на співіснування різноманітних та самобутніх культур. Політичні угоди та поступки спільнотам, що не забезпечують лояльності громадян загальнодержавним інститутам, можуть призвести до відцентрових тенденцій у політичному середовищі та руйнування державності.

Завчасне запровадження асиметричного федералізму зменшує ймовірність загострення сепаратизму, хоча більшість держав остерігаються, що введення самоврядування чи розширення автономії територій може підірвати їхню єдність та цілісність. Зусилля по розширенню представництва та участі різних етнічних груп дозволяють уникнути політичного насилля та сепаратистських акцій.

Права і зобов'язання держав, визначені Міжнародним пактом про громадянські та політичні права надають "всім народам право на самовизначен-

ня. За ним вони вільно визначають свій політичний статус та вільно забезпечують свій економічний, соціальний та культурний розвиток". Але застосування цього принципу щодо громадян незалежних країн та корінних народів має суперечливий характер.

Конвенція Міжнародної організації праці про корінні та общинні народи, прийнята та відкрита для ратифікації в 1989 році, сприяє вирішенню проблем корінних народів та самобутніх етносів у незалежних країнах. Оскільки її підписали лише 17 держав (із європейських лише Данія, Нідерланди та Норвегія), вона не набула чинності і не зобов'язує держави-члени МОП до її імплементації у національні законодавства.

Водночас проблема забезпечення полікультурності та збереження культурної самобутності набула глобального рівня, про що свідчать нещодавні засідання Постійного форуму з проблем корінних народів. Більшість держав – членів ООН вважають за необхідне розглядати кризові ситуації та їх врегулювання під егідою впливової міжнародної організації, враховуючи політичну та правову миротворчу практику ООН [107; 341-358.

Україна як держава-засновниця ООН підтримує зусилля організації з політики різноманітності та збереження культурної самобутності. Владні структури України запроваджують нову прогресивну модель культурної політики, покликану визначити демократичність політичної системи, орієнтованої на забезпечення культурних прав національних меншин країни.

3.4. Вплив розширення НАТО на публічну інтерпретацію проблем європейської безпеки

Роль НАТО в сучасній системі європейської безпеки визначається його функціями оборонного союзу держав-членів та провідної координаційної структури в галузі міжнародної безпеки з допоки невизначеними перспективними функціями. Стосовно розширення альянсу варто вирізняти суто безпековий та власне інформаційний контекст проблеми. Очевидно, що першочергова функція НАТО залишається в незмінному вигляді. Альянс і надалі залишатиметься військово-політичним механізмом, покликаним підтримувати в межах постійно діючої інституційної структури високий рівень політичної взаємодії держав Європи і Північної Америки, що становлять владно-силове ядро сучасної міжнародної системи. Звідси випливає комплекс пріоритетних завдань, якими НАТО керується в повсякденній практиці, включаючи визначення викликів і загроз, відпрацювання засобів і форм реагування на них, забезпечення політичної координації, а також здійснення впливу на прилеглі регіони (так звану напівperiферію), що власне пов'язано з процесами розширення географічних меж діяльності та збільшенням членства в НАТО.

НАТО і європейська безпека. Ідеологія розширення євроатлантичних інституцій ґрунтувалася на концептуальних розробках Ф.Фукуями,

С.Хантінгтона, Е.Тоффлера та інших теоретиків глобального розширення капіталізму, які розглядали розширення західних структур як атрибут глобалізації капіталістичної системи та притаманних їй форм політичного устрою. Від початку 1990-х рр. політичні кола США висували тези про доповнення функцій НАТО активними діями в напрямку поширення демократії, що власне слугувало інформаційно-ідеологічною інтерпретацією нової ролі НАТО. Оскільки ряд західно-європейських держав висловлювали побоювання відносно незгоди Росії з розширенням НАТО, американська дипломатія обстоювала уявлення, що нове призначення Альянсу полягає насамперед у зміцненні демократичних цінностей та інститутів. Проте справжньою метою першої після закінчення «холодної війни» хвилі розширення альянсу було його зміцнення як основної форми військово-політичної співпраці між США та ЄС. Такий розвиток подій гарантував пряму присутність США в питаннях європейської безпеки та закріплював за ними вплив на політику держав Центрально-Східної Європи (ЦСЄ).

Друга фаза розширення НАТО відбувалася за інших умов. Якщо в 1990-х рр. США вдалося переконати уряди європейських держав у доцільності розширення як засобу зміцнення демократичного ладу в країнах ЦСЄ, то після воєнної операції проти Іраку нова інтерпретація цього постулату стосовно держав пострадянського простору вже не виглядала безсумнівною. Друга хвиля розширення НАТО почала дискутуватися з літа 2001 р., відбиваючи корекцію інтересів США відносно практичного використання НАТО. До цього часу США бачили в союзниках по НАТО потенційних учасників воєнних операцій. Президент Б.Клінтон традиційно закликав європейські країни до збільшення частки витрат на спільну оборону. Проте в ході підготовки операції проти Іраку для США було важливішим дістати політичну підтримку, аніж залучати до участі в бойових діях малоефективні бойові підрозділи союзників. Саме ця обставина найбільше позначилася на рішенні залучити до Альянсу сімох нових членів (Болгарію, Естонію, Латвію, Литву, Румунію, Словаччину та Словенію) [359-360].

Важливим наслідком першої, та особливо – другої фази розширення ЄС і НАТО стало фактичне припинення дебатів щодо архітектури європейської безпеки, оскільки зміст цієї проблеми було зведено до визначення стосунків між НАТО і ЄС, а також формату відносин цих структур з Росією. Головною передумовою, що безпосередньо вплинула на зміну уявлень щодо перспектив європейської безпеки можна вважати поступове визначення засад співпраці в галузі безпеки між НАТО та ЄС за формулою «Берлін плюс», а також принципів відносин між НАТО та ЄС і укладення технічних домовленостей. З одного боку, було підтверджено, що НАТО «залишається основою колективної оборони країн-членів», а з іншого – було визнано спроможність ЄС проводити операції з врегулювання кризових ситуацій, у виконанні яких НАТО не бере участь як організація [361].

Для країн-членів ЄС НАТО зберігає привабливість у якості спільної оборонної організації. Попри розходження стосовно деяких "*зовнішніх*" проблем, центральну роль НАТО в питаннях європейської безпеки і вагомий вплив США на європейські процеси міг би послабити лише переконливий розвиток інтеграційних процесів у галузі зовнішньої політики та оборони в межах ЄС. Проте це не означає, що за збереження за НАТО ролі провідної військової структури європейської безпеки, функції НАТО і ЄС будуть збігатися. В цьому контексті розмежування функцій та сфер відповідальності виглядає неминучим.

До 1999 р. гострота полеміки щодо ролі і функцій НАТО гальмувалася відносною синхронністю розширення НАТО і ЄС. На початку XXI століття стала більш очевидною змістовна розбіжність завдань, що висувають ці інституції. Одна з причин — у тому, що за відсутності прямих військово-політичних загроз у межах своєї зони безпосередньої відповідальності ЄС дістав змогу діяти автономно, не залучаючи допоміжні військові можливості Альянсу. Ця суперечність все більш помітна в дискусії про межі просторового розширення НАТО і ЄС, а також про характер і перспективи відносин цих інституцій з Росією.

Проголошення США глобальної кампанії боротьби проти тероризму (2001 р.) та формальне залучення до неї Росії, проведення масштабних воєнних операцій в Афганістані (з 2001 р.) та Іраку (з 2003 р.), поряд зі спробами ЄС розпочати реалізацію Спільної зовнішньої політики та політики безпеки (СЗПБ) можна тлумачити як прояв різних тенденцій. Зокрема, воєнна операція проти Іраку (2003 р.) спричинила кризу механізму атлантичної солідарності та зменшення впливу США на міжнародну політику ЄС. Водночас, провал ратифікації Конституції Європейського Союзу суттєво загальмував процеси політичної консолідації в Європі. Пауза, що виникла, послаблює формування спільних позицій ЄС в сфері оборони і безпеки, але не означає кризи європейського проекту.

Роль основних інституцій, що діють у Європі, й надалі визначатиметься характером відносин між США та ЄС, які відбивають міцність системних зв'язків у межах євроатлантичної спільноти та в ширшому сенсі — відносну стабільність європейсько-північноамериканського цивілізаційного ареалу. Попри значні франко-американські та франко-німецькі розбіжності з проблем безпеки, впродовж 1990-х рр. відносна синхронність в розширенні НАТО і ЄС могла розглядатися як свідчення бажання сторін зберегти єдність "євроатлантичного ядра", принаймні з принципових питань. Цю синхронність, без сумніву, можна тлумачити як суттєву проміжну перемогу тактики США, що зміцнює американську присутність в Європі.

Під цим кутом зору військово-політичні аспекти виглядали як чи не найголовніший з елементів адаптації держав Центральної та Східної Європи до постбіполярної міжнародної системи, хоча насправді це неповною мірою відповідало дійсності. Принаймні, окрім відносно опосередкованих загроз

безпеці, спричинених кризою в колишній Югославії, держави ЦСЄ в 1991 - 2004 рр. не стикалися з гострими проблемами і викликами, що загрожували внутрішній стабільності. Стосовно країн пострадянського простору цей фактор мотивації навряд чи матиме аналогічну привабливість, оскільки поширення євроатлантичних структур на схід може супроводжуватися загостренням локальних конфліктів та посиленням міжнародної напруженості.

Європейські прихильники атлантизму очікують на повернення США до практики погодження принципових рішень з європейськими союзниками, що дозволить їм впливати на розвиток подій. Цей підхід вимагає, аби НАТО залишалася в центрі стратегічного мислення та планування США, й одночасно відігравала роль потенційного засобу кризового регулювання. З іншого боку, членство в НАТО має не заважати спрямуванню зусиль європейських союзників на власні оборонні й безпекові проекти в межах ЄС, включаючи розвиток власних Європейських сил швидкого реагування [360].

До принципових факторів, що визначають владно-силову композицію міжнародної системи, належить стан європейської інтеграції в сфері оборони й безпеки, включаючи рівень практичної готовності сил швидкого реагування ЄС. Міжнародна політика ЄС в цьому плані має виразну специфіку: європейські держави-члени НАТО, традиційно важко сприймають рішення щодо початку нових воєнних операцій, наполягаючи на якомога ширшому застосуванні дипломатичних, превентивних та упереджувальних заходів. Водночас підтримка європейських країн має для США величезну моральну вагу, оскільки без залучення держав ЄС глобальна стратегія США однозначно набуває рис гегемонізму, що полегшує спротив з боку важливих регіональних держав та системних політичних супротивників.

Попри явне невдоволення, урядові кола США були змушені погодитися з планами ЄС щодо створення власних сил швидкого реагування. В якості асиметричної поступки з боку європейців, у першу чергу Німеччини, 11 серпня 2003 р. було формалізовано і закріплено військову присутність НАТО в Афганістані. Адміністрація США також пропонувала поступове розширення ролі НАТО в Іраку за умови, що це не обмежить американське військове та політичне домінування, що забезпечує Центральне військове командування США в Індійському океані. Однак на саміті Великої вісімки в Евіані (2003 р.) європейські учасники відхилили цей план.

Натомість, за ініціативою Франції, ЄС без істотних застережень ухвалив рішення про відправку Європейських стабілізаційних сил до Конго, де відбувалися зіткнення на етнічному грунті. Адміністрація США і тодішній генеральний секретар НАТО Дж.Робертсон не приховували роздратування з цього приводу. Апарат генерального секретаря НАТО взагалі був схильний тлумачили започаткування ЄС окремих місій військового характеру як прямий виклик єдності НАТО, включаючи дублювання функцій та поглиблення розбіжностей між НАТО і ЄС. Натомість французьке політичне керівництво продовжувало обстоювати тезу, що ЄС має беззастережне право здійснюва-

ти військові операції там, де не залучено Атлантичний альянс, й демонстративно тлумачило це як «визнання пріоритетної ролі НАТО». Французька дипломатія підстрахувала свою ініціативу, діставши формальну згоду британського уряду, що було зафіксовано в підсумковій заяві франко-британського саміту в Ле Туке (лютий 2003 р.) [362].

Європейські союзники дорікали адміністрації Дж.Буша за односторонній підхід та надмірне застосування сили. В політичних колах країн ЄС висловлювалися очікування, що незабаром односторонній підхід США буде переглянуто прихильниками багатостороннього реагування, які усвідомлюють, що попри їхню могутність, США зберігають потребу в союзниках, що поділяють спільні переконання.

З точки зору Адміністрації США, стратегія однополярності тлумачить процеси в сфері безпеки як результат певних трансформаційних зрушень (в дусі концепцій «задіяності і розширення», «глобалізації демократії», «просування свободи»). В цьому відношенні, з початку 1990-х рр. можна чи не вперше спостерігати спроби здійснення цілеспрямованого впливу провідної держави на міжнародне середовище, що здійснюються в складній комбінації використання невійськових засобів, включаючи економічні, та примусових санкцій і методів загрози силою аж до її безпосереднього і в деяких випадках масованого застосування [363]. Проте якщо в європейському ареалі цей вплив був порівняно ефективним, доцільність його застосування в інших географічних ареалах викликає істотні сумніви.

Глобальна роль НАТО. Стратегічна концепція Альянсу 1999 р. в дещо приглушених формулюваннях передбачала застосування НАТО як механізму кризового реагування на глобальному рівні. Однак, якщо США наполягають на чіткому скасуванні географічних обмежень зони відповідальності НАТО, то серед членів ЄС лише Великобританія і Франція згодні розглядати свої збройні сили як засіб реалізації певних інтересів поза межами європейського простору [364]. Подібний підхід абсолютно не властивий більшості західноєвропейських країн.

Серед європейців висловлюються міркування, що ініційована США дискусія стосовно корекції функцій НАТО в сенсі глобалізації послаблює міцність Альянсу як оборонного союзу, поглиблюючи його функціональну кризу. В цьому сенсі можна очікувати, що приховані розбіжності між НАТО і ЄС будуть посилюватися. Вже зараз між ними помітне певне суперництво на теренах колишньої Югославії та в питаннях розширення присутності в басейні Чорного моря. Пропозиції щодо розширення діяльності НАТО в чорноморсько-каспійському субрегіоні та розгортання присутності в Центральній Азії, висунуті США й окремими причорноморськими та центральноєвропейськими державами, не викликали однозначної підтримки з боку більшості європейських членів НАТО. Політичні кола країн Західної Європи загалом не поділяють американську неоконсервативну концепцію демократизації «Великого Близького Сходу», ставлення до арабо-ізраїльського конфлікту та ряду інших конфліктів.

Уточнення функцій і завдань НАТО залишається відкритим питанням, принаймні з часу Празького саміту НАТО (листопад 2002 р.), який не дав відповіді на ці питання. Надання НАТО прямої відповідальності за військову операцію в Афганістані (з 2003 р.) розглядалась як перший крок до глобалізації функцій альянсу, що з точки зору європейців може спровокувати небажане загострення відносин з Росією, Китаєм та Індією. Напередодні Ризького саміту НАТО (листопад 2006 р.) предметом дискусії знову став план перетворення НАТО на ширшу організацію глобального рівня, зокрема шляхом залучення до деяких її постійних структур (політичний комітет, комітет оборонного планування) Австралії, Нової Зеландії, Японії та Південної Кореї. Очевидно, що погодження з цими пропозиціями США і Великобританії означало б, з одного боку, подальше розмежування сфер відповідальності НАТО і ЄС, а з іншого — істотне розгалуження функцій НАТО, включаючи надання більшої ваги комітетам і агентствам, відповідальним за проведення воєнних операцій на периферії. Проти перетворення НАТО на глобальну структуру з розширенням зони відповідальності на Азію і Далекий Схід виступили Франція і Німеччина (в порівняно м'якій формі). Франція побоюється прагнення США використовувати НАТО як активний інструмент свого глобального домінування в ключових регіонах світу. В ході підготовки до Ризького саміту цей проект набув ознак створення при НАТО дублюючої структури («НАТО-два»), або ширшої версії альянсу, в якому Японія і Австралія набули б статусу привілейованих партнерів. На думку ряду європейських експертів, подібна концепція провокувала б відновлення силового протистояння в Східній Азії.

Останні тематичні публікації щодо перспектив НАТО зосереджують увагу на потребі визначення її довгострокових перспектив як впливової міжнародної організації. Відзначається, що перспектива можливого членства залишається потужним мотиваційним чинником для країн Кавказу і Балканського півострова. НАТО є ефективним і незамінним засобом для організації взаємодії між арміями країн-членів альянсу, без якого було неможливе б створення ефективної коаліції сил. Крім того, НАТО відіграє ключову роль в забезпеченні ефективного реформування новими членами і партнерами альянсу в Східній Європі свого оборонного сектору.

З іншого боку, НАТО втратив роль *«стратегічної опори»* політики США. Вихід за межі традиційного кола завдань, включаючи проведення довгострокової операції в Афганістані, забезпечив альянс додатковою сферою практичної діяльності, але перетворив, по суті, в багатосторонню інституцію з непостійним складом учасників, що беруть участь у коаліційних силах. Все частіше висловлюються сумніви щодо успіху операції НАТО в Афганістані, яка вийшла далеко поза межі завдань антитерористичної операції та все більше переорієнтується на цілі підтримання мінімальної воєнної стабільності і сприяння державотворенню. Такі теми, як зростання могутності Китаю, ядерні амбіції Ірану і Північної Кореї, доля Близького Сходу — ці проблеми розглядаються переважно поза межами НАТО. Розширення НАТО досягло

тієї «межі, за якою альянс із стабілізуючої сили може перетворитися на чинник дестабілізації окремих регіонів» [365].

Останній аспект безпосередньо пов'язаний з розширенням діяльності НАТО в зоні Причорномор'я і Кавказу. В цьому сенсі позиції США і більшості країн ЄС не співпадають, оскільки на офіційному рівні ЄС дотримується настанови, що будь-яке врегулювання існуючих заморожених конфліктів має відбуватися виключно мирними, політичними засобами. Різне ставлення до проблем субрегіону можна вважати додатковим чинником, що заперечує подальшу синхронізацію розширення НАТО і ЄС.

Починаючи з 1993-1994 рр. в Європі домінували настрої на користь синхронізації цих процесів. У контексті поширення демократії навіть висувалися пропозиції визнати потенційне право на членство в НАТО за кожною європейською державою. Проте, незгода з стратегією США, якщо вона і надалі втілюватиметься без урахування точки зору європейців, та пауза в подальшому розширенні ЄС можуть бути використані урядами низки європейських країн як привід для гальмування розширення НАТО з метою уникнення участі країн-членів ЄС у периферійних збройних конфліктах.

На відміну від цих уявлень, логіка свідомого та прискореного переходу до однополярності, що її дотримується адміністрація США, заперечує тривалу консервацію відносин безпеки в певних проміжних фазах, оскільки це призводить до зменшення ефективності докладених зусиль. З точки зору американської адміністрації, розширення НАТО впродовж наступних декількох років є бажаною, тому що в такий спосіб легше підтримувати імпульс політичного співробітництва з державами Центральної та Східної Європи, який без "політики відкритих дверей" альянсу може поступово згасати. Воєнні операції в Боснії та Герцеговині, Косово, Афганістані та Іраку були лише локальними силовими проявами цього курсу, оскільки стратегія розширення «демократичного простору» потребує регулярної демонстрації успіхів.

Проте, незахідні великі (Росія, КНР) та, до певної міри, значні регіональні держави (Індія, Індонезія), керуються власними стратегічними уявленнями і розглядають подальшу трансформацію міжнародних відносин принаймні як небажаний чинник, що розширює роль США і НАТО в тих регіонах, де їхня присутність досі була незначною. В цьому сенсі США навряд чи можуть діяти ефективно без підтримки європейських союзників, а також низки регіональних партнерів. В системі, що складається з незалежних держав, навіть найбільш впливова країна завжди буде сприйматися як така, що становить загрозу для інших, оскільки вони не можуть бути впевнені, що ця держава буде використовувати свою могутність розумно та стримано. За свідченням американського дослідника С.Уолта, інші держави за звичай намагаються знайти засоби тримати владу панівної держави під королем, найчастіше за допомогою офіційних чи неофіційних альянсів. Ця тенденція буде гальмуватися, якщо поведінка сильнішої держави буде доброчинною, а її цілі – співпадають з інтересами інших головних держав, однак ніколи не зникне зовсім. «Прагнення таких

держав збалансувати сильніші держави пояснює, чому Франція, Росія та Китай поєднували зусилля з метою присікти політику США по відношенню до Іраку та Сербії, і це лежить в основі принципової мотивації договору про китайсько-російську дружбу... Воно також пояснює, чому європейські держави хочуть укріпити й розширити Європейський Союз, чому президент Венесуели підтримує світове протистояння пануванню США, й чому президент Путін висловив сподівання, що Індія стане великою державою та допоможе знову відтворити «багатополярний світ» [366]. З іншого боку, ЄС, Росія, Китай або впливові регіональні держави мають доволі обмежений вплив на глобальну міжнародну систему. Як відзначав С.Уолт, якщо ставити питання в контексті спроможності здійснювати цілеспрямований, свідомий вплив на міжнародні відносини та процеси, такий потенціал зараз мають лише США [366].

На основі аналізу ситуативних чинників можна стверджувати, що попри скасування чинників балансу сил на глобальному рівні, в окремих регіонах, де стикаються інтереси США, Росії, Китаю, Індії та Японії продовжує діяти тенденція до формування регіональних балансів сил, які, однак, не мають значної міцності, хіба що за винятком американсько-японського пакту безпеки. Тому відносини між США / НАТО та Росією, між США, Японією і Китаєм, а також відносини США з Індією і Пакистаном матимуть значний ступінь автономії, що зумовлено відмінним сприйняттям цими державами політичних і економічних загроз.

Інформаційно-політичні аспекти у відносинах Росія – НАТО. Інший важливий аспект, що став предметом дискусії, стосується еволюції відносин між НАТО і Росією. Досі офіційна позиція НАТО полягала у поширенні «крок за кроком» зони стабільності і миру в ЦСЄ за рахунок прийняття нових членів, розвитку програми *"Партнерство заради миру"*, нових ініціатив і програм та партнерства з Росією. За умов критичного послаблення Росії в 1990-х рр., принаймні в економічному і фінансовому плані, її позиція стосовно прийняття до НАТО нових членів якщо і враховувалася, то дуже опосередковано. Теперішня роль Росії, що визначається спробами набути статус енергетичної наддержави, спричинила на Заході гостру, але далеко мотивовану критику. Очевидно, що російські владні кола сприятимуть максимальному відновленню Росією функцій суверенітету як у внутрішніх справах, так і в питаннях міжнародних відносин. Новий прагматичний курс Росії супроводжується посиленням її окремої ролі у відносинах європейської безпеки і передбачає істотний перегляд відносин, в тому числі з сусідніми країнами-партнерами НАТО.

Більш радикальні атлантисти бачать у посиленні Росії прямі причини зупинки розширення НАТО, послаблення зв'язків між США та Європою, затримки з введенням в дію Сил оперативного реагування НАТО. Робиться висновок, що Кремль здобув право вето на розширення НАТО.

Варто визнати, що водночас із існуванням зважених експертних думок, в інформаційному просторі домінують апокаліптичні тези і твердження, які все частіше змальовують ситуацію в Східній Європі в термінах *«холодної*

війни». Можна навести безліч прикладів такого підходу. Лише в одній з останніх публікацій з приводу підготовки Ризького саміту НАТО присутні наступні кліше:

- Могутність США зменшилася, а потенціал Росії зріс; російський газ для Європи як зброя є набагато більш ефективним підривним засобом, аніж комунізм або Червона армія;
- Франція, Греція й інші проросійськи налаштовані країни заперечують вступ Грузії до НАТО, оскільки погоджуються з фальшивим аргументом Кремля, що це порушує сферу впливу Росії;
- Громадська думка України налаштована проти НАТО через пропаганду, яка зображала альянс як мілітаристську кліку, а не як союз успішних і процвітаючих демократій;
- Через монополію Росії на систему трубопроводів такі, як Польща, стають більш уразливими для шантажу з боку Кремля. Коли балтійський газопровід буде побудований, Росія зможе постачати газ до Німеччини, оминаючи Польщу і країни Балтії, які намагаються диверсифікувати джерела поставок енергоносіїв;
- Трубопровід Nabucco - принципово важливий європейський проект через Балкани, призупинений через незацікавленість проросійських урядів, зокрема, в Угорщині і Болгарії;
- Експерти НАТО вважають, що наступним кроком Росії стане створення картелю типу ОПЕК з іншими постачальниками газу, у тому числі з Алжиром, Лівією, Іраном, тощо, хоча досі немає інших підтверджень цієї версії, окрім рамкової угоди між Росією і Алжиром;
- Потрібне розширення повноважень НАТО в сфері енергетичної безпеки і супутніх економічних питаннях. Колективна безпека зараз вкрай необхідна, як і за часів холодної війни, проте «НАТО більше не може її гарантувати» [367].

Можна констатувати, що заповнення інформаційного простору такою відверто конфронтаційною риторикою призводить до викривлення суті процесів, гальмуючи неупереджену і взаємоповажну дискусію щодо сучасного стану європейської безпеки та ролі в ній різних держав та інституцій. Залучення до подібних кампаній України не сприяє дотриманню економічних і політичних інтересів держави, оскільки в першу чергу загрожує принциповим економічним інтересам. Варто зазначити, що домінування конфронтаційної риторики стосовно відносин між НАТО і Росією в американських і європейських ЗМІ негативно впливає на широкий контекст відносин України і з НАТО, і з Росією, попри безумовне врахування того, що газетна полеміка не відбиває офіційних підходів, що стримуються дипломатичним етикетом. Хоча досі російське керівництво запобігало втягненню в адекватні інформаційні кампанії, очевидно, що продовження цієї кампанії здатне істотно погіршити не тільки відносини Заходу з адміністрацією В.Путіна, але й надовго зіпсувати стосунки Росії з НАТО і Заходом у цілому.

З точки зору інтересів України найгірше полягає в тому, що інформаційно-ідеологічна війна змушує владні кола та громадськість перебувати на межі штучно провокованого протистояння, що вимагає або ухилятися від участі в полеміці, або опосередковано ставати на бік однієї з сторін.

Проблемні питання в контексті перспектив членства України в НАТО. Постановка питання про імовірне членство України в НАТО має передбачати ряд важливих уточнень і узгоджень:

- Дотепер не досягнуто визначеності в питанні про те, наскільки керівництво Альянсу і країни-члени НАТО готові розвивати співробітництво з українським сектором оборонної промисловості. Орієнтація на НАТО і США означає втрату для українського ВПК важливих ринків збуту в ряді країн, що не є союзниками чи партнерами США, включаючи КНР, Іран, Малайзію тощо. Також залишається проблемою встановлення таких організаційних форм для українських підприємств ВПК, які дозволили б їм відносно автономно співпрацювати з закордонними партнерами.
- Вважається, що до завершення в основному військової реформи Україна не буде повною мірою відповідати критеріям членства в НАТО. Проте цей чинник може бути в цілому залагоджений внаслідок створення в Збройних Силах України Об'єднаних сил швидкого реагування, як це передбачає План дій Україна – НАТО.
- Повною мірою не з'ясоване питання про те, чи вважається перебування бази російського ВМФ у Севастополі перешкодою для членства України в НАТО. (У 2003 р. з боку США була зроблена заява, що оскільки американо-російські відносини більше не розглядаються як конфронтаційні, перебування російської бази в Криму не буде тлумачитися як перешкода для вступу України в НАТО. Однак доки ця теза є достатньо сумнівною та дискусійною, оскільки Пентагон продовжує розглядати Росію в якості потенційного супротивника).
- Членство в НАТО передбачає наведення ладу в оборонній сфері, впорядкування складів боєприпасів та може передбачати істотне збільшення військових витрат.
- Помітна тенденція до розширення діяльності НАТО в зонах конфліктів поза межами Європи і простору Північної Атлантики (Афганістан, Ірак).
- На сьогоднішній день роль НАТО у світовій політиці не представляється остаточно визначеною. Можливо, Альянс буде приділяти основну увагу питанням безпеки у визначених кризових регіонах, однак також очевидно і те, що в континентальній Європі, за винятком хіба що Причорномор'я та Каспію головні функції безпеки перейдуть до Європейського Союзу.
- Набуття членства в НАТО потенційно підвищує загрозу терактів з боку Аль-Каїди та інших радикальних ісламістських угруповань. Тому при на етапі набуття членства України в НАТО має бути всесторонньо вивчене

і зважене питання про те, наскільки новий блоковий статус України реально впливатиме на стан безпеки країни в плані посилення терористичної загрози та потребує вживання додаткових запобіжних контртерористичних заходів. Універсальних методів боротьби проти тероризму не існує, однак деякі методи все-таки можна назвати. Це достатньо обережне і якісне здійснення зовнішньої політики, ефективність розвідки і спецслужб, охорона потенційно небезпечних об'єктів, виняткова твердість при проведенні контртерористичних операцій.

- Офіційно, з точки зору НАТО, територіальні претензії вважаються за перешкоду щодо набуття членства в Альянсі. Проте ця стандартна вимога не завадила Латвії та Естонії вступити до НАТО і ЄС без укладення договорів про кордони з Росією. Більш того, уряд Латвії висуває політичні претензії на Питаловський район Псковської області РФ. Отже, в разі потреби Брюссель може заплющити очі на явне порушення стандартних критеріїв членства в Альянсі.

Що стосується України, досі не вирішено три питання, що пов'язані з прикордонним та територіальним врегулюванням – визнання лінії морського кордону в Керченській протоці, розподіл територіальних вод і морського шельфу в Азовському морі та континентального шельфу Чорного моря в зоні румуно-українського кордону.

Попри всі розбіжності можна констатувати, які Північноатлантичний альянс залишатиметься військовою основою європейської системи безпеки. В цьому плані, ряд чинників роблять Україну не споживачем, а донором трансатлантичної системи безпеки.

До них належать:

- Потенційно вагома роль України у врегулюванні придністровського конфлікту.
- Підтримання достатньо високого рівня співпраці з державами Причорномор'я та Прикаспію, в тому числі – з Грузією та Азербайджаном.
- Участь в операціях та збройних силах НАТО на Балканах.
- Спроможність формувати боєздатні контингенти для участі в операціях з реагування на кризи в регіонах поза сферою традиційної відповідальності НАТО.

Політичні та галузеві аспекти в відносинах між Україною і НАТО. Будучи основою спільної офіційної платформи та демократичних цінностей Альянсу, політичні питання знаходяться в центрі уваги країн-членів НАТО. Питання внутрішньої політики користуються найбільшою увагою членів Альянсу, зокрема, їх законодавчих органів – при обговоренні питань ратифікації протоколів про вступ. Перелік основних вимог зводиться до наступного:

- зміцнення демократичних і виборних інституцій;
- зміцнення повноважень та незалежності судової влади;
- сприяння розвитку і зміцненню громадського суспільства, верховенству права, захисту основних прав людини і громадянських свобод;

- забезпечення свободи віросповідання та свободи зібрань;
- завершення адміністративної реформи;
- забезпечення рівноваги між трьома гілками влади законодавчою, виконавчою та судовою шляхом конституційних і адміністративних реформ і забезпечення їхньої ефективної співпраці.

Стосовно внутрішньо-політичних аспектів набуття Україною членства в НАТО, вступові до Альянсу мають передувати заходи щодо поширення в середовищі української громадськості позитивних уявлень про діяльність та роль НАТО, з акцентом на ті позитивні чинники, які Україна може здобути в разі набуття членства. Оскільки офіційні стандарти НАТО передбачають спільні цілі та цінності, в зовнішньо-політичній пропаганді варто продовжувати акцентувати увагу на втіленні в Україні норм і принципів демократії і ефективної ринкової економіки.

Економічні вимоги до членства в НАТО визначаються тим, що обороноздатність країни пов'язана з її економічними ресурсами. Головними економічними пріоритетами для України, що прагне набуття членства в НАТО, є: ринкові реформи та макроекономічне зростання; підтримка довгострокової стабільності та добробуту.

Ці два завдання суттєво не відрізняються від вимог до членства в ЄС, вони більш важливі для Європейського Союзу, ніж для НАТО. Проте, є і третій пріоритет: країна повинна бути здатною довгий час виділяти та правильно розпоряджатися необхідними ресурсами, які відповідали б її економічному потенціалу та завданням оборони — оскільки в галузі оборони немає довіри без можливостей, а можливостей — без ресурсів.

Підготовка до інтеграції в систему безпеки НАТО провадиться в контексті оборонної реформи. Спектр оборонної реформи не обмежується лише питаннями військової реформи та реформи збройних сил. Це, по суті, перебудова усього державного механізму, пов'язаного із гарантуванням безпеки. Оборонна реформа передбачає створення нової структури збройних сил з урахуванням масштабів терористичної загрози. Передбачається також вирішення нагальних питань, пов'язаних з воєнно-промисловим комплексом. Вважається, що українська армія та військова інфраструктура досі не відповідають стандартам НАТО через неефективну систему управління, застарілі озброєння і військову техніку.

У контексті перспектив членства в НАТО особливу проблему становить перебування в Україні російського Чорноморського Флоту. Українське керівництво усвідомлює ризики, пов'язані з перебуванням на українській території іноземної військово-морської бази. Перебування в Україні ЧФ Росії опосередковано містить загрозу терористичних актів. База російського ЧФ позначається на розвитку Севастополя, не даючи можливості його перетворення на повноцінний морський торгівельний порт і туристичний об'єкт. Перебування іноземної військово-морської бази на території України являє значну перешкоду на шляху України до НАТО. При гіпотетичному сценарії

воєнного конфлікту Росії з США чи НАТО Україна вимушено прив'язується до позиції Москви та має підтримувати нейтралітет, не маючи впевненості, що його визнаватимуть обидві сторони потенційного конфлікту. Перебування ЧФ Росії впливає і на політичну ситуацію в Криму та Севастополі. Наявність бази російського флоту в Криму дозволяє Москві здійснювати військовий контроль над морськими комунікаціями України. Таким чином, базування ЧФ у Криму залишається засобом утримання України в зоні військово-політичного впливу Росії.

Очевидно, що умови діяльності бази ЧФ у Криму будуть істотно обмежені. Проте поки що важко передбачити, скільки часу можуть зайняти відповідні переговори та узгодження. Водночас, внаслідок значної, в першу чергу, економічної взаємозалежності, для Києва принципово важливо зберегти неконфронтаційні та взаємовигідні відносини з Росією.

Вагомим політичним елементом в діалозі з Росією має бути визначення чітких політичних принципів та підходів, в тому числі — неворожого ставлення до Росії з боку України в разі її вступу до НАТО (на відміну від позиції, яку останнім часом декларували уряди країн Балтії).

У контексті підготовки України до членства в НАТО варто навести деякі найбільш типові висловлювання зарубіжних експертів з цього приводу. Більшість американських державних діячів та політичних аналітиків висловлювали загалом прихильне ставлення до євроатлантичних перспектив України. Водночас переважна більшість коментаторів робили акцент на необхідності послідовного демократичного реформування політичної системи, що дозволяє свідомо уникати визначення строків вступу України до НАТО. Більшість експертів наголошували на необхідності активізації участі України в програмі НАТО "*Партнерство заради миру*", модернізації української армії, вдосконалення цивільного контролю над військовою сферою, впровадження демократичних стандартів, тощо.

Найбільш зацікавлено до членства України в НАТО ставилися Пентагон та ряд депутатів з «*українського фокусу*» в палаті представників Конгресу США, які мало зважають на заперечення з боку Росії та стриману позицію Франції, ФРН, Іспанії та Бельгії. Взимку 2005 р. Пол Вулфовіц (в ранзі заступника міністра оборони США) назвав три роки як можливий термін, необхідний для підготовки вступу України в НАТО.

Водночас колишній міністр оборони США (за адміністрації Б.Клінтона), проф. Стенфордського університету Уїльям Перрі вважав питання про вступ України до НАТО передчасним. До тих пір "багато що може бути зроблено (Європою) для зміцнення відносин з Україною, що допоможе їй просунутися вперед, але військовий союз не має бути в числі першочергових справ". "Економічна допомога в прагненні допомогти входженню до ЄС має бути більш високим пріоритетом".

На думку колишнього посла США при НАТО, експерта Ренд-корпорейшн Роберта Хантера, Україна має пройти "*довгий шлях*" для входження в

НАТО. Зокрема, ставиться вимога продемонструвати відповідність вимогам НАТО, зокрема поліпшення демократичних стандартів.

Як привило, прискорення вступу України в НАТО обстоюють прихильники жорсткого курсу щодо Росії, які розглядають Україну як чинник нового стратегічного змагання між Заходом і Росією. Наприклад, Аріель Коен стверджував, що Україна перебуває в епіцентрі такого змагання. Певний час ряд американських експертів представляли українську помаранчеву революцію як чинник, що відсунув на другий план протиріччя між США і франко-німецьким альянсом та встановив *«більшу згоду у трансатлантичній політиці»*. Однак у підсумку стриманість дій Москви в ході зміни влади в Україні та Киргизстані призвели до відновлення розбіжностей, і на сьогодні цей чинник більше не діє.

Ерік Міллер звертав увагу на перспективу використання українських потужностей ВПК в інтересах США, зокрема для тестування балістичних ракетних систем радянського зразка на заводі "Південмаш".

Тарас Кузьо звертав увагу на той факт, що активна підтримка США євроатлантичних перспектив України збалансована апатичним ставленням "Старої Європи" – Франції, Німеччини, Бельгії та Люксембургу. Водночас США, Канада та нові члени ЄС будуть підтримувати вступ України до НАТО. В оцінках строків можливого вступу до НАТО згадуються як віхи парламентські вибори 2006 р., виповнення 10-ї річниці Хартії про обпливе партнерство України з НАТО, нова хвиля розширення ЄС в 2007 р. Очікується, що після 2007 р. європейські члени НАТО можуть стати більш прихильними для розгляду питання про вступ до НАТО України, так само як і щодо дискусії про перспективи відносин між Україною і ЄС.

Експерт Американського підприємницького інституту Радек Сікорський (кол. заступник міністра оборони Польщі) передбачав, що за президентства В.Ющенка процес входження України в НАТО *"піде скоріше"*. Однак вступ України в НАТО – це насамперед приєднання до західних цінностей, що ще треба продемонструвати.

На думку екс-міністра оборони Польщі Броніслава Коморовського, Франція, Німеччина і Російська Федерація не зможуть заблокувати вступ України до НАТО. Однак українці мають продемонструвати прагнення інтегруватися з Альянсом та впровадити усі необхідні реформи. За його словами, Росія пробувала використати цю тактику, аби не допустити членства в НАТО Польщі, але в неї нічого не вийшло. "Вже минула та епоха, коли Росія могла впливати на розширення НАТО через окремі країни-члени об'єднання". Німці незабаром обиратимуть нову владу, і у випадку приходу до неї християнських демократів, шанси України інтегруватися з НАТО тільки зростуть, оскільки вони повністю підтримують концепцію Східної політики Польщі.

Б.Коморовський зазначав, що перебування ЧФ Росії на території України не зашкодить інтеграції з НАТО. Українцям більше можуть шкодити прикордонні конфлікти: з Росією, Румунією (стосовно острова Зміїний), чи

проблема Придністров'я. "Власне це може стати доказом для деяких держав НАТО, що українців не варто приймати, оскільки доведеться взяти на себе вирішення цих всіх проблем". Українці для інтеграції з НАТО насамперед повинні впровадити стандарти НАТО в українську армію. "Головне, що українці повинні реформувати свою армію так, аби НАТО бачило її елементом мозаїки, котра пасує до усієї натовської картини". На темпи інтеграції позитивно впливає участь України в міжнародних миротворчих операціях. "Участь України в операціях на Балканах та в Іраку переконує, що держава хоче не тільки отримати гарантію безпеки, але сама здатна вирішувати питання безпеки в інших частинах світу".

Підсумкові міркування.

1. Якщо оцінювати внутрішню українську дискусію стосовно відносин з НАТО, попри високий і регулярний рівень консультацій та низку підписаних документів, досі залишається не з'ясованим цілий ряд важливих питань, включаючи власне визначення чітких інтересів України щодо співпраці та потенційного членства в НАТО, з'ясування можливостей взаємозацікавленого співробітництва між ВПК України та оборонними концернами держав НАТО, а також формування неконфліктної схеми відносин з Росією в межах європейської системи безпеки.
2. Гасло співпраці / членства в НАТО не є самоціллю. Проте досі не було запропоновано реалістичної моделі політичного курсу та формули інтересів України як потенційного члена НАТО.
3. На фоні проблемних відносин між США / НАТО і Росією, через невідповідність внутрішньої української та європейської шкали цін на газ, практична постановка питання про вступ України до НАТО вочевидь передчасна. Збереження економічної стабільності на спроможності до економічного зростання є вочевидь пріоритетним напрямом. Відповідно, якщо це потребуватиме збереження позаблокового статусу України, жодні інші аргументи (політичні та інформаційні чинники, за винятком хіба що виникнення прямої воєнної загрози) не зможуть переважити потреби сприятливого економічного розвитку держави, від яких залежить спроможність України зберегти статус економічно розвиненої держави.
4. Приклади російсько-польських економічних конфліктів (при тому, що Польща є членом ЄС і НАТО) переконливо доводять, що захист інтересів держави потребує не тільки посилення ролі і механізмів міжнародного права, але й врегулювання існуючих конфліктних проблем і не вирішених питань в українсько-російських відносинах.
5. Економічне і політичне посилення Росії спонукатиме її керівництво гостріше реагувати на подальші спроби розширення НАТО в басейні Причорномор'я. Реакція Росії на вступ України до НАТО може коливатися від провокування жорсткої кризи в відносинах, включаючи торговельну війну, до відновлення всього комплексу спірних проблем, таких

як режим Азово-Керченської акваторії, демаркація кордону, статус бази в Севастополі, тощо. В вигляді припущення можна прогнозувати, що якби Україна спробувала вступити до НАТО під гаслом провокування «холодної війни» з Росією, ці проблеми в решті решт могли б призвести до відкладення самого вступу України в альянс через занепокоєння західноєвропейців та загострення регіональних проблем безпеки. Відтак, інтереси України потребують формування моделі відносин з Росією, яка б передбачала мінімальну конфліктність в двосторонніх стосунках. Київ природно зацікавлений в тому, аби російське керівництво не відчувало збільшення політичних та військових загроз, які могли б постати як наслідок зовнішньополітичних рішень України, або, принаймні, мінімізувати ці загрози, включаючи посилення заходів щодо зміцнення довіри, обмеження військової діяльності в прилеглому просторі, політичне вирішення спірних і конфліктних проблем, тощо.

6. З огляду на теперішню європейську ситуацію, набуття членства України в НАТО навряд чи означало б істотне наближення перспектив вступу до ЄС. В якості спільного чинника, який має пряме відношення як до визначення перспектив членства і в НАТО, і в ЄС, можуть розглядатися лише внутрішні реформи, що втілюють сучасні цілі та цінності, поширені в євроатлантичній спільноті.

7. Вступ до НАТО може означати лише опосередковане зміцнення стану безпеки країни, оскільки воєнні конфлікти з сусідніми державами Україні безпосередньо не загрожують. Проте для поліпшення стану безпеки в відносинах з Росією, підготовка до членства України в НАТО потребувала б цілої низки додаткових запобіжних заходів, які мали б пом'якшити очікуване напруження в відносинах з Росією та дозволити російському керівництву «зберегти обличчя». Ці чинники можуть включати розробку додаткових угод про умови перебування бази ЧФ у Севастополі, визначення, спільно з Росією та НАТО, загальних засад військової діяльності в українській зоні відповідальності на Чорному морі, обговорення та затвердження заходів довіри щодо військової діяльності сторін, які мають посилити відчуття безпеки з боку Росії внаслідок безпосереднього наближення НАТО до російських кордонів після вступу України до Альянсу.

8. Вагомим чинником просування інтересів України в ЄС має стати розвиток військово-політичного та оборонного співробітництва з структурами оборони та безпеки Європейського Союзу. По-перше, в цьому плані Росія вже обігнала Україну. По-друге, лише через акцентування пріоритетності ЄС з точки зору українських інтересів Київ може спробувати нейтралізувати упереджене ставлення з боку Франції та ФРН щодо потенційної ролі України як члена НАТО.

Водночас виглядає доцільним більш активний діалог з державами ЄС з метою формування «проєвропейської» позиції України в питаннях

безпеки Європи та ситуації в навколишніх регіонах. Така лінія означала б, що Україна не стане черговим суто проамериканським гравцем в системі європейської безпеки і мала б дотримуватися більш виваженої та конструктивної лінії.

9. В контексті глобальної антитерористичної кампанії триває процес формування нових партнерських відносин. Ця тенденція може радикально змінити уявлення про майбутню систему глобальної безпеки. З точки зору США, нова роль НАТО передбачає розширення діяльності Альянсу за межами традиційної зони відповідальності. Проте проти цього свідомо і послідовно виступає більшість європейських урядів. Цей чинник має постійно перебувати в зоні уваги та потребує надзвичайно обережного реагування.
10. З точки зору потенційної небезпеки втягнення до складних конфліктів в грузинських автономіях, навряд чи, з огляду на теперішню ситуацію, Україні варто надмірно втягуватися до проблем врегулювання конфліктів в Абхазії та Південній Осетії. Проте, безумовно, пріоритетної уваги заслуговують зусилля, спрямовані на врегулювання придністровського конфлікту, який безпосередньо зачіпає інтереси України. Прив'язка вступу України до НАТО з синхронним членством Грузії виглядає недоцільною.
11. З точки зору Брюсселя, надмірна самостійність політики країни – кандидата на вступ до НАТО, як правило, не заохочується. Окрім цього, з точки зору інтересів Альянсу відносини з Росією мають цілком конкретне, самостійне значення. Через це, використання таких інструментів зовнішньої політики України, як трикутник Україна – Польща – Литва та організація ГУАМ в ряді найбільш ризикованих аспектів має узгоджуватися принаймні з основними партнерами України серед європейських членів НАТО. Певної обережності вимагають публічні форми підтримки революцій у країнах СНД, оскільки в ряді випадків важко визначити конкретні інтереси, які переслідують ініціатори масових виступів, а також передбачити розвиток подій у тих чи інших країнах. Принагідно слід зазначити, що саме така обережність змусила президента А.Кваснєвського утриматися від участі у саміті ГУАМ у Кишиневі.
12. Доцільність діалогу основних українських виробників озброєнь з структурами НАТО очевидна як у контексті підготовки до членства в НАТО, так і за умов збереження позаблокового статусу. В сенсі постановки питання про подальші відносини України з НАТО потребує визначення ряд організаційних та політичних питань, включаючи створення умов для виживання та розвитку підприємств ВПК, а також налагодження зв'язків українських підприємств ВПК із західними виробниками. Виглядає доцільною організація експертних нарад і проведення зустрічей зацікавлених українських суб'єктів з Комітетом оборонного планування

НАТО або з Нарадою національних керівників у галузі озброєнь (CNAD).

13. В контексті проблем безпеки вагомим пріоритетом залишається визначення кордонів в Азово-Керченській акваторії. Водночас, наявність не врегульованих прикордонних питань російська сторона буде використовувати як перешкоду для вступу України до НАТО. Проте, з українського боку не варто визнавати в будь-якій формі наявності стану спору. Російська сторона пропонує визначити Керченську протоку як зону спільного користування.
14. Значної уваги потребує поширення в Україні інформації про роль та діяльність Альянсу. В інформації про НАТО висвітлюються переважно протокольні події без аналізу позитивних аспектів співробітництва з НАТО. Проте, з іншого боку, явно бракує моментів, які б свідчили про прагнення допомоги з боку Альянсу, як це, наприклад, демонструвало керівництво Польщі.
15. Очевидно, після Ризького саміту НАТО подальша роль альянсу виглядатиме чіткіше, в тому числі в контексті взаємин між європейськими державами та США. Інтересам України напевно сприяли б процеси зближення між Росією та ЄС, що водночас дозволило б гармонізувати роль НАТО в системі європейської безпеки та відвернути розвиток кризових сценаріїв, що їх все частіше пропонують найбільш радикально налаштовані представники інтервенціоністських течій в політичних колах США.

3.5. Використання інформаційних інструментів і механізмів "передвступної стратегії" та "передвступного партнерства" у взаєминах Україна-НАТО: досвід неурядових організацій

Перші контакти Україна-НАТО були започатковані восени 1991 року, а вже у січні 1992 року представник України вперше взяв участь у засіданні Робочої групи високого рівня Ради північноатлантичного співробітництва. 14 вересня 1995 року було прийнято Спільну заяву України і НАТО, яка відкрила нову сторінку у стосунках з Альянсом шляхом започаткування «розширених і поглиблених» відносин України з НАТО, які наприкінці 1996 року дійшли у своїй еволюції до «особливих та ефективних», заклавши основи для офіційних двосторонніх переговорів щодо формалізації відносин особливого партнерства між Україною та НАТО.

9 липня 1997 року у рамках Мадридського саміту НАТО відбулось підписання Хартії про особливе партнерство між Україною та НАТО. У Хартії визначені основні механізми двостороннього співробітництва Україна-НАТО, зокрема: Комісія Україна-НАТО (регулярні засідання на рівні послів, міністрів закордонних справ, міністрів оборони, глав держав у форматі

«26+1»); спільні засідання з відповідними Комітетами НАТО у форматі «26+1»; спільні робочі групи; взаємні візити високого рівня та обмін експертами; кризовий консультативний механізм для проведення спільних консультацій у випадку, коли Україна вбачатиме пряму загрозу своїй територіальній цілісності, політичній незалежності або безпеці.

У травні 2002 року Рада національної безпеки і оборони України ухвалила Стратегію України щодо НАТО, яка визначила кінцевою метою євроінтеграційної політики України вступ до цієї організації як основи загальноєвропейської системи безпеки. І вже 22 листопада 2002 року Президент України взяв участь у Празькому саміті Ради євроатлантичного партнерства, де під час засідання Комісії Україна-НАТО було схвалено План дій Україна-НАТО.

План дій Україна-НАТО чітко визначив стратегічні цілі і пріоритети України для досягнення її мети – повної інтеграції у євроатлантичні структури безпеки і створив стратегічні рамки для існуючого і майбутнього співробітництва Україна-НАТО відповідно до Хартії про особливе партнерство.

Отже, Україна та НАТО мають чималу історію відносин. Напрацьовано значну договірно-правову базу двосторонніх стосунків. У березні 1992 р. Україна стала членом Ради Північно-Атлантичного співробітництва (РПАС). У 1997 р. Україна стає співзасновницею та учасником наступниці РПАС – Ради Євроатлантичного партнерства (РЄАП), яка на сьогодні налічує 26 держав-членів НАТО та 20 країн-партнерів.

Починаючи з 1994 р., наша держава бере активну участь у програмі "*Партнерство заради миру*" (ПЗМ), в рамках якої українські військові були залучені до кількох десятків спільних з країнами-членами та партнерами НАТО миротворчих навчань як на території нашої країни, так і за кордоном.

Україна пройшла шлях від Хартії про особливе партнерство, підписаної 09.07.1997 р. в Мадриді, через План дій, схвалений 22.11.2002 р. у Празі, в рамках якого реалізується щорічний Цільовий план Україна – НАТО, до Інтенсифікованого діалогу з НАТО з питань набуття членства та відповідних реформ, який було започатковано 21.04.2005 р. у Вільнюсі. У рамках такого діалогу розглядається повний діапазон політичних, військових і фінансових питань, пов'язаних з членством в Альянсі. Цільовий план Україна – НАТО на 2006 р. за своєю філософією та структурою побудовано за схемою Плану дій щодо членства в НАТО (ПДЧ). Виконання ПДЧ є останнім етапом на шляху до отримання країною-претендентом запрошення приєднатися до Альянсу.

На сьогодні, 15 двосторонніх документів регулюють відносини Україна-НАТО. Ще 17 внутрішніх правових актів України та НАТО слугують правовою базою розбудови взаємин.

З квітня 1999 р., згідно з положеннями Хартії, формат відносин переведено у площину спільного форуму – Комісії Україна-НАТО (КУН). Поряд з цим консультативним механізмом співробітництва Україна використовує також й такі механізми, як спільні робочі групи (СРГ) Україна-НАТО з питань

воєнної реформи, озброєнь, економічної безпеки, планування на випадок надзвичайних ситуацій, з питань науки і захисту довкілля, а також регулярні засідання Україна-НАТО на рівні політичного, політико-військового, керівного, військового, економічного та спеціального комітетів.

Значного прогресу у відносинах України з НАТО було досягнуто у 2005 р. У лютому на саміті Комісії Україна-НАТО в Брюсселі Президент України В.Ющенко проголосив набуття членства в НАТО кінцевою метою співробітництва України з Альянсом. Цей сигнал України був позитивно сприйнятий у Брюсселі, і вже в квітні на засіданні Комісії Україна-НАТО на рівні міністрів закордонних справ було ініційовано Інтенсифікований діалог з питань членства та відповідних реформ.

Процес Інтенсифікованого діалогу, започаткований на виконання рішень Мадридського саміту НАТО 1997 р., пропонується країнам, що висловили зацікавленість стати членами Альянсу, і є першим етапом офіційного процесу підготовки країн-аспірантів до членства в НАТО.

У червні 2005 р., на реалізацію рішень Вільнюського засідання Комісії Україна-НАТО, Генсекретарю НАТО під час його візиту в Україну був переданий Початковий дискусійний документ, у якому викладена позиція держави з реформування усіх сфер суспільного життя країни для досягнення високих стандартів державного управління, які встановлені у розвинутих демократичних країнах.

Практичне обговорення підходів України та НАТО в рамках запровадження Інтенсифікованого діалогу відбулося під час візиту делегації Північноатлантичної Ради (ПАР) НАТО в Україну 18-20 жовтня 2005 р. на чолі з Генеральним секретарем Альянс. У рамках зустрічі було проведене чергове засідання Комісії Україна-НАТО за участю Міністрів закордонних справ та оборони України, а також здійснені поїздки членів делегації НАТО в регіони України в інформаційно-роз'яснювальних цілях. Вперше в історії відносин Україна-НАТО відбулося спільне засідання РНБО України та ПАР НАТО під головуванням Президента України В.Ющенка за участі Генсекретаря НАТО Я.Схеффера.

А в грудні за підсумками засідання Комісії Україна-НАТО на рівні Міністрів закордонних справ було прийнято спільну заяву, в якій вперше у документах Україна-НАТО йде мова не лише про відкритість «дверей НАТО», а й про конкретні перспективи залучення України до Плану дій щодо членства.

Під час засідання КУН на рівні Міністрів закордонних справ 28 квітня 2006 р. в Софії (Болгарія) держави-члени НАТО високо оцінили проведення вільних та справедливих парламентських виборів в Україні у відповідності із загальновизнаними демократичними стандартами. На підсумковій прес-конференції за результатами засідання Генсекретар НАТО Я.Схеффер відзначив позитивне ставлення всередині Альянсу до питання стосовно запрошення України до ПДЧ, наголосивши у цьому зв'язку на очікуванні формування нового українського уряду та підтвердження ним Євроатлантичного курсу країни. За

день до цього, підсумовуючи результати зустрічі Міністрів закордонних справ держав-членів НАТО 27 квітня 2006 року, Генсек НАТО також відзначив, що країни, які прагнуть членства в Альянсі, отримають під час осіннього саміту НАТО в Ризі певного роду сигнал про підтримку їхніх зусиль, наповнення якого залежатиме від реальних досягнень країн-аспірантів у цій сфері. Це стосується як країн, які вже виконують ПДЧ (Албанія, Македонія, Хорватія), так і України та Грузії.

На сучасному етапі вступ України до НАТО є одним з пріоритетів зовнішньої політики держави й у короткостроковій перспективі вважається практично єдиною реальною можливістю інституціалізації статусу України як європейської країни.

Під час реалізації стратегічного курсу України на вступ до Організації Північноатлантичного договору (НАТО) важливого значення набуває активізація інформування громадськості про цілі, перспективи, здобутки та актуальні питання Євроатлантичної інтеграції України, поширення об'єктивної інформації про діяльність НАТО.

Але у той же час, суспільне ставлення до можливості вступу України до НАТО залишається негативним, про що говорять останні результати опитування, опубліковані нещодавно Українським інститутом соціальних досліджень: лише 20% опитаних підтримують членство нашої держави в Північно-Атлантичному Альянсі, а 60% — виступають проти. Причиною такого ставлення значною мірою є неефективна інформаційна політика держави.

Наприкінці 2003 року Президент України затвердив три профільні державні програми, а саме: Державну програму інформування громадськості з питань Євроатлантичної інтеграції України на 2004 — 2007 роки, Державну програму підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері Європейської та Євроатлантичної інтеграції України на 2004 — 2007 роки, а також Державну програму інформування громадськості з питань Європейської інтеграції України на 2004 — 2007 роки.

Метою програми інформування громадськості з питань Євроатлантичної інтеграції України на 2004 — 2007 роки є:

- підвищення рівня інформованості громадян України про євроатлантичні інтеграційні процеси, НАТО, його розвиток, переваги членства в цій організації, напрями, стан та перспективи співробітництва України з НАТО;
- підвищення рівня обізнаності молоді щодо Євроатлантичної інтеграції України;
- залучення громадян, громадських і політичних діячів України, представників НАТО та держав-членів НАТО до обговорення актуальних питань, напрямів, організаційних форм співробітництва України з НАТО;
- забезпечення підтримки державної політики Євроатлантичної інтеграції громадянами України.

Координація і контроль за виконанням Програми покладена на Кабінет Міністрів України. З метою виконання Програми Кабінет Міністрів України

затверджує щороку до 10 грудня план відповідних заходів на наступний рік. Для забезпечення організації виконання Програми Кабінет Міністрів України утворює координаційну групу.

Однак, ні 2004 року, ні 2005-го кошти з державного бюджету на їхнє виконання виділені не були. Незважаючи на відсутність цільового бюджетного фінансування згаданих програм, Міністерство закордонних справ продовжувало роз'яснювальну роботу. Експерти МЗС брали участь у семінарах, які проводилися спільно з Громадською лігою Україна-НАТО, Центром інформації і документації НАТО в Україні. З 2005 року керівництво МЗС регулярно почало здійснювати регіональні поїздки з метою роз'яснення актуальних питань зовнішньої політики України, у першу чергу курсу на вступ до НАТО.

Але відсутність ефективної кооперації між владними структурами та авторитетними недержавними аналітичними центрами, іншими громадськими організаціями, які в питаннях інформування більш гнучкі, ніж держава, все зводять нанівець. За словами директора Фонду «Демократичні ініціативи» Ілька Кучеріва, необхідно поєднати зусилля держави і третього сектору, щоби доносити до громадян неупереджену інформацію про всі переваги і недоліки перебування України в Альянсі. Звичайно, держава повинна платити громадським організаціям за участь в інформуванні та просвіті громадян. Для західних країн це звичайна справа, а у нас вона тільки започатковується. Лише минулого місяця держава зробила помітний крок до її вирішення, оголосивши в особі МЗС тендер на проведення 12 інформаційних кампаній стосовно НАТО. До цих пір найбільш помітний вклад у фінансування інформаційної діяльності робили недержавні донорські організації.

Також наступним недоліком у інформуванні населення є те, що в Україні не існує централізації інформаційної діяльності. Стосовно її реалізації ключову роль мав би зіграти Національний центр з питань Євроатлантичної інтеграції, і основні бюджетні кошти для виконання завдань треба було б направляти саме на нього. Потрібно розробити якісну комплексну державну програму, чітко визначити кінцеві результати, скоординувати діяльність, проконтролювати виконання. Вкрай важливо визначити конкретні цільові аудиторії, способи донесення до них інформації, треба працювати з певними фокус-групами, робити моніторинг зміни обізнаності населення.

Сьогодні у рамках Держпрограми інформування головним виконавцем і розпорядником коштів є Держкомтелерадіо, який лише 2006 року отримав 5,2 млн. гривень. Цей комітет активізував свою діяльність у цьому напрямку. Так, з 26 по 30 вересня 2006 року на базі Українського інституту підвищення кваліфікації працівників телебачення, радіомовлення і преси відбувся семінар на тему «*Європейська та Євроатлантична інтеграція України і вступ до СОТ: подолання стереотипів та міфів*». Слухачами семінару були 30 журналістів, які представляли національні, обласні та регіональні телерадіокомпанії, а також Всесвітню службу українського телебачення та радіомовлення.

Що стосується МЗС, то в 2006 році вдалося зняти інформаційну блокаду щодо висвітлення проблематики Євроатлантичної інтеграції українськими ЗМІ. Одними з поштовхів для цього стали зустрічі Міністра закордонних справ України Бориса Тарасюка та першого заступника міністра Антона Бутейка з головними редакторами провідних телевізійних каналів, впливових друкованих ЗМІ та популярних Інтернет-видань.

Позитивну роль зіграло збільшення кількості контактів представників МЗС, зокрема Департаменту НАТО, з журналістами українських ЗМІ як в центрі, так і в регіонах. Департамент НАТО запровадив практику забезпечення українських журналістів інформаційними матеріалами з різноманітних аспектів Євроатлантичної інтеграції.

Представники МЗС регулярно відвідують обласні, районні центри, де проводять зустрічі з громадськістю, місцевими ЗМІ, розповідають про зовнішню політику нашої держави, зокрема і про Євроатлантичну інтеграцію, відповідають на запитання наших співгромадян. З початку року представники лише Департаменту НАТО МЗС здійснили близько 30 поїздок до регіонів держави.

Доказом успішності проведення подібних заходів є збільшення кількості інформаційних повідомлень, передач та публікацій на згадану тематику у вітчизняному інформаційному просторі. Зросла кількість звернень журналістів до Департаменту НАТО з проханням надати інтерв'ю, коментар або інформацію щодо відносин Україна—НАТО. Крім цього, тематика НАТО постійно присутня у брифінгах МЗС з питань зовнішньої політики.

МЗС України сприяє в проведенні ознайомчих візитів представників України до штаб-квартири НАТО. Наприклад, у візиті 13—16 вересня 2006 року взяли участь керівники 11 університетів та інститутів України. Міністерство надає допомогу в організації різноманітних конференцій та круглих столів з тематики НАТО. Зокрема, можна згадати про зимову школу НАТО у Львові в лютому, весняну школу НАТО в Одесі у травні, проведення Першого всеукраїнського форуму проєвропейських організацій у травні в Києві.

2006 року на виконання Держпрограми започатковано чотири проекти:

- розробка логотипу інформаційної кампанії та інтернет-сайту «Україна—НАТО» і виготовлення іміджевої продукції з цим логотипом;
- підготовка комплектів фотовиставки з тематики становлення відносин Україна—НАТО для використання їх в ході публічних інформаційних заходів;
- проведення фокус-груп експертів у контексті їхньої оцінки перспектив Євроатлантичної інтеграції України;
- виготовлення інформаційних флаєрів щодо НАТО та проведення круглих столів в усіх регіонах України з роз'ясненням складової НАТО у зовнішній політиці України.

Наразі готуються до підписання договори щодо виготовлення та розміщення соціальної реклами про Євроатлантичну інтеграцію на зовнішніх

носіях. На краще змінилася ситуація з інформаційним наповненням розділів з Євроатлантичної інтеграції інтернет-сторінок обласних державних адміністрацій (ОДА). Усе більше ОДА використовують інформаційно-роз'яснювальні матеріли та щотижневі добірки інформаційних повідомлень щодо діяльності НАТО, які готуються та розсилаються Департаментом НАТО. Ці матеріали розсилаються в органи державної влади, засоби масової інформації, українські вищі навчальні заклади, громадські організації. Повна версія цих матеріалів розміщена на інтернет-сторінці Міністерства закордонних справ. На завершальній стадії розробки та інформаційного наповнення знаходиться україномовна версія інтернет-сайту «Україна—НАТО» (www.ukraine-nato.gov.ua.). Проект виконується в рамках Держпрограми інформування громадськості з питань Євроатлантичної інтеграції. І, по суті, весь він виконаний силами Департаменту НАТО.

Наше головне завдання — донести до максимальної кількості людей думку, що вибір нашої долі на користь ЄС і НАТО є найбільш оптимальним. Ніхто не каже, що не можна жити без цього, але давайте подивимося на практику інших посткомуністичних держав. Ви можете сказати: хіба ми повинні когось сліпо копіювати? Ні. Але теж не можна ігнорувати їхній позитивний досвід, який свідчить, що після вступу до ЄС і НАТО значно збільшилися інвестиції до цих держав, покращився рівень соціального забезпечення громадян, підвищився рівень життя. У нас майже ніхто на широкому загалі не говорить про те, що являє собою НАТО і ЄС. А ці структури є організаціями, в яких народи згуртувалися навколо таких цінностей, як демократія, захист прав людини, свобода ЗМІ і соціально-орієнтована, конкурентоспроможна ринкова економіка.

На сьогоднішній час в Україні діють наступні структурні підрозділи НАТО:

Центр інформації та документації НАТО (ЦІДН), який відкрився у Києві у 1997 році з метою поліпшення інформованості про НАТО та взаєморозуміння між Україною та НАТО. Центр надає інформацію, сприяє проведенню досліджень, а також фінансує здійснення проектів громадянами України та організаціями за темами, пов'язаними з діяльністю НАТО. ЦІДН надає фінансову підтримку офіційно зареєстрованим українським неурядовим організаціям у проведенні заходів, починаючи від видання публікацій та розробки навчальних програм до проведення конференцій та круглих столів, присвячених НАТО та відносинам Україна-НАТО.

Офіс зв'язку НАТО в Україні, який був відкритий у квітні 1999 року. Його відкриття стало конкретним проявом важливості відносин Особливого партнерства між Україною та НАТО. Метою його діяльності є сприяння участі України у програмі "Партнерство заради миру" (ПЗМ) із максимально повним використанням можливостей, закладених у цьому механізмі, а також поглиблення співпраці між НАТО та державними структурами України.

Офіс зв'язку має три основних завдання. Насамперед, це підтримання контактів з різними українськими установами та відповідними структурами

НАТО, які опікуються розробкою та виконанням заходів співробітництва між Україною та НАТО у рамках ПЗМ та відповідно до Хартії Україна – НАТО. По-друге, надання консультацій для відповідних органів та інституцій України й НАТО щодо поточних заходів та галузей можливого поглиблення співпраці. По-третє, ми беремо безпосередню участь у виконанні деяких практичних заходів, таких як військові навчання або проведення курсів з питань НАТО при Національній академії оборони України, та сприяємо втіленню офіційних контактів між Україною та НАТО на усіх рівнях.

З метою реалізації державної політики у сфері Євроатлантичної інтеграції, подальшого вдосконалення національної системи координації співробітництва України з НАТО на підставі Указу Президента України від 28 лютого 2006 року офіційно розпочав свою роботу Національний центр з питань Євроатлантичної інтеграції України, який є дорадчим органом при Президентові України.

Основними завданнями Національного центру є підготовка висновків і рекомендацій щодо:

- здійснення стратегічного планування та проведення єдиної державної політики у сфері інтеграції України до НАТО;
- розроблення системного підходу до поглиблення співпраці України з НАТО в політичній, оборонній, економічній, правовій, інформаційній, науковій та інших сферах і підготовки проектів програмних документів стосовно дальшої інтеграції України до НАТО;
- подальшого вдосконалення національної системи координації співробітництва України з НАТО та підвищення ефективності контролю заходів державних органів, здійснюваних ними у сфері Євроатлантичної інтеграції;
- вдосконалення нормативно-правового регулювання євроатлантичних процесів.

До складу Національного центру входять посадові особи Апарату Ради національної безпеки і оборони України, Міністерства економіки України, Міністерства закордонних справ України, Міністерства оборони України, Міністерства внутрішніх справ України, Міністерства промислової політики України, Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Міністерства фінансів України, Міністерства юстиції України, Державного комітету телебачення та радіомовлення України, Служби безпеки України, Служби зовнішньої розвідки України, а також за згодою народні депутати України - члени комітетів Верховної Ради України у закордонних справах, з питань національної безпеки і оборони та інші особи.

Останнім часом в Україні розпочався процес утворення неурядових структур, метою яких є інформування громадськості щодо діяльності НАТО та вступу України до нього зокрема.

Так, 26 вересня 2003 року представниками 26 громадських організацій України було засноване громадське об'єднання «***Громадська Ліга Україна-***

НАТО», яка є всеукраїнською спілкою громадських організацій, що поділяють євроатлантичні цінності, підтримують курс на набуття Україною повноцінного членства в НАТО та мають намір своєю діяльністю сприяти виконанню Плану дій Україна-НАТО.

Цілями створення Ліги є:

- Підвищення рівня обізнаності громадськості з діяльністю НАТО через співробітництво України з НАТО у сфері інформації, включаючи співпрацю з Центром інформації і документації НАТО в Україні.
- Координація діяльності та об'єднання зусиль громадських організацій України, їх інтелектуальних, організаційних, технологічних та комунікаційних ресурсів, зокрема в інформаційній, дослідницькій та освітні сферах, з метою підвищення рівня інформованості громадськості України про співробітництво нашої держави з НАТО.
- Сприяння регулярному обміну досвідом та інформацією між громадськими організаціями у сфері співробітництва України з НАТО, створення та розширення інформаційної мережі з урахуванням існуючих структур та проектів.
- Об'єднання зусиль громадських організацій та органів державної влади України щодо спільної реалізації державної політики у сфері співробітництва України з євроатлантичними структурами в контексті виконання Плану дій та цільового плану Україна – НАТО.
- Подальший розвиток інформаційного та гуманітарного співробітництва України з НАТО.
- Запровадження ефективних форм співпраці громадських організацій України з Центром інформації та документації НАТО в Україні, дипломатичними місіями країн-членів НАТО, іншими міжнародними організаціями, а також Національним Центром з питань Євроатлантичної інтеграції України, Державним комітетом телебачення і радіомовлення України, Верховною Радою України, іншими органами державної влади України, відповідальними за розвиток Євроатлантичної інтеграції України.
- Сприяння міжнародному співробітництву та покращенню міжнародного іміджу України, зокрема у сфері взаємовідносин Україна – НАТО шляхом популяризації євроінтеграційної активності України на загальнонаціональному та міжнародному рівнях.

Інститут Євроатлантичного Співробітництва (ІЄАС) - незалежна громадська дослідницька організація, діяльність якої спрямована на Євроатлантичну інтеграцію України шляхом здійснення аналізу, вироблення рекомендацій та прогнозів у галузі міжнародних відносин в цілому та зовнішньої політики зокрема. Метою ІЄАС є сприяння Євроатлантичній інтеграції України як передумови та гарантії демократичного розвитку країни шляхом проведення ґрунтовних досліджень та просвітницьких заходів, спрямованих на подолання викликів сталому демократичному розвитку українського

суспільства. Борис Тарасюк є Директором та засновником Інституту Євроатлантичного співробітництва, який по суті є незалежним аналітичним центром.

Асоціація міжнародного співробітництва «Атлантична Рада України» (АРУ) заснована для підтримки розвитку і поглиблення процесу демократизації в Україні шляхом розповсюдження знань і поглиблення інформованості і розуміння спільнотою актуальних міжнародних подій з метою більш ефективного впливу на виготовлення і реалізацію офіціальних зовнішньополітичних рішень.

АРУ була створена 4 січня 1995 року і є неурядовою, неприбутковою громадською організацією, яка сприяє розширенню контактів і діалогу на міжнародному рівні, поглибленню взаємодії представників державних органів, органів влади, політиків, освітніх академічних організацій, мас-медіа, підприємців, представників громадськості з метою дослідження і визначення суспільної думки відносно інтеграції України в Європейське суспільство та реалізації її національних інтересів в рамках євроатлантичних структур. Діяльність Асоціації поширюється на територію України, Росії та інших держав.

Основними цілями діяльності Асоціації є:

- сприяти розвитку неурядової дипломатії, політичному, економічному і гуманітарному співробітництву в Євроатлантичному регіоні світу;
- розширення впливу на нього громадськості і її взаємодії з державними структурами на регіональному, національному і міжнародному рівнях, представлення і захист загальних інтересів своїх членів.
- При Атлантичній Раді України також створений Молодіжний Центр Атлантичної Ради України, який реалізує проекти за Євроатлантичною тематикою, зокрема, семінари, круглі столи, акції та конкурси для учнівської і студентської молоді, що відбуваються за підтримки центру інформації та документації НАТО в Україні, посольств різних країн та інших зацікавлених установ і організацій.

До роботи інформування громадськості щодо європейського та євроатлантичного вибору, аналізу переваг та недоліків курсу євроінтеграції України, досліджень зовнішньополітичної та зовнішньоекономічної діяльності нашої держави долучаються й інші профільні організації та структури, різного роду фонди, які мають недержавне фінансування.

Зокрема на території України діє Фонд «Демократичні ініціативи», який був заснований у 1992 році як неприбуткова, недержавна, аналітична організація.

Фонд поширює інформацію трьома шляхами:

- організовує конференції стосовно актуальних економічних і політичних тем, а також організовує круглі столи, які збирають разом журналістів і аналітиків з метою обговорення ключових питань, пов'язаних з громадською думкою;
- організовує прес-конференції і видає прес-релізи з інформацією, яку він зібрав і проаналізував. Такі відомі засоби масової інформації, як газети

«Washington Post», «Ukrainian Weekly», «Gazeta Wyborcza», «Голос України», «Урядовий кур'єр», «Факты и комментарии», «День», УТ-1, УТ-2 і Радіо «Свобода» регулярно оприлюднюють результати опитувань та аналізу;

- публікує власну інформацію у своєму бюлетені «Політичний портрет України», а також серії брошур «Україна на шляху до відкритого суспільства», має сторінку в Інтернеті.

З Фондом «Демократичні ініціативи» співпрацюють відомі в Україні економісти, соціологи, політичні аналітики і журналісти. Ці аналітики, чиї дослідження публікуються у грунтовних монографіях, низці журналів і газет, регулярно використовуються на радіо та телебаченні, добре відомі в академічному світі. В аналізі соціополітичної та економічної ситуації в Україні також регулярно беруть участь видатні політики і журналісти.

Фонд «Демократичні ініціативи» тісно співпрацює з організаціями в Україні та усьому світі, зокрема зі Світовим Банком, Канадською Агенцією Міжнародного Розвитку, Національним демократичним інститутом міжнародних відносин (США), Центром Ропера (США).

На сьогодні Фонд реалізовує спільні проекти з Міжнародним Фондом «Відродження», «Домом Свободи» (США), Агенцією міжнародного розвитку США, посольствами США, Канади, Нідерландів, Національним фондом підтримки демократії (США), Фондом Чарльза Стюарта Мотта. Фонд «Демократичні ініціативи» веде постійний діалог з багатьма українськими офіційними інституціями, включно з Верховною Радою, Секретаріатом Президента України, Кабінетом Міністрів, Київською міськрадою, міністерствами закордонних справ, освіти та культури.

Фонд «Європа XXI» — неурядова неприбуткова дослідницька організація, заснована у грудні 1998 року з метою надання інтелектуального сприяння процесам євроінтеграції України, а саме до Європейського Союзу та НАТО як способу забезпечення розвитку України як європейської демократії. Засновниками організації є українські та британські фахівці, які мають значний досвід розробки і реалізації проектів, керівництва дослідницькою роботою неурядових організацій.

Серед проектів Фонду «Європа XXI» є програми з розвитку НУО, політичних партій та виборчих технологій; програми з питань Європейської інтеграції для журналістів; серія «круглих столів» для українських та іноземних політиків, фахівців у галузі зовнішньої політики та міжнародних відносин і журналістів «Україна: Європейський вимір», серія міжнародних конференцій для українських і західних урядовців і дослідників про розвиток відносин України і західних демократій (спільно з Wilton Park, Велика Британія); проведення багатосторонніх фокус-груп з фахівцями, які працюють у галузі Європейської інтеграції в країнах Центральної та Східної Європи і ЄС, участь у створенні мереж НУО-бізнес (спільно з Координаційно-експертним центром об'єднань підприємців України); інформаційно-просвітницька програма з

питань Європейської інтеграції для журналістів (за підтримки Міністерства закордонних справ і Співдружності Великої Британії), дослідження і публікації про роль журналістів у просуванні демократії і ринкової економіки та ідей Європейської інтеграції в Україні (спільно з Делегацією Європейської Комісії в Україні), проекти "Розбудова аналітичної спроможності політичних партій" (за підтримки Вестмінстерського фонду демократії), "Громадянське суспільство: крок за кроком" (фінансоване Національним фондом підтримки демократії), "Сприяння поширенню толерантності у поліетнічному суспільстві" (за підтримки Фонду проектів у галузі прав людини Міністерства закордонних справ і Співдружності Великої Британії).

Фонд "Європа XXI" є членом Громадської експертної ради при Міністерстві закордонних справ України, Громадської ради при Комітеті ВР України з питань свободи слова, Контактної групи НУО по співпраці з місією Світового Банку в Україні та Координаційно-експертного центру об'єднань підприємців України.

Останнім часом до інформаційного висвітлення діяльності Північно-Атлантичного Альянсу долучається низка засобів масової інформації, зокрема такі як: тижневик «Дзеркало тижня», газета «День», газета «Україна молода», інтернет-видання «Українська правда» та багато інших [368-384].

Отже, можна стверджувати, що в Україні відбувається процес інформування громадськості щодо Євроатлантичної стратегії України. Була прийнята низка законів та рішень, зокрема «*Державна програма інформування громадськості з питань Євроатлантичної інтеграції України*», яка поставила мету й завдання, визначали пріоритети та цілі інформування населення України. Наприклад, за останні два роки різко зросла чисельність недержавних та громадських установ, фондів, науково-дослідних інституцій, котрі проводять аналіз діяльності організації Північно-Атлантичного Договору, преваг та недоліків вступу України до Альянсу, а також висвітлюють результати досліджень через ЗМІ, конференції, «круглі столи», семінари тощо. Тобто основним інформаційним інструментом «Євроатлантичної стратегії України» є проведення інформаційно-роз'яснювальних заходів.

Але, якщо говорити про результати такої політики, то тут виникає велика дискусія. У той час, коли вступ України до НАТО проголошений одним з пріоритетів зовнішньої політики держави й у короткостроковій перспективі є практично єдиною реальною можливістю ствердження статусу України як європейської країни, суспільне ставлення до такої можливості залишається негативним. В Україні, як і раніше, зберігається стереотип, в якому НАТО розглядається як ворожий військово-політичний блок. За результатами опитування центру соціологічних досліджень «Софія», проведеного 10.05.2006 року, число опитаних громадян України, які вважають, що Україні не слід вступати до НАТО ні за яких обставин складає 44,8%, 10,3% опитаних респондентів вважають вступ України до НАТО обов'язковим процесом, який

повинен відбутися якнайшвидше. Решта опитаних вважає, що в даний момент вступ до НАТО є невчасним.

В той же час 73,4% респондентів переконані, що ухвалювати рішення про вступ України до НАТО повинні українські громадяни на всенародному референдумі. У разі проведення такого референдуму, за вступ до НАТО мають намір проголосувати 21,5%, проти – 60,2%. Окрім деяких політичних сил, опонентами вступу України до НАТО також виступають більшість керівників українських підприємств оборонно-промислового комплексу. За даними експертного опитування, проведеного у вересні 2006 року Центром досліджень армії, конверсії та роззброєння, 17 із 39 опитаних директорів оборонних підприємств очікують збитків від вступу України до Альянсу, оскільки це скоротить ринки збуту для українського збройного експорту в Росію. Як зауважив експерт Інституту зовнішньої політики Олександр Палій, це можна пояснити лише тим, що бізнес не любить змін і для українських оборонних підприємств перспектива виходу на нові ринки – це шок. Тому для подолання розбіжностей, які існують серед українського населення, важливу роль у процесі інформування щодо вступу до НАТО необхідно відвести саме засобам масової комунікації, які найбільше впливають на формування громадської думки. Для досягнення кращого результату ця робота повинна бути системною і включати нові підходи та шляхи розповсюдження інформації, виготовлення друкованої продукції, залучення громадськості до обговорень на «круглих столах» та громадських слуханнях.

Щодо ефективного використання інструментів та засобів проведення інформаційної політики у рамках державної програми інформування громадськості з питань Євроатлантичної інтеграції України, то необхідно зауважити, що український уряд не докладає великих зусиль у формуванні чітко визначених механізмів та етапів реалізації цієї програми. Основні державні інституції, які найбільше переймаються інформуванням громадськості – це Міністерство Закордонних Справ та Міністерство Оборони. А щодо інших урядових інституцій, то вони не сприймають серйозно своєї участі у процесі інформування населення щодо Євроатлантичного вибору нашої держави. Іншою основною проблемою є взаємовідносини державних установ з неурядовими організаціями. Як вже зазначалося раніше в Україні існує чимало недержавних громадських організацій, котрі займаються проблематикою висвітлення діяльності та створення позитивного іміджу НАТО. Для ефективного проведення інформаційно-роз'яснювальних заходів серед населення України необхідна чітка і злагоджена співпраця саме з неурядовими організаціями. Адже вони набагато тісніше спілкуються з громадськістю і цей фактор необхідно використовувати.

Крім того, важливого значення має освітній аспект. Згідно Указу Президента № 1861, починаючи з 2006/2007 навчального року, до змісту загальної середньої та вищої освіти необхідним стало включення питань, пов'язаних із проблемами міжнародної безпеки, діяльністю НАТО та Європейського Со-

юзу, співробітництвом України з цими міжнародними інституціями. Від того, яким чином буде викладений матеріал викладацько-професорським складом навчальних закладів буде залежати подальше формування поглядів молоді стосовно вищевказаних питань. Отже, доцільним вважається розробка, публікація та розповсюдження навчального посібника, в якому будуть коректно висвітлені дані питання, а також враховані завдання для самостійної роботи. Крім того, необхідним є проведення курсів підвищення кваліфікації та семінарів з даної тематики для вчителів й викладацького складу навчальних закладів.

Стає системним те, що на інформаційно-роз'яснювальні заходи, котрі проводять недержавні організації чи міністерства, запрошуються одні й ті самі люди, результатом чого стає неефективне поширення інформації серед населення. Цю проблему можна вирішити, визначивши та розподіливши аудиторії, спільно з іншими аналогічними установами розробити програму інформування населення та шляхи її реалізації.

Не можна забувати й про те, що вступ України до Північно-Атлантичного Альянсу — це питання геополітики. У Росії, як у політичних елітах, так і в масовій свідомості, існує думка про те, що ніякої України немає і не було, що українці за будь-яких умов в результаті звернуться за допомогою до «старшого брата». Якщо Україна вступить до НАТО, то це стане своєрідною «точкою неповернення», й означатиме, що ми ніколи більше не станемо частиною Росії. Тому інформування населення щодо вступу до НАТО буде зустрічати великий інформаційний спротив. І до цього необхідно бути підготовленим.

Також необхідно залучати до інформаційної політики держави PR-структури, котрі раніше залучались російськими політтехнологами для формування негативного ставлення до НАТО в Україні. Серед них може бути проведений тендер на кращий PR-проект, за результатами якого переможець отримав би державний контракт. Доцільним також є трансляція хоча б однієї інформаційно-аналітичної програми, яка повинна передаватися недержавним каналом й бажано в prime-time (на відміну від „*Території безпеки*" на 1-му національному вранці в неділю).

На завершення треба додати, що в цілому є суттєві ознаки інформування громадськості щодо Євроатлантичного вибору України, але для її подальшої реалізації необхідна рішучість та чіткість у прийнятті рішень як на загальнодержавному, так і на нижчих рівнях, системність підходів до планування інформаційних заходів з даної тематики, врахування особливостей різних аудиторій, залучення до цієї проблеми засобів масової інформації, які повинні надавати більш аргументовані переваги при набутті Україною статусу держави-члена НАТО.

3.6. Оцінка загроз та ризиків інформаційної безпеки держави

Проблема прийняття рішень в області міжнародних відносин часто може ускладнюватися невизначеністю, унікальністю обставин, що складаються, гострим дефіцитом часу на вироблення рішення. Знання про предметну область можуть бути неточними або неповними, можуть використовуватися недостатньо чітко сформульовані концепції або недостатньо вивчені явища. Крім цього, невизначеність може бути внесена неточними або ненадійними даними про конкретну ситуацію. Таким чином, експерти на практиці користуються неточними методами, виходячи з наступних причин: точних методів не існує; точні методи існують, але не можуть бути застосовані на практиці через відсутність необхідного обсягу даних або неможливості їхнього накопичення по міркуваннях вартості, ризику або через відсутність часу на збір необхідної інформації.

При використанні класичної або булевої логіки зразу виникає істотний недолік – з її допомогою неможливо описати асоціативне мислення людини. Булева логіка оперує тільки двома поняттями: „істина" й „хиба", виключаючи будь-які проміжні значення. Такі підходи зручно використовувати для обчислювальних машин, але спробувати представити весь навколишній світ тільки в чорному й білому кольорі, виключивши з мови будь-які відповіді на питання, крім "так" й „ні" неможливо.

Постає потреба у вирішенні аналітичних задач оцінки стану та ідентифікації моделей складних динамічних систем в умовах невизначеності. Існує багато підходів для вирішення задач такого типу. Однією з найбільш ефективних математичних теорій, спрямованих на формалізацію і обробку невизначеної інформації є теорія нечіткої логіки. Дана математична теорія дозволяє з єдиних позицій розглянути різні види невизначеності, врахувати найкращим чином досягнення і позитивні властивості інших теорій і отримати новий, більш якісний результат. З'являється можливість описувати як кількісно, так і якісно виражену інформацію, враховувати семантичні модальності інформаційних одиниць, нечіткість даних, мультиплікативний вплив факторів невизначеності, синергетичні ефекти, вплив ризиків і суб'єктивних думок і ряд інших моментів, які підвищують неадекватність рішень [385].

Нечітка логіка забезпечує інтуїтивний метод для опису систем в лінгвістичних термінах зрозумілих експертам даної області.

Головними перевагами нечіткої логіки при вирішенні задач з області міжнародних відносин є:

- можливість оперувати вхідними даними, заданими нечітко;
- можливість нечіткої формалізації критеріїв оцінки та порівняння;
- можливість проведення якісних оцінок як вхідних даних, так і вихідних результатів.

У розробці методу оцінки та ідентифікації об'єктів на основі нечітких баз знань використовується ряд принципів [386]:

1. Принцип лінгвістичності вхідних і вихідних змінних. У відповідності до цього принципу, входи об'єкту і його вихід розглядаються як лінгвістичні змінні, які оцінюються якісними термами. Згідно Л. Заде [387], лінгвістичною змінною називається така змінна, значеннями якої є слова чи речення природної мови, тобто якісні терми. З терміном "лінгвістична змінна" можна зв'язати будь-яку фізичну величину, для якої потрібно мати більше, ніж два значення („так" й „ні"). У цьому випадку потрібно визначити необхідну кількість термів і кожному з них поставити у відповідність деяке значення описуваної фізичної величини.

2. Принцип формування структури залежності "вхід-вихід" у вигляді нечіткої бази знань. Одним з основних методів подання знань в експертних системах є продукціонні правила, що дозволяють наблизитися до стилю мислення людини. Будь-яке правило продукцій складається з посилок і висновку. При наявності у правилі декількох посилок вони поєднуються за допомогою *логічних зв'язок* І, АБО. Продукціонні правила записується у вигляді

ЯКЩО <вхід11> *зв'язка* <вхід12> *зв'язка* ... , ТО <вихід1>

ЯКЩО <вхід21> *зв'язка* <вхід22> *зв'язка* ... , ТО <вихід2>

Головним недоліком продукціонних систем залишається те, що для їхнього функціонування потрібна наявність повної інформації про систему. Нечіткі системи керування засновані на правилах продукціонного типу, однак у якості посилки й висновку в правилі використовуються лінгвістичні змінні, що дозволяє уникнути обмежень, властивих класичним продукціонним правилам.

Сукупність правил ЯКЩО-ТО можна розглядати як набір експертних точок у просторі "входи-вихід". Застосування апарату нечіткого логічного висновку дозволяє встановлювати по цим точкам багатовимірну поверхню, яка дозволяє отримувати знання виходу при різних комбінаціях значень вхідних змінних.

За допомогою спеціальної математичної теорії, що базується на теорії нечітких множин, стає можливим перехід від нечітких значень змінної до цілком певних (кількісних) значень, які необхідні для фізичного виконавчого пристрою. Використовуються так звані алгоритми р-перетворення нечітких значень умов і виводів у кількісну форму. І відповідно обернене перетворення p^{-1} отриманих результатів у вихідний простір до нечіткої лінгвістичної змінної.

Моделі, створені за допомогою теорії нечіткої логіки, можуть суттєво допомогти при формуванні стратегії розвитку нашої держави. Може бути створена автоматизована експертна система оцінки та ідентифікації, яка призначена для прогнозування подальшого розвитку ситуації і дає можливість визначити пріоритетність наявних альтернатив на основі висновків експертів.

Практична цінність таких моделей, наприклад, моделі оцінки стану національної безпеки держави, полягає в тому, що на основі проведеної класифікації основних ознак національної безпеки та їх оцінки можна визначити, який з цих показників більше всього впливає на стан національної безпеки, на

що потрібно звернути увагу першочергово, що потрібно покращити чи змінити, що негативно впливає на стан національної безпеки держави. Тобто, за допомогою запропонованого методу можна сформувати стратегію розвитку держави, ефективну систему забезпечення національної безпеки.

Останнім часом суттєво змінилися концептуальні підходи до визначення поняття та змісту безпеки. Змінюються підходи до визначення її складових, постає потреба в більш широкому визначенні безпеки. Вона має складатися не тільки з військових елементів, „а об'єктом безпеки є не тільки держава, а й індивіди та, ширше, суспільство"[388]. Поняття "національна безпека" безпосередньо пов'язано з такими поняттями як „національні інтереси", „загрози національним інтересам та „система забезпечення національної безпеки".

До основних життєво необхідних національних інтересів можна віднести [389-390]: територіальна цілісність, державний суверенітет, намагання посісти гідне місце у світовому співтоваристві, добробут громадян на основі забезпечення прав і свобод особи, а також усіх соціальних груп. Оскільки з просторово-географічною взаємодією країн та народів пов'язана наявність трьох геополітичних рівнів безпеки — міжнародної, регіональної і безпеки окремо взятої держави, то в просторово-географічному плані сфера національних інтересів не може обмежуватися національною територією. Процеси, які розгортаються у різних регіонах ближнього і навіть дальнього зарубіжжя, можуть безпосередньо впливати на стан нації, можливості та перспективи її розвитку і, таким чином, на розуміння та визначення національних інтересів. Відповідно до цього будемо розрізняти внутрішню та зовнішню безпеку.

Загрози національним інтересам — це дії політичних, військових або природних сил, вплив перебігу соціальних, економічних та інших подій, а також ситуацій, що складаються в результаті цих подій, на процес життєдіяльності людини, суспільства, держави, які змушують країну йти на додаткові зусилля, вимагають надмірно великих витрат, мобілізації ресурсів з метою збереження своєї державності, національної та культурної ідентичності, надійного захисту власного народу. Загрози національним інтересам завдають або здатні завдати шкоди національним цінностям, зробити неможливою або ускладнити реалізацію життєво важливих інтересів держави. Загрози розрізняють за кількісними та якісними характеристиками, за джерелами їх виникнення, рівнем інтенсивності впливу тощо. Масштабність загроз визначається фронтом їх розповсюдження (кількісні параметри території, населення, виробництва), а інтенсивність — темпами та обсягами деструктивних змін. Загрози діють головним чином у відповідній сфері національних інтересів, але негативний вплив їх розповсюджується на інші національні інтереси. Хоча можна виділити загрози, що діють одночасно на значну кількість національних інтересів. Необхідно враховувати, що загрози, як правило, мають декілька стадій розвитку: зародження (початок формування), прояв (знаходження виразних форм), загострення (критична стадія негативного впливу з відповідними наслідками).

Система забезпечення національної безпеки — це комплекс організаційних структур, засобів і скоординованих дій і заходів, що здійснюються з метою розробки та реалізації цілеспрямованих рішень щодо захисту життєво важливих інтересів людини, суспільства і держави від внутрішніх і зовнішніх загроз. Метою системи забезпечення національної безпеки є реалізація політики національної безпеки, зміст якої визначається пріоритетними національними інтересами і діючими на них загрозами, ідентифікація та оцінка яких стає можливою з використанням нечітких експертних баз знань.

Постає необхідність у розробці методологічних основ оцінки поточного рівня національної безпеки держави з використанням багатьох показників, визначення межі неприпустимості зони значень рівня національної безпеки держави, зони ризику та зони повної реалізації життєво важливих інтересів людини, суспільства і держави. Це дозволить виробляти обґрунтовані пропозиції щодо нейтралізації загроз національним інтересам, планувати та вживати необхідні заходи щодо забезпечення потрібного рівня національної безпеки держави.

Аналізуючи практичні спостереження та сучасні наукові розробки, можна виділити групу нетрадиційних загроз міжнародній безпеці: поширення зброї масового знищення, асиметричні збройні конфлікти, міжнародний тероризм, придбання зброї масового знищення державами-паріями, організована злочинність, розвиток внутрішнього життя в державах, „що не відбулися", поширення військових можливостей, зокрема зі ЗМЗ, на недержавних акторів, деградація довкілля, етнічні конфлікти, переміщення біженців та міграція, так звана „екологічна міграція", зростаюча непередбачуваність місця виникнення конфліктів [388].

З використанням теорії нечіткої логіки стає можливим створення автоматизованих систем моніторингу загроз національним інтересам держави (природного, екологічного, техногенного, соціального характеру), що дозволяє визначити їх якомога раніше й розробити систему заходів (економічного, політичного, воєнного, екологічного, соціального та іншого характеру), які з найменшими втратами нейтралізують загрози та припиняють деструктивні процеси.

Для оцінки стану національної безпеки пропонується використовувати методи нечіткої логіки на основі визначених пріоритетних показників національної безпеки у політичній, економічній, інформаційній, соціальній, військовій, екологічній, технологічній сферах. Національна безпека розглядається як лінгвістична змінна, рівні якої оцінюються за допомогою якісних термів. Відокремлюються сукупності внутрішніх та зовнішніх чинників по кожній сфері, що впливають на стан національної безпеки держави.

Розглянемо запропоновану методику оцінки більш детально для однієї з складових національної безпеки держави — інформаційної безпеки.

Будемо розглядати інформаційну безпеку України як стан захищеності національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави.

Загрози національним інтересам в інформаційній сфері визначаються як сукупність умов і факторів, які створюють небезпеку заподіяння шкоди об'єктам національних інтересів у інформаційній сфері й діяльності щодо реалізації цих інтересів. Їх можна поділити на:

- загрози діяльності влади щодо реалізації національних інтересів в інформаційній сфері;
- загрози об'єктам національних інтересів в інформаційній сфері, які, в свою чергу, можна поділити на загрози інформації, інформаційній інфраструктурі та правовому статусу людини в інформаційній сфері.

Серед загроз вільному використанню результатів діяльності в галузі науки і техніки, тобто сукупності умов і факторів, які створюють небезпеку життєво важливим інтересам особистості, суспільства і держави, можна виділити такі [391]:

- недостатню потребу у нових передових науково-технічних рішень і оригінальних розробок;
- скорочення обсягів досліджень на стратегічно важливих напрямах світового науково-технічного розвитку;
- небезпеку вільного обігу певних результатів інтелектуальної діяльності, обмежених законодавством України;
- нерозвиненість організаційної інфраструктури, адекватної ринковим умовам, і системи захисту результатів інтелектуальної діяльності в науково-технічній сфері як комерційної таємниці;
- роз'єднаність системи обліку результатів науково-технічної діяльності, виконаних за бюджетні кошти, і засобів контролю за їхнім використанням;
- недостатність нормативної бази для включення результатів інтелектуальної діяльності до економічного обігу, недооцінка нематеріальних активів підприємств, галузей і економіки країни в цілому;
- зниження комерційного потенціалу результатів інтелектуальної діяльності військового і подвійного призначення внаслідок недосконалості процедур передачі таких результатів з військової до цивільної сфери;
- деформація системи відтворення науково-технічних кадрів і науково-технічного потенціалу країни;
- тенденція створення пільгових умов для поширення на українському ринку зарубіжних технологій і науково-технічної продукції і, як наслідок, посилення технологічної залежності України в інформаційній сфері;
- активізація дій закордонних організацій, спрямованих на неправомірне одержання результатів інтелектуальної діяльності українських вчених;
- експансія імпортних технологій, що значно знижує попит на вітчизняну продукцію.

У розробці методу оцінки чи ідентифікації нелінійних об'єктів, таких як, рівень загроз інформаційної безпеки держави, на основі нечітких баз знань використовується ряд принципів. Ці принципи є узагальненням і подальшим

розвитком аналогічних принципів, сформульованих для прийняття діагностичних рішень.

У відповідності до принципу лінгвістичності вхідних і вихідних змінних, входи об'єкту і його вихід розглядаються як лінгвістичні змінні, які оцінюються якісними термами. Для створення певного математичного оформлення чисто людських лінгвістичних методів опису явища, а саме на основі яких міркувань робляться ті чи інші висновки, можна зробити певні попередні дії, які стосуються основ позначення тих чи інших ознак чи явищ. Використовуючи поняття функції належності, кожен з термів, який оцінює лінгвістичну змінну, можна формалізувати у вигляді нечіткої множини, заданої на відповідній універсальній множині.

Згідно принципу формування структури залежності "вхід-вихід" у вигляді нечіткої бази знань, формується сукупність правил вигляду:

ЯКЩО <входи>, ТО <вихід>,

які відображають досвід експерта і його розуміння причинно-наслідкових зв'язків у задачі прийняття рішення. Наприклад,

ЯКЩО змінна X висока і У низька, ТО R є середнім.

Особливість подібних висловлювань складається в тому, що їх адекватність не змінюється при незначних коливаннях умов експерименту. Тому формування нечіткої бази знань можна трактувати як аналог етапу структурної ідентифікації, на якому будується модель об'єкту з параметрами, які можна настроювати. В даному випадку настройці підлягають форми функцій належності нечітких термів, за допомогою яких оцінюється входи і виходи об'єкта.

Отже, позначимо R – інтегральний показник рівня загроз інформаційної безпеки України, вільному використанню результатів діяльності в галузі науки і техніки. Інтегральний показник R оцінюється сукупністю пріоритетних ознак, які характеризують інформаційну безпеку в галузі науки і техніки, і включає в себе 11 показників. Але в зв'язку з дуже великою розмірністю матриць, які будуть використовуватися для розрахунків, відокремимо для побудови моделі три основних показника:

r_1 – небезпека вільного обігу певних результатів інтелектуальної діяльності, обмежених законодавством України;

r_2 – нерозвиненість організаційної інфраструктури, адекватної ринковим умовам, і системи захисту результатів інтелектуальної діяльності в науково-технічній сфері як комерційної таємниці;

r_3 – експансія імпортних технологій, що значно знижує попит на вітчизняну продукцію.

Більшість показників має якісний характер, тобто не мають точного кількісного виміру при визначенні відповіді щодо рівня загрози інформаційній безпеці держави. Тому при оцінюванні одного і того ж показника декількома експертами можуть виникати різні думки. Крім того експерт не завжди здатен словами оцінити окремий показник, хоча інтуїтивно відчуває його рівень.

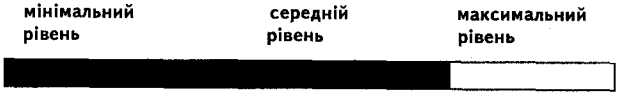
Для подолання таких складностей можна оцінювати показники за принципом термометра. Користуючись принципом термометра, експерт робить висновки щодо певної ознаки, користуючись не математичними поняттями — мінімальний, середній, вище середнього, максимальний — а зрозумілими йому термінами з області дослідження.

Суть цього принципу полягає в тому, що експертна оцінка деякої змінної здійснюється шляхом замальовування частини шкали, ліва і права межі якої відповідають найменшому і найбільшому рівням змінної, що розглядається. Принцип термометру зручно застосовувати в тих випадках, коли експерт не в змозі оцінити деяку змінну ні числом, ні якісним термом, а лише інтуїтивно відчуває її рівень.

Для оцінювання трьох, виділених для дослідження показників, будемо використовувати таку градацію: високий рівень загрози (мінімальний), середній рівень загрози (середній), низький рівень загрози (максимальний).

Кожному з термів поставимо у відповідність лінгвістичний опис в термінах області дослідження:

r_1 — небезпека вільного обігу певних результатів інтелектуальної діяльності, обмежених законодавством України

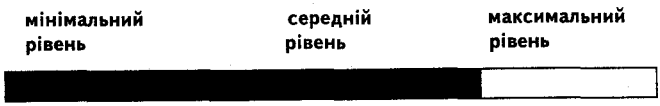


Повне невиконання норм законів відносно розповсюдження результатів інтелектуальної діяльності	Часткове невиконання норм законів відносно розповсюдження результатів інтелектуальної діяльності	Відповідність нормам законів відносно розповсюдження результатів інтелектуальної діяльності

r_2 — нерозвиненість організаційної інфраструктури, адекватної ринковим умовам, і системи захисту результатів інтелектуальної діяльності в науково-технічній сфері як комерційної таємниці.

Повна невідповідність законодавства та нерозвиненість *інфраструктури системи* захисту інтелектуальної діяльності в науково-технічній сфері	Недоскональна система захисту інтелектуальної діяльності в науково-*технічній сфері, часткова* відповідність законодавства Європейській практиці захисту	Досконала система захисту інтелектуальної діяльності в науково-*технічній сфері, часткова* відповідність законодавства Європейській практиці захисту

$г_3$ – експансія імпортних технологій, що значно знижує попит на вітчизняну продукцію



Повна експансія зарубіжних технологій і науково-технічної продукції, що значно знижує попит на вітчизняну продукцію і робить Україну цілком технологічно залежною	Часткова експансія зарубіжних технологій і науково-технічної продукції, що значно знижує попит на вітчизняну продукцію і сприяє технологічній залежності України	Законодавче регулювання імпорту технологій і науково-технічної продукції, обмеження створення пільгових умов для поширення на українському ринку зарубіжних технологій і науково-технічної продукції

При оцінці будь-якого об'єкту необхідно виділити певні показники і визначити ієрархію показників якості. Традиційно використовується 5-ти бальна система оцінки якості показника чи об'єкта, але вона не повністю враховує різні градації (відтінки) якості. Тому визначення якості показника пропонується проводити за 7-ма рівнями, наприклад:

$г_1$ - дуже низький;
$г_2$ - низький;
$г_3$ - нижче середнього;
$г_4$ - середній;
$г_5$ - вище середнього;
$г_6$ - високий;
$г_7$ - дуже високий.

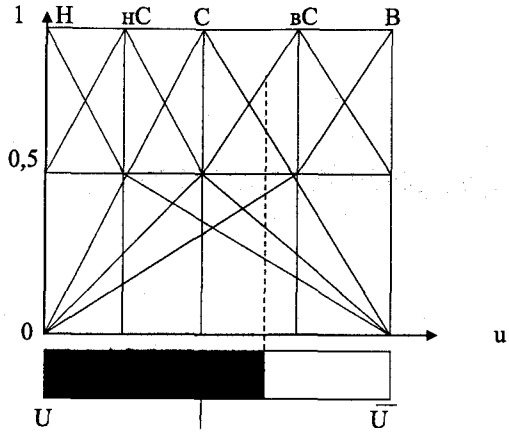


Рис.1. Функції приналежності нечітких термів (5-ти бальна система оцінки якості показника).

Для прикладу розглянемо систему оцінки за трьохбальною шкалою. Користуючись нечіткими термами *Н*-низький, *С*-середній, *В*- високий, які визначені за допомогою функції приналежності, задамо знання про співвідношення, у вигляді матриці (Таблиця 1). Кожна група рядків відображає умовне висловлювання, яке зв'язує нечіткі значення вхідних і вихідних змінних.

Наприклад, з Таблиці 1 видно, що умовою високого рівня загрози (r_3) інформаційної безпеки держави є висловлювання типу:

ЯКЩО $[(r_1=B)\ I\ (r_2=B)\ I\ (r_3=B)]$ *АБО* $[(r_1=B)\ I\ (r_2=B)\ I\ (r_3=C)]$

АБО $[(r_1=C)\ I\ (r_2=B)\ I\ (r_3=B)]$ *АБО* $[(r_1=B)\ I\ (r_2=C)\ I\ (r_3=B)]$

ТО R=B

Таблиця 1

r_1	r_2	r_3	R
B	B	B	B
B	B	C	
C	B	B	
B	C	B	
C	B	C	C
C	C	B	
B	C	C	
C	C	C	
H	B	B	
B	B	H	
B	H	B	
H	B	C	
C	B	H	
H	C	B	
C	H	B	
B	C	H	
B	H	C	
C	H	C	
C	C	H	
H	C	C	
C	H	H	H
H	C	H	
H	H	C	
B	H	H	
H	B	H	
H	H	B	
H	H	H	

Нечіткі логічні рівняння, поставлені у відповідність Таблиці 1, дозволяють оцінювати рівень загроз інформаційної безпеки України, а саме, вільному використанню результатів діяльності в галузі науки і техніки, для фіксованих значень окремих показників.

Високий рівень загрози інформаційній безпеці України (вільному використанню результатів діяльності в галузі науки і техніки):

ЯКЩО / (r_1=*B*) / (r_2=*B*) / (r_3=*B*) / TO R=B
ЯКЩО / (r_1=*B*) / (r_2=*B*) / (r_3=*C*) / TO R=B

ЯКЩО / (r_1=*C*) *І* (r_2=*B*) *І* (r_3=*B*) / ТО R=B
ЯКЩО / (r_1=*B*) *І* (r_2=*C*) *І* (r_3=*B*) / ТО R=B

Або узагальнююче правило

ЯКЩО / (r_1=*B*) *І* (r_2=*B*) *І* (r_3=*B*) / *АБО* / (r_1=*B*) *І* (r_2=*B*) *І* (r_3=*C*) / *АБО* / (r_1=*C*) *І* (r_2=*B*) *І* (r_3=*B*) / *АБО* / (r_1=*B*) *І* (r_2=*C*) *І* (r_3=*B*) / ТО R=B

Середній рівень загрози інформаційній безпеці України (вільному використанню результатів діяльності в галузі науки і техніки):

ЯКЩО / (r_1=*C*) *І* (r_2=*B*) *І* (r_3=*C*) / ТО R=C
ЯКЩО / (r_1=*C*) *І* (r_2=*C*) *І* (r_3=*B*) / ТО R=C
ЯКЩО / (r_1=*B*) *І* (r_2=*C*) *І* (r_3=*C*) / ТО R=C
ЯКЩО / (r_1=*C*) *І* (r_2=*C*) *І* (r_3=*C*) / ТО R=C
ЯКЩО / (r_1=*H*) *І* (r_2=*B*) *І* (r_3=*B*) / ТО R=C
ЯКЩО / (r_1=*B*) *І* (r_2=*B*) *І* (r_3=*H*) / ТО R=C
ЯКЩО / (r_1=*B*) *І* (r_2=*H*) *І* (r_3=*B*) / ТО R=C
ЯКЩО / (r_1=*H*) *І* (r_2=*B*) *І* (r_3=*C*) / ТО R=C
ЯКЩО / (r_1=*C*) *І* (r_2=*B*) *І* (r_3=*H*) / ТО R=C
ЯКЩО / (r_1=*H*) *І* (r_2=*C*) *І* (r_3=*B*) / ТО R=C
ЯКЩО / (r_1=*C*) *І* (r_2=*H*) *І* (r_3=*B*) / ТО R=C
ЯКЩО / (r_1=*B*) *І* (r_2=*C*) *І* (r_3=*H*) / ТО R=C
ЯКЩО / (r_1=*B*) *І* (r_2=*H*) *І* (r_3=*C*) / ТО R=C
ЯКЩО / (r_1=*C*) *І* (r_2=*H*) *І* (r_3=*C*) / ТО R=C
ЯКЩО / (r_1=*C*) *І* (r_2=*C*) *І* (r_3=*H*) / ТО R=C
ЯКЩО / (r_1=*H*) *І* (r_2=*C*) *І* (r_3=*C*) / ТО R=C

Або узагальнююче правило

ЯКЩО / (r_1=*C*) *І* (r_2=*B*) *І* (r_3=*C*) / *АБО* / (r_1=*C*) *І* (r_2=*C*) *І* (r_3=*B*) / *АБО* / (r_1=*B*) *І* (r_2=*C*) *І* (r_3=*C*) / *АБО* / (r_1=*H*) *І* (r_2=*B*) *І* (r_3=*B*) / *АБО* / (r_1=*B*) *І* (r_2=*B*) *І* (r_3=*H*) / *АБО* / (r_1=*B*) *І* (r_2=*H*) *І* (r_3=*B*) / *АЬО* / (r_1=*H*) *І* (r_2=*B*) *І* (r_3=*C*) / *АБО* / (r_1=*C*) *І* (r_2=*B*) *І* (r_3=*H*) / *АБО* / (r_1=*H*) *І* (r_2=*C*) *І* (r_3=*B*) / *АБО* / (r_1=*C*) *І* (r_2=*H*) *І* (r_3=*B*) / *АБО* / (r_1=*B*) *І* (r_2=*C*) *І* (r_3=*H*) / *АБО* / (r_1=*B*) *І* (r_2=*H*) *І* (r_3=*C*) / *АБО* / (r_1=*C*) *І* (r_2=*H*) *І* (r_3=*C*) / *АБО* / (r_1=*C*) *І* (r_2=*C*) *І* (r_3=*H*) /*АБО* / (r_1=*H*) *І* (r_2=*C*) *І* (r_3=*C*) / ТО R=C

Низький рівень загрози інформаційній безпеці України (вільному використанню результатів діяльності в галузі науки і техніки):

ЯКЩО / (r_1=*C*) *І* (r_2=*H*) *І* (r_3=*H*) / ТО R=H
ЯКЩО / (r_1=*H*) *І* (r_2=*C*) *І* (r_3=*H*) / ТО R=H

ЯКЩО $/ (г_1=Н) / (г_2=Н) / (г_3=С) /$ ТО R=H
ЯКЩО $/ (г_1=В) / (г_2=Н) / (г_3=Н) /$ ТО R=H
ЯКЩО $/ (г_1=Н) / (г_2=В) / (г_3=Н) /$ ТО R=H
ЯКЩО $/ (г_1=Н) / (г_2=Н) / (г_3=В) /$ ТО R=H
ЯКЩО $/ (г_1=Н) / (г_2=Н) / (г_3=Н) /$ ТО R=H

Або узагальнююче правило

ЯКЩО $/ (г_1=С) / (г_2=Н) / (г_3=Н) /$ *АБО* $/ (г_1=Н) / (г_2=С) / (г_3=Н) /$
АБО $/ (г_1=Н) / (г_2=Н) / (г_3=С) /$ *АБО* $/ (г_1=В) / (г_2=Н) / (г_3=Н) /$
АБО $/ (г_1=Н) / (г_2=В) / (г_3=Н) /$ *АБО* $/ (г_1=Н) / (г_2=Н) / (г_3=В) /$
АБО $/ (г_1=Н) / (г_2=Н) / (г_3=Н) /$ ТО R=H

Завдяки нечітким методам й, взагалі, теорії нечіткого мислення, експертові, легше знайти оптимальне рішення. В даному випадку це рішення стосується оцінки рівня загроз національної безпеки держави.

Переваги розглянутої методики оцінки рівня загроз інформаційній безпеці України, а саме, вільному використанню результатів діяльності в галузі науки і техніки.

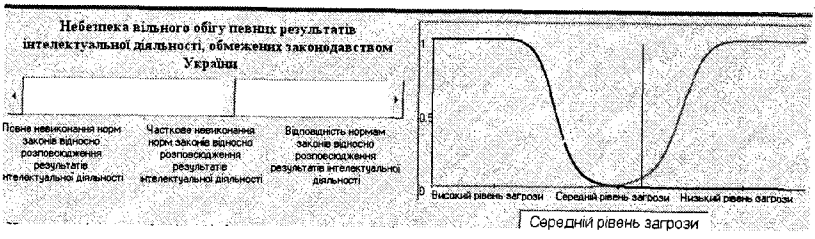
Розглянута нечітко-множинна методика оцінки рівня загроз інформаційній безпеці України, а саме, вільному використанню результатів діяльності в галузі науки і техніки, має наступні переваги:

- вона відтворює розумові процеси людини, основані на суб'єктивних судженнях;
- нечіткі моделі найбільш адекватні не тільки до об'єкта, що досліджується, але й до специфічних особливостей суб'єкта оцінки (оцінюючої особи);
- при знаходженні комплексного показника рівня загроз інформаційної безпеки України, а саме, вільному використанню результатів діяльності в галузі науки і техніки, використовується не просто адитивний узагальнений показник, а здійснюється згортання значень приналежності до тих або інших термів лінгвістичних змінних, що забезпечує коректність використовуваної нечіткої моделі;
- нечітко-множинна методика враховує невизначеність без використання імовірнісних розподілів оцінок показників, що особливо підходить для випадків, коли відповідні процеси не є стохастичними, або коли їхні імовірнісні оцінки не можуть бути отримані через непрезентабельність або неоднорідність відповідних вибірок.

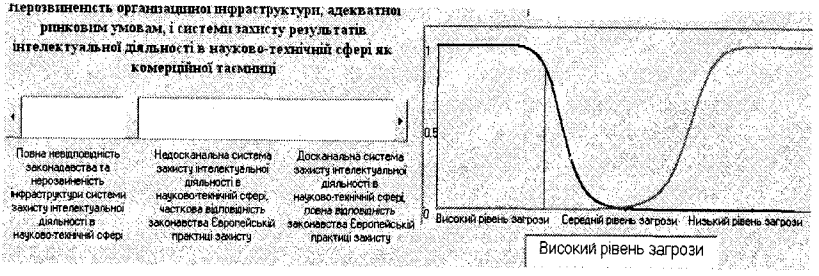
Результати роботи системи оцінки рівня загроз інформаційній безпеці України, а саме, вільному використанню результатів діяльності в галузі науки і техніки, можуть бути представлені у вигляді програмного комплексу.

Оцінюється кожен показник:

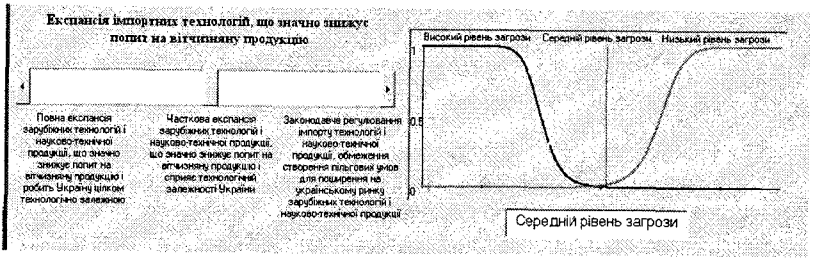
r_1 – небезпека вільного обігу певних результатів інтелектуальної діяльності, обмежених законодавством України;



r_2 – нерозвиненість організаційної інфраструктури, адекватної ринковим умовам, і системи захисту результатів інтелектуальної діяльності в науково-технічній сфері як комерційної таємниці;



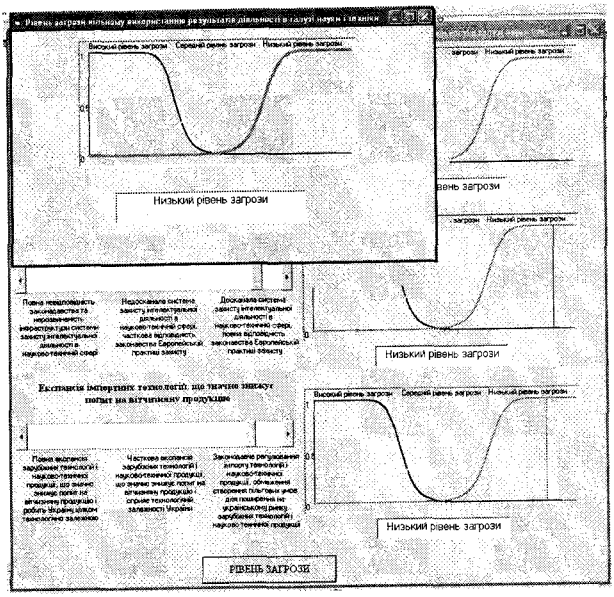
r_3 – експансія імпортних технологій, що значно знижує попит на вітчизняну продукцію.



І в результаті отримаємо значення загального інтегрального показника рівня загроз інформаційній безпеці України (вільному використанню результатів діяльності в галузі науки і техніки), який оцінюється сукупністю пріоритет-

них ознак, які характеризують інформаційну безпеку в галузі науки і техніки, і включає в себе показники r_1, r_2, r_3.

$$R=f_R(r_1, r_2, r_3)$$



Використання методів нечіткої логіки для задач прийняття рішень та оцінки в міжнародних відносинах, а саме для оцінювання рівня загроз національній безпеці держави, дозволяє максимально наблизити математичну модель оцінки якості до логіки міркувань кваліфікованих спеціалістів, які приймають оціночні рішення. Побудова нечітких експертних систем, які грунтуються на запропонованій методиці, дає можливість не лише оцінити якість, але і створює умови для її проектування, тобто такого управління вхідними показниками, при якому інтегральний показник буде приймати бажане значення.

3.7. Інформаційна політика та інформаційна безпека України на сучасному етапі

Концептуальні засади національної інформаційної політики. Системна цілеспрямована інформаційна політика покликана, насамперед, забезпечити реалізацію наступних стратегічних напрямів розвитку суспільства і держави:

1. Захисту конституційних прав та свобод громадян в інформаційній сфері,

- свободи висловлювання й права на поінформованість.

2. Протидії структурам міжнародної організованої злочинності, що зловживають прозорістю світових інформаційних потоків.
3. Інформаційного-аналітичного забезпечення діяльності ЗМІ, владних, наукових, господарчих та інших структур.
4. Пришвидшеного входження України до європейського та світового інформаційного простору.
5. Розв'язання протиріч між національною нормативно-правовою базою та європейським та міжнародним законодавством в інформаційній сфері тощо.
6. Розвитку в Україні "*електронного урядування*" на засадах пришвидшеного розвитку національного сегменту Інтернету та впровадження новітніх медіа-інформаційних технологій.
7. Формування бюджету розвитку, який стимулював би примноження "людського капіталу" й протидіяв "*відпливу мізків*" з України.
8. Стимулювання "інтелектуальної економіки" на засадах нормативно-правової бази, спрямованої на ефективний захист в Україні інтелектуальної власності, інтелектуальних продуктів і боротьбу з проявами "*піратства*".

До побудови глобального та європейського інформаційного суспільства нині залучені усі інтелектуальні, політичні та економічні еліти провідних світових держав. Інформаційні технології та інформаційно-комунікативні системи за нинішніх умов глобального цивілізаційного розвитку – ключовий ресурс суспільства та держави й необхідна передумова їх конкурентоспроможності на глобальних ринках. Саме інформаційна сфера здатна виступати провідним фактором реалізації найважливіших суспільних проектів динамічного розвитку, становлення громадянського суспільства, входження у світову спільноту тощо. Вона ж може за неуважного до себе ставлення перетворитися у фактор хаотизації й гальмування соціального, політичного, економічного й культурного розвитку.

Світ переживає епоху бурхливої інформаційної революції та формування глобального інформаційного простору, – переходу від індустріального суспільства до суспільства постіндустріального, інформаційного. Або ж, – за висловом американського мислителя О. Тоффлера, – суспільства «*Третьої Хвилі*».

Значимість інформаційного вектора розвитку засвідчують й такі концептуального змісту документи, як ухвалена у липні 2000 р. країнами "Великої Вісімки" Окінавська хартія глобального інформаційного суспільства та Програма інтеграції України до Євросоюзу, п.13 якої є входження України до глобального та європейського інформаційного суспільства.

Пришвидшено розвиваються світова мережа Інтернету, а на її засадах – електронна комерція, електронне врядування тощо. Формуються мультимедійні комплекси і цілі нетрадиційні галузі дистанційного навчання, праці і

управління. Але поки що більшість із зазначеного стосується України вельми опосередковано. Існує чимало інших проблем, пов'язаних з елементарною непоінформованістю України про те, що діється в світі та у світі — про Україну, яка є порівняно новим державно-політичним феноменом.

Брак достовірної інформації про Україну у світі створює передумови для інформаційної ізоляції нашої країни, яка нині сприймається світовою спільнотою переважно як "*туманний острів*" з невизначеними перспективами. Звичайно така тенденція підсилює хуторянські настрої у самій Україні. Певні позитивні зрушення намітилися після славнозвісного Майдану, але вони поки що остаточно не закріпилися ані в суспільній свідомості, ані в суспільному бутті.

Досить зауважити, що Україна є однією із небагатьох європейських країн, яка не спромоглася ухвалити закон "Про свободу інформації" (йдеться про правові гарантії доступу громадян до офіційної публічної інформації) та комплексну програму розвитку інформаційного суспільства типу "*Електронної України*" (справа закінчилася першим читанням у Верховній Раді у 2003 році).

Для будь-якого соціуму із українським включно завжди актуальною є проблема розв'язання суперечності між необхідністю підтримання інформаційної безпеки як кожної особистості зокрема, так і суспільства в цілому і об'єктивною загрозою обмеження у виняткових випадках права на приватність взагалі та приватність інформації зокрема. Такий стан речей актуалізує дослідження реального стану і можливостей розв'язання зазначеної проблеми пошуку того припустимого балансу між інформаційною відкритістю та закритістю у законодавчо-нормативних актах та в системі управління держав з розвинутою демократією, який, власне, й становить предмет інформаційної безпеки у широкому розумінні цього поняття.

При цьому важливо зауважити, що держава залишається головним "гравцем" на інформаційно-політичному полі доти, поки вона активно "грає" на інформаційне випередження. В іншому разі вона ризикує перетворитися на політичного аутсайдера аж до ризикованої перспективи стати заручницею не лише певних економічних угруповань, але навіть структур організованої міжнародної злочинності. Такі держави, згідно термінології, прийнятої у Стратегії національної безпеки США (2002 р.) називають "помилковими" (failure states).

Інформаційна безпека — це завжди балансування між інформаційною відкритістю та закритістю, між двома прагненнями: максимально розширити доступ громадян до невтаємниченої публічної інформації (державної, комерційної, наукової, освітньої, персональної тощо) й максимально захистити інформацію корпоративного й приватного змісту.

У свою чергу, право на отримання й розповсюдження інформації (ст. 9 та ст. 10 Закону України "*Про інформацію*") часто не лише de jure, але й de facto суперечить праву на захист інформації від небажаної особи, організації,

установи тощо. Дану колізію намагається розв'язати ст. 47 вищезгаданого закону, яка передбачає відповідальність, що її несуть особи, які поширюють несанкціоновану інформацію.

Дійсна проблема полягає у тому, що витримувати баланси інтересів особистості, суспільства й держави у *"глобальному суспільстві ризиків"* (Ульріх фон Бек) вдається дедалі важче. Президент російського "Медіасоюзу" Олександр Любимов у даному контексті свого часу зазначав, що „після Дубровки з'явилося розуміння того, що право на життя важливіше від права на інформацію".

Погоджуючись із цією слушною думкою, важко не висловити водночас застереження, що обмеження на діяльність мас-медіа, виправдані надзвичайними умовами та моніторинг засобів масової комунікації державою за умов антитерористичної війни може призвести (і насправді призводить) до наступу на основні громадянські свободи включно із правом на інформацію, на висловлення думок, на таємницю приватного життя тощо.

Поки що виглядає на те, що міжнародне співтовариство Україні відводить роль пасивного користувача інформаційних товарів і послуг, хоча вона жодним чином не ухиляється від продуктивного міжнародного співробітництва в інформаційній сфері, враховуючи досвід найрозвиненіших країн (США, Канади, Японії, Німеччини, Франції, Англії). Йдеться про підтримання динамічної конкуренції, забезпечення відкритого доступу до інформаційно–телекомунікаційних систем та універсального доступу до інформаційних продуктів та послуг.

Прикладом світової інтелектуальної конкуренції є відкриття в 1999-2000 роках у США, Німеччині та інших провідних країнах значної квоти (до 100 тис. річно) робочих місць для програмістів з числа громадян України та інших держав СНД.

Для країн, що розвиваються, у тому числі і для України, вагомим чинником економічного зростання в інформаційній галузі стає участь на ринку офшорного програмування (на якому Індія, наприклад, заробляє біля 4 млрд. доларів річно).

Сучасний етап розвитку людства є переходом до інформаційного суспільства й глобальної інформаційної економіки (економіки знань), коли практично зникають межі національних та регіональних ринків, кардинально зближуються сфери виробництва і споживання, вкрай загострюються різноманітні ризики, виклики тощо.

Приватна власність включно із медіа-власністю встановлювалася в Україні часто-густо поза правилами відкритої конкуренції й рівних умов приватизації. Тому структура медіа-ринку змінюється радше відповідно до структури політичних інтересів, аніж до об'єктивних ринкових законів балансування попиту й пропозиції.

Стан економіки взагалі також не стимулював досі можливості рекламного ринку, а відтак – існування мас-медіа як прибуткового бізнесу. Подібна

олігополія на ринку ЗМІ зумовила орієнтацію українських мас-медіа не на збут якісного інформаційного продукту, а на забезпечення інформаційного впливу на громадян. Володіння ЗМІ перетворилося таким чином не стільки на вид отримання прибутку, скільки на важливу частку політичного капіталу. А це вкрай небезпечно, як для журналістів, так і їх аудиторії.

Тим часом, глобальна інформаційна сфера, темпи розвитку якої у світовому вимірі перевищують нині 20 % річних, стрімко трансформує економічне, соціальне та суспільно-політичне життя світової спільноти і національних держав. Інформаційні ресурси, ступінь їх розвиненості і використання визначатимуть місце конкретної країни в світовій системі економічних і політичних відносин у XXI столітті.

Метою національної інформаційної політики України є створення умов для побудови в Україні розвиненого інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захисту національних моральних і культурних цінностей, забезпечення конституційних прав на свободу слова та вільний доступ до інформації.

Саме таке тлумачення пропонує ухвалена у 2002 р. Верховною Радою України *"Концепція національної інформаційної політики"*, – досить різнобічний документ, який складається із 11 розділів й охоплює майже усі основні сфери інформаційної діяльності, починаючи від мас-медіа й закінчуючи музейною справою. До честі розробників цього документу слід зауважити, що їм вдалося витримати "золоту середину" між екстенсивним та інтенсивним підходами. З одного боку, тут намічені національні пріоритети у глобальному інформаційному проектові, а, з іншого, - сформульовані суто конкретні тактичні завдання у розбудові національного інформаційного простору.

Отже, найголовнішим завданням національної інформаційної політики є, в остаточному підсумкові, входження України у глобальне інформаційне суспільство. Для цього потрібно:

- модернізувати національну інформаційну інфраструктуру, створивши або запозичивши відповідні інформаційні технології;
- повною мірою реалізувати конституційні права громадян, суспільства та держави на інформацію;
- розв'язати низку актуальних проблем становлення та розвитку національних інформаційних ресурсів, інформаційно-аналітичного забезпечення діяльності владних, наукових, господарчих та інших структур;
- у стислі терміни розвинути принципово нові напрями інформаційної діяльності, починаючи від електронного мережевого урядування й управління й закінчуючи електронною мережевою торгівлею тощо.

Основним напрямом національної інформаційної політики визнано підвищення інтелектуального творчого рівня вітчизняних виробників інфор-

маційного продукту (включно із продуктом медійним), досягнення їхньої конкурентоспроможності на світовому та вітчизняному медіа-інформаційному ринку. Бо лише конкурентоспроможне на світовому рівні інформаційне виробництво може гарантувати реалізацію національних інтересів в інформаційній сфері. І навпаки, жодні державно-адміністративні заходи протидії "*інформаційній експансії*" та забезпечення "*інформаційного суверенітету*" в епоху глобалізації не можуть бути ефективними.

Водночас, доцільно зауважити, що головні рушійні сили становлення й розвитку інформаційного суспільства є не стільки національними, скільки інтернаціональними за своїм походженням й характером. У свою чергу, це підтвердив Всесвітній саміт з інформаційного суспільства під егідою ООН, перший етап якого відбувся в грудні 2003 р. в Женеві, а другий – в листопаді 2005 р. в Тунісі.

Напередодні першого етапу цього саміту Міжнародний союз електрозв'язку (International Telecommunication Union) оприлюднив показники інформаційного розвитку країн світу (у долях від одиниці). Україна із показником 0,43 потрапила до списку країн із середнім рівнем доступу до інформаційних ресурсів, який відкриває Білорусь (0,49) й замикає Вірменія (0,30).

Обсяги світової інформаційної індустрії уже на початку 90-х років досягли 2 трлн доларів на рік, а через 10 років зросли майже на порядок. Для порівняння: світові видатки на військові цілі у цей же період 90-х років сягали біля 800 млрд. доларів США на рік. Сьогодні в інформаційній сфері працює біля півмільярда осіб, щороку створюється понад 10 млн. нових робочих місць. У США, Японії та інших розвинутих країнах у ній зайнято майже 60 % працюючого населення та створюється більше 50% ВВП.

Загалом епоха глобальної "інтелектуальної економіки" руйнує межі національних та регіональних ринків, кардинально зближує виробництво й споживання, підвищує роль неурядових акторів й, зокрема, ТНК, загострює боротьбу за такий специфічний ресурс як інтелектуальний людський капітал.

Але про остаточне відмирання інформаційно-регулятивних функцій держави в умовах глобалізації поки що говорити зарано. Практика інформаційної політики розвинених держав світу засвідчує, що, поряд із лібералізацією та дерегулюванням, для створення сприятливих економічних та політичних передумов пришвидшеного розвитку інформаційної галузі, вони посилюють важелі впливу держави на цю сферу.

Зокрема, саме національні держави виступають чи не найбільшими виробниками інформаційного продукту на національному рівні й найбільшими "промоутерами" інформаційної експансії приналежних до даних держав компаній.

У США понад 60 % відомостей про діяльність держави продукується самою ж американською державою, а інформаційна сфера перебуває під безпосередньою увагою президента, який безпосередньо контролює реалізацію Програми розвитку національної інформаційної інфраструктури.

Необхідною складовою Програми технологічного розвитку ЄС є Європейська стратегічна програма інформатизації, головна мета якої – скорочення технологічного відставання від США і Японії та зменшення залежності в інформаційних технологіях від цих країн. Як відомо, на саміті ЄС у Лісабоні навесні 2000 р. ухвалено нову програму просування Європи до інформаційного суспільства, що передбачає випереджувальний розвиток інформаційної сфери.

Щодо української точки зору, то вона полягає у тому, що державі передусім належить провідна роль гаранта цілісності національного інформаційного простору, ефективного координатора розвитку інформаційних ресурсів. Для цього держава має бути спроможною забезпечити:

1. Становлення та розвиток в Україні інформаційного суспільства на засадах ефективного регулювання й стимулювання інформаційного обміну, заохочення позитивних мотивацій щодо виробництва та споживання інформаційного продукту та надання різноманітних інформаційних послуг.
2. Становлення "правил гри" у єдиному інформаційному нормативно-законодавчому полі, обов'язкових для усіх, хто більшою або меншою мірою причетний до діяльності у національному інформаційному просторі, незалежно від його походження, форм власності тощо.
3. Визначення нормативних засад і меж діяльності зарубіжних та міжнародних (транскордонних) суб'єктів у національному інформаційному просторі України
4. Захист інтересів України у світовому інформаційному просторі, у міжнародних інформаційних відносинах.
5. Розвиток інформаційної (електронної) економіки, інформаційного врядування, шляхом заохочення впровадження сучасних комп'ютерних інформаційних технологій в усі сфери систем державного управління, фінансово-банківської й підприємницької діяльності, освіти, медицини, правової допомоги тощо.
6. Належний стан власності держави на провідні об'єкти національної культурно-інформаційної спадщини, належної бази здійснення державного регулятивного впливу на суспільні відносини у сфері інформації.
7. Захист інформаційних ресурсів (електронних мереж, банків і баз даних тощо) від несанкціонованого доступу або руйнації, розробку й впровадження відповідних засобів захисту.
8. Забезпечення широкого доступу громадян, навчальних, наукових та інших установ і організацій усіх форм власності, органів державної влади та регіонального й місцевого самоврядування, суб'єктів підприємницької діяльності до інформаційних ресурсів включно із засобами мережі Інтернет.
9. Функціонування державної системи професійного навчання і підвищення кваліфікації працівників інформаційної сфери та ЗМІ, наукової та експериментальної діяльності.

10. Інформаційну безпеку суспільства, особи й держави у якнайповнішому розумінні цього поняття.

Водночас, на вітчизняного виробника медіа-інформаційного продукту та на Українську державу нині чинять помітний тиск іноземні виробники та державні й міжнародні структури, які лобіюють їхні інтереси. Часто-густо такий тиск має форму звинувачень у недоброчесній конкуренції тощо. Звичайно, низка таких претензій є цілковито обґрунтованими, але вистачає й необґрунтованих.

В Україні складається загальне враження, що часто йдеться не про альтруїстичні наміри допомогти нашій країні розвинути медіа-інформаційний ринок і на гідних умовах увійти до європейських та світових медіа-ринків, а, радше навпаки, — про бажання витіснити українського виробника з власного медіа-інформаційного ринку, поставити його у залежність від виробника іноземного. А відтак, — раз і назавжди завоювати цей потенційно багатий український ринок.

Підсумовуючи, можна констатувати, що в інформаційній сфері, окрім позитивних, склалися також негативні тенденції, що посилюють загрози національним інтересам України у внутрішньополітичній сфері та шкодять її міжнародному іміджу.

Найважливішою проблемою в сфері вдосконалення інформаційної політики України є формування її стратегії та визначення пріоритетів. Інформаційна політика держави повинна бути переглянута докорінним чином і забезпечити прискорені темпи адаптації українського суспільства та держави до реалій глобального та європейського інформаційної суспільства.

Ключовим напрямом такої політики має стати підвищення інтелектуального, творчого, технічного рівня вітчизняних виробників інформаційного продукту, підвищення їхньої конкурентоспроможності на світовому інформаційному ринку. Лише розвинене конкурентоспроможне на світовому рівні інформаційне виробництво може гарантувати реалізацію національних інтересів у інформаційній сфері, вирішити завдання ефективного інформаційного забезпечення державної політики в інших сферах.

Нагальні завдання держави мають бути спрямовані на реалізацію комплексу заходів щодо:

- забезпечення належної прозорості та інформаційної відкритості в діяльності усіх без винятку органів державного управління та місцевого самоврядування;
- впорядкування структури та функціонування державних органів, що формують інформаційну політику держави та забезпечують відповідну безпеку в медіа-інформаційній сфері;
- створення цілісного нормативно-правового поля із регламентації розвитку національного інформаційного простору і відповідних сучасних технологій, діяльності господарюючих суб'єктів, забезпечення прав особистості, суспільства і держави на інформацію;

- посилення ролі держави, як рівноправного і конкурентоспроможного суб'єкта інформаційних відносин, виробника і поширювача інформаційного продукту і послуг на внутрішньому і зовнішньому інформаційному просторі;
- реформування інформаційної діяльності органів державної влади у напряму адаптації до використання новітніх інформаційних технологій.

У кінцевому підсумку, основним напрямом національної інформаційної політики має стати не протекціонізм щодо вітчизняного виробника, а підвищення інтелектуального, творчого, технічного рівня вітчизняних виробників інформаційного продукту, підвищення їхньої конкурентоспроможності на європейському та світовому інформаційному ринку. Бо лише розвинене й конкурентоспроможне інформаційне виробництво може гарантувати реалізацію національних інтересів в інформаційній сфері.

Інформаційна політика в сфері безпеки й безпека інформаційної діяльності в Україні. Нерозвиненість інформаційної складової у діяльності соціуму в цілому, й державних структур зокрема, призводить до послаблення двосторонніх комунікативних зв'язків між владою і суспільством та окремими верствами й групами суспільства. А це загрожує не лише непорозуміннями у державному центрі між різними гілками влади, але й непорозуміннями між центром та регіонами. Небажаним наслідком тут може стати порушення інтегральної цілісності держави, соціального миру й ладу тощо.

Зазначене значною мірою є наслідком того, що вітчизняні ЗМІ не стали в масі своїй повноцінними органами "масової комунікації" у точному розумінні цього поняття, але навіть за критеріями масовості охоплення аудиторії усе ще не відповідають поняттю "масового інформування".

Разом з тим, варто нагадати що Конституція України (ч.1, ст.17) визначає забезпечення інформаційної безпеки як одну з найважливіших функцій держави і справу всього народу. У свою чергу, Концепція (основи державної політики) національної безпеки від 1997 року та відповідний Закон від 2003 року серед основних напрямів державної політики виокремлюють безпеку в інформаційній сфері, визначаючи основні напрями її розвитку і основні загрози національним інтересам у даній сфері. Про теж саме йдеться у проектові *Стратегії національної безпеки.*

Нині український соціум виразно усвідомлює той факт, що головною загрозою в інформаційній сфері є можливість витіснення України з ринку інформаційних послуг та технологій. Уже на сьогодні це обертається чималими економічними втратами та надмірною залежністю від імпорту. Зрештою, від розвиненості ринку інформаційних послуг та технологій залежить і модернізація вкрай застарілої матеріальної інфраструктури ЗМІ. Відповідно, в діях структур влади стали набагато помітнішими ознаки інформаційної політики й медіа-супроводу політичних рішень на усіх етапах їх підготовки, прийняття та імплементації.

Варто нагадати, що Національна програма інформатизації діє з 1998 року, але все ще здійснюється без належної системності. Далекими від досконалості є міжвідомче узгодження робіт з інформатизації на галузевому та регіональному рівнях. Досі не здійснено комплексної перевірки ефективності використання бюджетних коштів на виконання цієї Програми та для потреб інформатизації поза нею. Не забезпечене належне фінансування проектів інформатизації з Державного бюджету України.

Зокрема, на Програму інформатизації з року в рік планується півтора-два десятки мільйонів гривень, тоді як на виконання робіт з інформатизації поза межами цієї Програми витрачаються сотні мільйонів із державної казни. Така ситуація з фінансуванням *"де-факто"* є усталеною, тобто щороку держава витрачає на ці та інші проблеми кошти в основному поза діючою Програмою. Тоді незрозуміло, для чого укладаються подібні Програми і якою має бути їх регулятивна роль в державі.

Існує, принаймні, три головних аспекти інформаційної безпеки — технологічний, комунікативний та психологічний. При чому, інформаційно-психологічна безпека, найближча до характеру діяльності ЗМІ, передбачає державний та громадянський контроль за діяльністю усіх установ, організацій та приватних осіб, які вдаються до інформаційно-психологічних засобів впливу на масову та індивідуальну свідомість. Адже за певних умов можна завдати непоправних збитків суспільному та індивідуальному здоров'ю. А тому свобода висловлювання й незалежність ЗМІ у жодній цивілізованій країні світу не означають їх повної безконтрольності. Інша справа, хто, як і на яких засадах вповноважений здійснювати подібний контроль.

До головних загроз в інформаційно-психологічній сфері доцільно віднести:

- протиправне застосування спецслужбами іноземних держав та міжнародними злочинними угрупованнями впливів, здатних зруйнувати єдиний інформаційно-духовний простір України, традиційні засади суспільства та його моральності, порушити інші життєво важливі інтереси особистості, суспільства та держави;
- цілеспрямовані інформаційно-психологічні операції антиукраїнського змісту, що реалізуються шляхом опрацювання, виготовлення і поширення негативних інформаційно-психологічних впливів із застосуванням спеціальних засобів і методів такого впливу;
- протиправне застосування кримінальними і напівкримінальними структурами спеціальних засобів впливу на індивідуальну, групову і масову свідомість, здатних заблокувати на неусвідомленому рівні свободу волевиявлення людей, прищепити їм синдром залежності.

Дії певних політичних сил, спрямовані на маніпулювання суспільною свідомістю, яке призводить до:

- втрати цілими суспільними групами, верствами або окремими людьми, що їх представляють, спроможності до політичної, культурної та морально-етичної самоідентифікації;

- зловживання свободою масової інформації з метою протиправного розкриття таємниці персональних даних;
- використання ЗМІ з метою обмеження права людини на вільний вибір переконань;
- зловживання свободою совісті та світогляду з метою насаджування деструктивних культів;
- пропаганди низькопробних зразків масової культури, заснованих на культі насильства та цінностях, що суперечать традиційним морально-етичним нормам суспільства та його окремих верств;
- обмеження законного права людини на захист її духовно-інтелектуальної діяльності та власності;
- руйнації культурно-просвітницьких систем та систем збереження й пропаганди культурних цінностей включно з музейними, бібліотечними та архівними фондами тощо.

Достатньо зауважити, що:

- близько 60% ефірного часу телерадіотрансляцій заповнено продуктом неукраїнського походження;
- кабельними мережами розповсюджується переважно сигнал провідних російських телекомпаній (ОРТ, РТР, НТВ), передачі яких доволі часто мають антиукраїнську спрямованість.

До зазначеного слід додати:

- низький загальний рівень художньо-естетичної і публіцистичної якості передач (лише одиниці з тих біля 1100 ТРО, які отримали ліцензії, виконують свої програмні зобов'язання, – ефір натомість заповнюється примітивною зарубіжною маскультурою);
- стихійний, без належного нормативно-правового регулювання, розвиток кабельного телебачення та сучасних цифрових технологій мовлення;
- занепад вітчизняної електронної промисловості, зокрема, зі створення сучасної приймальної апаратури, та відсутність науково-дослідницької підтримки телерадіоінформаційної галузі;
- мляве впровадження цифрових стандартів, яке вимагає заміни парку телеприймачів, тоді як купівельна спроможність населення низька; водночас існує рішення Європейської конференції Адміністрацій Пошт і Телекомунікацій про припинення ліцензування телерадіоорганізацій аналогового мовлення, внаслідок чого Україна може опинитися у інформаційній ізоляції й буде вилученою з європейського інформаційного простору.

Низький якісний стан національної системи телерадіомовлення призводить до подальшого падіння популярності та впливовості цих ЗМІ і падіння їх конкурентоспроможності у порівнянні з іноземними мовниками.

Україна суттєво поступається не тільки розвиненим країнам, але і Російській Федерації у сфері впровадження новітніх комп'ютерних інформаційних технологій.

Це стосується, зокрема, стану, темпів та нормативно-правового забезпечення розвитку національної складової глобальної інформаційної мережі Інтернет, яка, з огляду на світовий досвід, є перспективним засобом організації інформаційної підтримки усіх галузей управлінської, економічної та суспільної діяльності, набула ознак нового виду електронних засобів масової інформації.

Іноземні компанії контролюють левову частку рекламного бюджету інформаційного простору України. Недосконала нормативна база, досить ліберальна система ліцензування та недосконалість контролю за дотриманням національних інтересів у сфері електронних ЗМІ дозволили іноземному капіталу отримувати право мовлення на телеканалах загальнонаціонального рівня, уникнувши при цьому необхідності вкладати кошти в розвиток інформаційної сфери.

Такий стан створює небезпеку переважаючого інформаційного впливу на населення України іноземних інформаційних центрів, - передусім тих, що знаходяться під впливом окремих партій, політичних угрупувань, промислово-економічних груп тощо, які можуть переслідувати цілі, далеко не сумісні з національними інтересами України.

В Україні спостерігається тенденція до концентрації та монополізації ЗМІ. Формуються потужні холдинги, які розглядаються фінансово-політичними угрупованнями як специфічні інструменти політичного впливу. Спостерігаються також тенденції до відтворення на українському ґрунті російської моделі медіа-холдингів, функціонування яких призвело у сусідній країні до формування джерел перманентної політичної нестабільності через постійні «інформаційні війни». Притаманне подібним структурам нехтування національними інтересами на користь власних може створити постійну загрозу національній безпеці.

Позиціонування українських ЗМІ у просторі національної безпеки.

Роль та місце ЗМІ у забезпеченні національної безпеки визначається насамперед їхньою роллю важливого чинника впливу на суспільно-політичну ситуацію та процеси її розвитку. ЗМІ недарма називають *"четвертою владою"*, бо це дійсно важлива соціальна інституція, яка формує політичні комунікації і без якої важко собі уявити як прямі, так і зворотні зв'язки між владою і суспільством. З цього погляду, певна опозиційність засобів масової інформації владі щодо чинної влади є явищем цілковито нормальним, притаманним усім демократичним країнам.

Але, щоб бути опозиційними щодо влади, конструктивно їй опонувати, ЗМІ мають бути економічно самодостатніми. І лише у цьому разі можна говорити про їх відносну незалежність і автономність. З іншого боку, надмірна за-

лежність мас-медіа від держави призводить до втрати ними ролі важливого інструменту формування громадянського суспільства, серйозно обмежує свободу висловлювання та відносну економічну самодостатність ЗМІ.

Нині в Україні нагромаджено понад 100 нормативно-правових документів, що регулюють інформаційну діяльність у сфері ЗМІ. Проте, досі не вирішено питання про кодифікацію зазначених правових актів, тобто затвердження *"Інформаційного кодексу"*. Залишаються юридично не врегульованими питання:

- використання багатоканальних супутникових, кабельних та стільникових телеінформаційних технологій;
- функціонування корпоративних комп'ютерних мереж типу Інтранету та Екстранету;
- діяльності у національному сегменті мережі Інтернет і, зокрема, - щодо регулювання Інтернет-видань, захисту національного домену "UA", ліцензування Інтернет-провайдерів;
- захисту та моніторингу інформації тощо.

Не опрацьовані також достатньо ефективні нормативно-правові механізми протидії тенденціям до монополізації ЗМІ.

Існують істотні розбіжності між законами «Про плату за землю» (1992 р.) і «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (1998 р.), що призводить до завищеного оподаткування (зокрема, - КРРТ).

Неврегульованою і суперечливою є тарифна і податкова політика щодо користувачів радіочастотного ресурсу України.

Існуюча в Україні система державних органів інформаційної політики (профільний Комітет ВРУ, Мінтранс із департаментом зв'язку, Держкомінформ, Національна Рада України з питань телебачення і радіомовлення, відповідні підрозділи в органах виконавчої влади і СБУ тощо) є надто громіздкою, а її діяльність нескоординованою як у центрі, так і на місцях. Більше того, останнім часом у діяльності цих органів намітились ознаки серйозних незгод і розбіжностей, що стають предметом не лише відкритої дискусії але і взаємних звинувачень на сторінках газет та екранах телебачення.

Результатом цього є невизначеність у розподілі функцій і повноважень, прийняття недостатньо скоординованих і виважених рішень, непослідовність намірів та практичних дій. Це призводить, у підсумку, до хаотизації інформаційного простору, яка не має нічого спільного зі свободою преси та висловлювань.

Зокрема, подібна неузгодженість зумовила невиправдані зволікання зі створенням Єдиної супутникової системи передачі інформації та її складової - супутникового телерадіомовлення та інших неприйнятних, з точки зору національних інтересів України, не виважених технічних рішень. Не створено також рівних умов оподаткування для користувачів радіочастотного ресурсу.

Існуючий канал супутникового мовлення на закордонну аудиторію переважно своїм сигналом "***гріє космос***", але аж ніяк не працює на користь Україні.

Закон України "Про інформацію", прийнятий ще в 1992 р., не враховує особливостей сучасних інформаційних технологій та перспектив участі України в інформаційному обміні. Відповідно, його слід доповнити наступними законами:

- "Про електронний підпис";
- "Про участь в інформаційному обміні";
- "Про електронну торгівлю";
- "Про порядок виділення і реєстрації доменних імен українському сегменті мережі Інтернет".

За чисто формальними ознаками стан друкованих ЗМІ можна вважати задовільним. Тим часом, майже катастрофічною є ситуація в українському книговидавництві й книгорозповсюдженні, оскільки ця галузь як за рівнем розвитку інфраструктури, так і за якісними показниками перебуває в занепаді, а економічні умови її функціонування обумовлюють високі ціни на українські видання (вдвічі вищі ніж на російські). Внаслідок цього, у 1990 р. видані в Україні мали аж три книжки й брошури. У 2000 р. – стосовно зазначеного показника – 0,25, а наприкінці 2002 р. – 0,1. Тим часом, відповідна Національна програма від 1994 р. передбачала цифру 10.

Варто принагідно нагадати, що Росія активно впроваджує податкові пільги для друкованої видавничої продукції. Зокрема, ще в червні 2000 року Держдума РФ, голосуючи за новий податковий кодекс, зробила виняток щодо сплати ПДВ для видань та медіа з питань науки, культури, освіти.

Явно недостатня увага приділяється розвитку і підтримці державних інформаційних агентств, на яких повинні покладатись завдання щодо оперативного донесення до української і світової аудиторії новин, які стосуються внутрішньої та зовнішньої політики держави, забезпечення «інформаційної присутності» України в найрозвиненіших країнах світу.

Серед десятків інформагентств, що працюють в Україні, лише одне - ДІНАУ - державне. До того ж, з боку центральних владних структур перевага щодо надання інформації часто віддається не державним, а інколи навіть не національним, інформагентствам.

Телерадіоінформаційна галузь, за ознакою зростання кількості телерадіокомпаній, теж начебто перебуває у стадії злету, але за більш глибокого аналізу виявляється, що галузь, особливо її державний сектор, знаходиться у незадовільному стані, ознакою якого є, зокрема:

- регіональна нерівномірність теле- і радіообслуговування населення України;
- технічне і технологічне відставання електронних ЗМІ;
- кризовий стан (фізична зношеність і моральна застарілість) інфраструктури вітчизняного телерадіомовлення, зокрема, діючих мереж і парку технічних засобів, які практично не оновлюються з 80-х років.

На сьогодні понад 70 відсотків телерадіомовного обладнання повністю відпрацювало свій ресурс, значна його частина знаходиться в аварійному стані, обладнання фізично та морально застаріло і є надзвичайно енергоємним. За розрахунками фахівців, фінансові потреби на модернізацію мереж складають понад 50 млн. доларів США.

Складним є фінансово-економічне становище радіотелевізійних передавальних центрів і компаній (що обумовлює технічний і технологічний занепад галузі). Так, провідна національна компанія, яка транслює інформацію на Україну і світ про політичні, економічні, культурні та інші аспекти життя країни – Концерн РРТ – знаходиться у надзвичайно складному фінансовому становищі, що межує з банкрутством. Аналогічна ситуація існує і в обласних радіотелевізійних передавальних центрах.

З нормативно-правової та безпекової точки зору, на особливу увагу заслуговують ключові поняття захисту духовно-інтелектуальної діяльності та власності на «національний інформаційний продукт», виготовлений «національним інформаційним виробником».

В Україні досі законодавчо не окреслені належним чином поняття власності творчого журналістського колективу на створений ним інтелектуальний продукт (статтю, радіо-, телепередачу тощо). Так само неврегульованими залишаються юридичні відмінності між "*засновником*" та "*власником*" ЗМІ. Дані аспекти є винятково важливими, оскільки від їх юридичного тлумачення залежать процедури ліцензування ЗМІ, визначення податкових умов їх економічної діяльності тощо.

Тлумачення цих термінів має, зокрема, безпосереднє відношення до тих українських ЗМІ, які функціонують як партнери провідних російських та інших закордонних ЗМІ. Як відомо, тут існують істотні розходження точок зору щодо статусу таких видань, як «*Комсомольская правда в Украине*», «*Известия-Украина*» тощо. Творчі колективи вважають ці видання українськими з тією лише особливістю, що, відповідно до підписаних угод, вони купують інформацію у своїх російських партнерів. Але органи влади час від часу пред'являють претензії до зазначених та інших подібних видань, які зводяться до звинувачень в тому, що вони нелегально або напівлегально завозять в Україну виготовлений у сусідній країні інформаційний продукт, обходячи таким чином українське оподаткування та ставлячи українських колег в умови нерівної конкуренції.

У будь-якому разі, питання щодо регулювання діяльності іноземних та "напівіноземних" ЗМІ в Україні залишається поки що невирішеним. Воно є особливо актуальним, якщо йдеться про радіомовників, оскільки не є особливою таємницею, що чимало українських радіокомпаній не виробляють свій продукт самостійно, а ретранслюють популярні іноземні радіостанції, - переважно російські. При цьому не лише виникають нерівні умови конкуренції, але в українських виробників інформації зникають стимули для створення власного інформаційного продукту. По суті, виникають проблеми із того ж са-

мого ряду, що й проблеми поширення як в Україні, так і за її межами так званої піратської продукції, відтиражованої в Україні.

Якщо справи так підуть і надалі, то можемо в найближчій перспективі взагалі втратити творчих людей, здатних до виготовлення національного інтелектуального продукту. В епоху інформаційної революції це дуже небезпечна загроза.

Адже йдеться не лише про виробника, але й масового споживача, про формування сучасних стандартів споживання. Налаштувавшись на інформаційний "секенд", український споживач масової інформації може, образно кажучи, відвикнути харчуватись із позначкою "Мейд ін Юкрейн". Із цієї точки зору РНБО України хвилює доля вітчизняного кінематографа, телемистецтва тощо.

Водночас, зі звинуваченнями в «інформаційній експансії», які лунають на адресу деяких ЗМІ з боку їх конкурентів, слід бути вкрай обережними. Не варто будь-яку інформацію з України й про Україну, яка виходить від іноземних ЗМІ, вважати актом інформаційної експансії.

По-перше, інформаційний простір – не місто або дачна ділянка, які можна обгородити парканом. Він завжди буде прозорим або напівпрозорим, а про стратегію інформаційної закритості, властиву радянським часам, слід забути. Інша справа, що ми самі ще не навчилися використовувати зазначену інформаційну прозорість для обстоювання власних національних інтересів.

По-друге, про медіа-експансію можна говорити лише в разі проведення іншими державами (із сусідами України включно) спеціальної політики, здатної деструктивно впливати на формування громадської думки в Україні, дестабілізувати внутрішню ситуацію тощо.

Так само некоректними у більшості своїй є звинувачення на адресу деяких ЗМІ у розголошуванні державних таємниць. Тут має спрацьовувати «презумпція невтаємниченості». Тим більше, що від радянсько-компартійних часів ми успадкували погану звичку втаємничувати багато чого із того, що є "*таємницею Полішинеля*". На це працюють чисельні перші відділи, спецсховища в бібліотеках тощо. Власне на цій манії втаємничування й була заснована тоталітарна система, яка не лише політично, але й морально-психологічно остаточно не подолана й донині.

Якщо усе зазначене підвести під певний "спільний знаменник", то йдеться, зрештою, про проблему дотримання балансу між демократичною еволюцією суспільства і регуляторною функцією держави.

Здається, з цієї ж "опери" цілий ряд питань, які виникають у процесі спілкування журналістів з органами державної влади, а представників влади з журналістами. Якщо абстрагуватися від усім відомих фактів відвертого використання ЗМІ в політичному або економічному протиборстві, то йдеться, з одного боку, про малоуспішні спроби журналістів отримати більш-менш об'єктивну інформацію щодо перебігу соціально-політичних процесів в Україні, щодо намірів та дій влади.

І справа тут, звичайно, не в журналістах, більшість з яких професійно роблять свою справу й задовольняють право людей на поінформованість. Справа в деяких державних "достойниках", яким слід, нарешті, визначитись, хто і що вповноважений компетентно говорити в кожній конкретній ситуації. Слід розвинути інститут не лише прес-секретарів, але й речників, які покликані компетентно інформувати ЗМІ, а в потрібних випадках організовувати медіа-кампанії на підтримку тих або інших рішень. При чому, – організовувати ці кампанії на дійсно професійному рівні, не вдаючись до підмоги так званих темників. Зрештою, це питання довіри до влади як такої й престижності державної служби.

Сьогодні суспільство болісно відчуває, зокрема, відсутність цілеспрямованої медіа-кампанії на підтримку аграрної реформи на селі. Теж саме стосується геостратегії та зовнішньої політики. Скажімо, відправка українського військового контингенту до Кувейту й Іраку в 2003 році або питання ймовірного вступу України до Альянсу, яке актуалізувалося у 2006 році, – усе це акти політичної волі частини політичної еліти, але не більшості населення. А це означає, що такі контроверсійні дії влади слід легітимізувати засобами масового інформування хоча би з позицій здорового глузду й "заднього розуму".

Влада ставить, наприклад, питання про європейську й євроатлантичну інтеграцію України, але за відсутності цілеспрямованих медіа-інформаційних кампаній, які орієнтували б людей у плані європейського вибору й євроатлантизму, руйнували би застарілі стереотипи, упередження й забобони. Адже не секрет, що у свідомості багатьох українців НАТО й США сприймаються не як союзники, а як джерела потенційних загроз.

Не менше стереотипів і упереджень щодо України й Росії як спадкоємниць колишнього СРСР накопичилося за роки холодної війни на Заході. Але лише з 2001 року почала діяти громадська організація "Відома Україна" (Ukraina Cognita), яка мала би посприяти формуванню позитивного міжнародного іміджу нашої країни, але робить це, як і інші подібні структури, без помітних успіхів.

Прикрі інциденти типу того, що трапився у жовтні 2001 р. із потраплянням української ракети у літак з ізраїльськими пасажирами, а ще раніше – у житловий будинок в Броварах, трагедія, що сталася під час авіашоу у Скнилові, уже хронічні вибухи на складах у Новобогданівці, – усе це завдало тяжкого удару по репутації українських Збройних Сил, а відтак і по репутації України як держави. Дехто в іноземних, і навіть вітчизняних, ЗМІ звідси почав робити далекосяжні висновки про нежиттєздатність української незалежності тощо. Звичайно, таким спробам слід давати відсіч. Але відсіч дієву й аргументовану.

Для цього існують певні правила й антикризові стратегії, які називаються репутаційними й мають пряме відношення до так званої екстремальної журналістики. Адже від різних малих та великих прикрощів, які завдають

ударів по репутації окремих лідерів, політичних діячів, корпорацій, фірм, банківських організацій і навіть — по репутації цілих країн ніхто не застрахований. Уміння журналістів діяти в ситуаціях подібних криз надзвичайно важливе.

У сфері медіа-інформаційної політики слід формувати, так би мовити, певні ієрархічні правила гри й своєчасно інформувати про них ЗМІ, що дозволить зняти, якщо не всі, то більшість проблем довкола проблем забезпечення свободи слова в Україні. Що останнім часом в Україні активно робиться. Але це бажання влади запропонувати ЗМІ "*правила гри*", максимально наближені до інформаційної прозорості, викликає спротив тієї частини журналістів, які вбачають у конфронтації з владою мало не показник свого фахового рівня. Зрозуміло, що така журналістика виступає не позитивним фактором врегулювання суспільних та політичних конфліктів, а навпаки, - сама є джерелом перманентної конфліктності. Відверто кажучи, такі журналісти не стільки вболівають за загальнодержавні справи, скільки виконують волю власників ЗМІ, в яких працюють. Спрацьовує й конфронтаційна логіка виборчої боротьби з її запеклою боротьбою за медіа-ресурс. На жаль, така логіка в Україні продовжує діяти, не дивлячись на те, що парламентські вибори закінчилися навесні 2006 року, а президентські відбудуться лише за 3 роки.

З іншого боку, самим журналістам слід опрацювати і включити в свій морально-етичний професійний кодекс певні правила висвітлення діяльності владних органів. Критикувати певні персоналії можна і потрібно. Але справою вкрай негідною і, за великим рахунком, непрофесійною є спроби атакувати цілі державні інституції лише тому, що їх представляють не ті люди, яких хотілось би бачити на відповідних посадах авторам так званих компроматних інформаційних матеріалів та замовникам цих матеріалів.

Тут є та морально-етична межа, яку за жодних умов не варто переходити журналісту, який справді поважає свою професію. І, чим швидше це зрозуміють окремі журналісти і цілі журналістські колективи, тим конструктивніше у них будуть укладатися стосунки не лише з владою, але й з власними читачами, глядачами та слухачами, тим вищим буде ступінь довіри до масмедіа.

Загалом, проблема низького професіоналізму та творчого рівня української журналістики є вкрай актуальною. Жоден закон не змусить журналіста творчо розвиватися, не створить талановитого журналіста. Так само до внутрішніх проблем журналістського середовища слід віднести небажання журналістів займатися досудовим, корпоративним розглядом конфліктів на, скажімо так, "*судах журналістської честі*". Адже відомий євангельський вислів на подібну тему стверджує, що, часом, замість того, щоб шукати скалку у чужому оці, краще пошукати поліно у своєму власному.

Зазначене жодною мірою не знімає відповідальності з чинної влади, яка все ще "по-совєцьки", за відомою ленінською формулою, що стосується "колективних пропагандистів й організаторів", хотіла би поводитися з мас-медіа,

не даючи їм можливості перетворитися у конкурентну "*четверту гілку*" влади.

Повертаючись до проблем діалогу влади із ЗМІ, варто зауважити, що особливо актуальним є питання спілкування журналістів з регіональними органами державної влади. Бо, знову ж таки, не є таємницею той факт, що для представників ЗМІ набагато складніше отримати інформацію у губернатора або його заступників, аніж у міністра або іншого представника центральних органів влади. Інакше кажучи, влада на місцях, зазвичай, не звикла рахуватись з "четвертою владою", є менш демократичною, значно закритішою і менш налаштованою на зворотні зв'язки за посередництвом ЗМІ з громадянами. Зрештою, – більш безконтрольною з боку громадських структур й навіть органів місцевого самоврядування. Є навіть приклади не просто нетактовності, а відвертої грубості щодо журналістів, яку дозволяють собі деякі можновладці на місцях.

У кінцевому підсумку, найголовнішою проблемою інформаційної політики та інформаційної безпеки України є її потенційна й реальна здатність "вписатися" в координати світового розвитку як органічної складової європейського й глобального інформаційного суспільства.

3.8. Вплив зарубіжних концепцій розвитку пострадянських держав на інформаційну безпеку України

Україна 1991 року прийшла до незалежності цілковито несподівано. Ця теза багато кому неприємна, але її слід розвинути і в тому сенсі, що в державі була відсутня елементарна політологія і адекватна вимогам нового часу політекономія капіталізму.

Численні концепції і програми ринкового реформування і запровадження суспільної демократії, що розроблялися науковцями-ентузіастами і направлялися до владних інститутів та нових політичних партій України, навіть у тих випадках, коли вони більш-менш адекватно враховували західні розробки та досвід, наштовхувалися на бар'єри нерозуміння або ідеологічних ілюзій.

На допомогу були запрошені все ті ж західні фахівці, які, як згодом з'ясувалося, були цілковито неспроможні зрозуміти національні, регіональні і місцеві особливості. Водночас їм була надана практично нічим не обмежена можливість доступу до будь-якої державної інформації під приводом необхідності врахування в розробці програм розвитку. Водночас вони своїми часто чужими українським реаліям пропозиціями вносили розгардіяш в інформаційне поле нової держави.

Згодом Україну буквально заполонили зарубіжні спеціалісти, котрі, як це відомо більшості з нас, у повному розумінні слова «виманювали» потрібну їм інформацію про політичні сили, події, процеси і явища. Таємниця інформації на якийсь час фактично в державі була повністю зруйнована.

У не менш складній ситуації опинилися вітчизняні засоби масової інформації. Ейфорія незалежності і свободи слова подекуди виливалася у вседозволеність. Річ і у тім, що журналістам явно бракувало відповідного наукового забезпечення, що могло б посприяти правильному науковому розумінню ними того, що відбувається в державі і суспільстві. Міжнародний, у першу чергу західний, досвід ідеалізувався і подавався як взірець для обов'язкового врахування українською владою, політичними силами, підприємствами тощо.

Основні положення та ідеї. Серед базових результатів дослідження даної проблематики найбільш суттєвими встановлення, доведення чи підтвердження низки чинників, які продовжують справляти як позитивний, так і цілковито деструктивний вплив на інформаційну безпеку нашої держави. Причому розглядаю цю наукову і суспільну категорію звужено, тобто майже винятково у контексті формування національних концепцій і програм розвитку. У них часто-густо не беруться до уваги такі з'ясовані мною чинники:

- Наявність принципових і сутнісних диспропорцій у західних політологічних і економічних оцінках реформ в перехідних суспільствах пострадянського типу. Відповідні розходження спричиняють помилкові, часом деструктивні рекомендації практичного характеру. Яскравим прикладом практичного застосування відповідного інформаційного багажу і теоретичних ідей у цьому контексті можна вважати майже одностайну підтримку українськими ЗМІ лібералізації економічних відносин, що вилилася в цілковиту втрату державою і суспільством контролю за ходом приватизації. Де-факто, вона стимулювала руйнацію навіть тих підприємств, які були здатні вписатися в конкуренцію не тільки на вітчизняному, а й світових ринках. Поклавши в основу своїх підходів фінансово-економічну та політичну ідеологію міжнародних валютно-фінансових організацій, щирі прихильники прискорених реформ, схоже, просто забули, що наука є, насамперед, критикою усталених підходів. У випадку з пострадянськими особливостями на це додатково накладалися руйнівні накопичення століть життєдіяльності в умовах тоталітарних режимів і вседозволеності влади, що стала джерелом переважно незаконного збагачення.
- Помітні розходження між положеннями, висновками і рекомендаціями політологів і економістів, спричинені різними, але кожного разу значимими методологічними похибками. Вітчизняна міжнародно-політична думка ідеалізувала Захід як цілісність, часом повністю ігноруючи притаманний його представникам прагматизм, у тому числі й на рівні порад. Для них, зокрема, поряд з власне темпами і якістю українського поступу до ринкової економіки і суспільної демократії іншим над-завданням нібито було прагнення за будь-яку ціну і якомога швидше включити Україну в сферу західних впливів. Тим часом, ще в радянські часи в Українській РСР існували серйозні наукові підтвердження того факту, що для «старої» Європи і Сполучених Штатів наш континент у політично-

му вимірі завершується на західних кордонах колишнього СРСР. Це, наприклад, за всіх суперечностей, викликаних відомою ідеологічною одновимірністю, переконливо показав у своїй докторській дисертації О.Потехін. Елементарне ознайомлення з положеннями і висновками цієї дисертації давало можливість зрозуміти, що пріоритетом для західних державних адміністрацій і політикуму будуть держави, які радянська і західна наука відносила до Східної Європи, а з легкої руки, професора М. Кірсенка – до Центрально-Східної Європи. Хоча цей відомий історик пропонував віднести до цього регіону і Україну, на практиці це мало значення переважно тільки для політичного і політологічного дискурсу. Насправді ж, із появою у 1994 році американської Стратегії розширення і задіяності стало ясно, що політичний Захід або трансатлантична спільнота у ближче десятиліття мала бути поповнена винятково за рахунок традиційної Східної Європи + прибалтійські республіки колишнього СРСР, котрі завжди сприймалися у Вашингтоні та інших західних столицях як незаконно захоплені сталінським режимом. В українських ЗМІ, тим часом, буквально оспівувалася перспектива швидкого включення нашої держави в європейський і євроатлантичний інтеграційний процес.

- Не помічалося при цьому і те, що окремі західні експерти прямо ставили під сумнів сам факт наявності власної національної історії в українців. Зокрема, нинішній активний прихильник української незалежності професор Колумбійського університету (США) Марк фон Хаген у статті під кричущою назвою "Чи є в України історія" відносив українців до «неісторичних народів». Взагалі ж, ігнорувалася популярна в західній політичній думці теза про те, що неісторичними фактично нібито є всі народи, які, перебуваючи у складі імперських формувань, не належали до титульних націй. Такими заявами штучно заперечувалося, що в українському випадку мова йде не про «творення нової нації», на зразок, скажімо, американської чи канадської, а про суспільно-політичну консолідацію та об'єднання громадян держави, котра має велику, хоча й суперечливу передісторію. Паралельно важко давалося українським фахівцям і журналістам усвідомлення того, що в національній історії закладені витоки недооцінки власного національно-державного та інтеграційного потенціалу. Мало хто шукав саме у цій сфері причини антинаціональних деформацій у підходах і діях лідерів лівих політичних партій України. З іншого боку, у повному розумінні слова націонал-демократичними ЗМІ мусувалися висновки деяких істориків, котрі "увічнювали" той факт, що процес формування власне українського етносу протікав у дуже складних зовнішніх і внутрішніх умовах, збігаючись з періодом феодальної роздробленості Київської Русі. При цьому такі автори уникали порівняльного аналізу, який підтверджував, що аналогічною свого часу була ситуація, скажімо, в Італії та Німеччині, які

прийшли до єдності через багатовікові внутрішні і зовнішні територіальні колізії. У такий спосіб відбувалося руйнування позитивного *історико-політичного дискурсу, який мав вирвати державу і суспільство* з лещат як недооцінки національного потенціалу, так і його небезпечного переоцінювання.

- Кардинальні неузгодженості між позиціями сучасних західних аналітиків (як економістів, так і політологів) та експертами й управлінцями міжнародних валютно-фінансових організацій, з позицією яких частіше збігаються програмні підходи вищих ешелонів влади ключових акторів західного співтовариства націй. Що стосується науковців, то вони ідеалізували можливість швидкого запровадження так званих євро-американських критеріїв суспільного розвитку в пострадянських умовах. Поступово ця теза була підхоплена українськими фахівцями і журналістами, перетворившись у певне заклання, на тлі якого йшло первісне накопичення капіталу насправді з використанням західного досвіду, але періоду переходу від феодальних до капіталістичних відносин. Тобто, в Україні насправді був перейнятий західний досвід, але зовсім не той, що мався на увазі розробниками концепцій реформування української політичної системи. На цьому тлі вітчизняні нувориші, підпорядкувавши собі більшість ЗМІ, поблажливо дозволяли говорити і писати про доцільність залучення західних критеріїв до української політичної і економічної практики, переважно аби виглядати прихильниками відповідних цінностей.

Найбільш помітним недоліком західних підходів до аналізу перехідних суспільств пострадянського типу є очевидне ігнорування чи недостатнє врахування об'єктивно і неминуче критичних тенденцій становлення нових *політичних і економічних відносин. Наслідком стають поспішні, більше розраховані* на розвинуті західні демократії і, частково, на постсоціалістичні перехідні суспільства Центрально-Східної Європи, а тому часто малоприйнятні в поточній життєдіяльності пострадянських держав претензії, висновки і рекомендації критеріального характеру. Вони бувають повністю неспроможними вже тому, що базуються на ідеальному варіанті, до того ж, у його західному представленні й поданні. Воно, в силу своїх особливостей, зокрема, неспроможне оптимально врахувати поточні особливості світосприйняття в українському суспільстві та його елітах. Тим часом, неоднозначний досвід перебування України у складі СРСР підтверджує висновок про суспільні небезпеки спроб втілити політичні ілюзії, якою виявилася й комуністична ідея, в життєдіяльність держави. В певному сенсі такою ж ілюзією на перехідному етапі, як переконала практика перших 12 років незалежності, є і маніпулятивні, у своїй здебільшого пропагандистській спрямованості, спроби відстоювати ідеї прискореного впровадження принципів західної демократії та ліберальної ринкової економіки за відсутності належного підґрунтя в суспільстві й політикумі.

Критичним тут стало мимовільне підтримування чи й навіть провокування окремими інформаційними та аналітичними матеріалами антизахідних настроїв серед представників нового бізнесу, які вбачали у надто швидкій реалізації пропозицій західних експертів загрози своїм особистим інтересам. З огляду на те, що саме цей прошарок населення зайняв домінуючі позиції в засобах масової інформації, здійснювалася цілеспрямована ідеологізація позиції західних експертів, результатом чого стало додаткове стимулювання масового негативізму до Заходу як політичної системи.

Поглиблений аналіз уможливлює й такі положення, висновки та ідеї для тих, хто в Україні займається питаннями інформаційної безпеки, яка значною мірою залежать від вміння критично оцінювати рекомендації, що йдуть від західних науковців і політиків.

Західні економічні школи переважно здійснюють свій аналіз на суто економічних показниках і статистичних даних, які виводяться з класичних і неокласичних теорій і концепцій реформувань ринкових систем, а також з урахуванням домінуючих на Заході стратегій економічного розвитку. Зі свого боку, провідні західні політологічні школи основують свої позиції та загальні оцінки здебільшого на даних, пов'язаних з впливами громадянського суспільства, зокрема, наявністю законодавчої та політико-системної можливостей здійснення контролю за розробкою й реалізацією рішень загальнодержавного характеру. В обох випадках закладені теоретико-методологічні вихідні, які спричиняють очевидну упередженість висновків і рекомендацій. Річ у тім, що рекомендації і критеріальні вимоги основуються на аналізі не просто "ідеальної" ситуації, взятої з життя, але саме такої, що штучно формується на рівні мислення та уявлень людей, вихованих в радикально інших умовах. Відтак, закономірно спостерігаємо поступове відчуження між уявною системою у поданні західних аналітиків і реальними позиціями значної частини української громадськості. Спроба методами інформаційного нав'язування прискорити перехідний етап від командної економіки і тоталітарної політичної системи до лібералізму і демократії справила зворотній вплив, спричинивши якраз сповільнення цих процесів.

Втім, проблему не слід зводити до штучності об'єкту дослідження, яким є пострадянська держава, та його формальне створення як модельованого образу. Не менш важливо, що реально існуючий об'єкт, яким є економічні показники і відповідна статистика перехідних суспільств, аналізовані західними економістами, безумовно, страждає на недосконалість. Існує проблема врахування наслідків розпаду колись єдиного економічного комплексу, суперечностей епохи первісного накопичення капіталів і неминучої після десятиліть командної економіки тінізації економічних відносин та фінансових потоків. Існуючих у відповідному наборі західних економістів методологій і теоретичних конструкцій тут явно не вистачає, що, виступає стимулом для об'єднання дослідницьких зусиль, які могли б бути покладені в основу концепції інформаційної діяльності в Україні.

З іншого боку, відсутність демократичної традиції і, як наслідок, досвіду впровадження й діяльності справді впливових організацій громадянського суспільства у поєднанні із закономірним процесом боротьби щойно створених груп фінансово-економічних інтересів за політичне домінування майже механічно породжує конфлікт між інтересами більшості громадян і означеними групами, до чого додається негативний вплив міжкланових суперечностей. Цей елемент політологами на Заході обговорюється чи, принаймні, декларується як такий, що береться до уваги. Але практично маємо справу із ще однією ілюзією, яка полягає в тому, що громадянське суспільство в організованій формі нібито в пострадянських державах може стати міцним і структурованим, ефективним і впливовим без відповідної фінансово-організаційної підтримки представників бізнесу. Тут існує й інша інформаційна крайність, а саме: часто-густо весь український бізнес подається в одному кольорі. Його безоглядна і не надто зважена дискредитація стає додатковим приводом для настороженості західних інвесторів, тим часом не відлякуючи російських капітал, що формувався в ідентичних умовах.

В українському випадку слід додати ще кілька суттєвих аспектів, які відносяться до чинників впливу на положення і висновки як економічних, так і політологічних досліджень. У першу чергу, маються на увазі політичні і політико-системні наслідки від збереження загальної залежності вітчизняної економіки від Російської Федерації. Відбувається, зокрема, парадоксальне явище: західні урядові інстанції сприяють відчуженню своїх корпорацій від України як країни з підвищеними ризиками, у той час як російські бізнесмени буквально вриваються в український економічний простір. Одним з виразніших наслідків є відсутність реального позитивного впливу на політичну систему в Україні, оскільки російський бізнес надто близький за своїми підходами і впливами до українського. Цей аспект в українському інформаційному просторі практично не проявляється.

Говорячи про відмінності у позиціях західних політологів і економістів, слід відзначити також, що для перших пріоритетними виступають теоретико-методологічні виміри дослідження перехідних суспільств, а факти з їхньої політичної дійсності виступають як би вторинними, наводячись на підтвердження або для заперечення певних заготовлених концептуальних постулатів. Західні економісти ж, як правило, більшого значення надають фактичному матеріалу, йдучи до розробки, підтвердження або заперечення рівня і якості використання перехідними державами теоретичних напрацювань через аналіз конкретних подій, процесів і явищ. Зрозуміло, що особливості пострадянських економічних систем також спричиняють передбачені заздалегідь висновки. В українському інформаційному полі вони тривалий час подавалися поза межами завжди доцільного критичного оцінювання.

Вдалося встановити й таке:

- Західні економісти й політологи, не пов'язані фінансуванням та іншими формами залежності з міжнародними валютно-фінансовими ор-

ганізаціями, схильні виразніше враховувати національні особливості розвитку перехідних суспільств. Як перші, так і другі в своїх оцінках не перебільшують формально самостійної ролі й ефективності теорії, котра переростає у програму дій певної політичної сили, коли йдеться про специфіку розвитку конкретної посткомуністичної держави. У свою чергу, експерти й управлінці МВФ схильні оцінювати результати здійснюваних реформ переважно у межах відповідності певних трансформаційних програм прийнятим і затвердженим Фондом методів і підходів, часто-густо нав'язуючи власні варіанти реформування без огляду на особливості національних традицій і досвіду.

Наступне концептуальне положення, знову таки, логічно випливає з розходжень між політологами й економістами: експерти й управлінці Європейського Союзу та інших спільних структур Західної Європи більшою мірою ладні прислуховуватися до розробок і рекомендацій політологічних шкіл, а не тільки економістів, коли йдеться про перехід тієї чи іншої держави до ринкової економіки.

Що стосується рекомендацій, які подаються представниками різних політологічних шкіл, то тут їхні автори часом виходять за рамки принципу верховенства теорії, а тому бувають практично єдиними, принаймні на стратегічному рівні.

Українським інформаційним службам та державним інститутам, відповідальним за інформаційну безпеку, слід, врешті-решт, взяти до уваги і застосування, що суспільні перетворення в перехідних суспільствах посткомуністичного типу можуть здійснюватися ефективно тільки за двома логічними моделями:

- базованою на замкненій схемі перетворень, за якої наголос робиться на підготовці концепції та оцінці наслідків її впровадження, а також на проведенні попередніх консультацій держави з експертами-практиками, представниками громадськості і політичних партій. Вважається і підтверджується реаліями, що у такому випадку підготовка реформ є тривалішим у часі процесом, але основні теоретичні положення набувають статусу безсумнівних і роблять програми трансформацій стійкішими;
- основаною на відкритій схемі реформувань, згідно з якою в ході трансформацій вносяться певні корекції з урахуванням набутого досвіду. Такі реформи, як правило, не відрізняються точністю і стійкістю, нерідко призводять до відхилень від стратегічного курсу, коригувань та доповнень. Тут на практиці важливішим стає процес, а не спосіб досягнення політичного консенсусу стосовно характеру реформ. Практично всі західні економісти й політологи стверджують, що в Україні початково існував намір скористатися замкненою схемою перетворень, але жодна з наукових концепцій не могла бути покладена в основу реформувань з огляду на відсутність консолідованої політичної нації та обурювані зсе-

редини і ззовні розходження між регіонами. При цьому, вважають вони, в новій незалежній державі так і не знайшлося політичної сили, спроможної висунути прийнятну і ефективну національну ідею. Спроба зробити такою європейський вибір поки що також відображена переважно в президентських указах і розпорядженнях, а також заявах і деклараціях урядовців.

Окрема, більш консолідована позиція західних політологів виглядає так: Україні не вдалася організація дієвого громадського контролю за ходом реформ, причиною і наслідком чого стало тотальне засилля кланів та груп інтересів. Вказується, що пересічний український виборець продовжує демонструвати неспроможність до так званого згуртованого голосування, базованого на усвідомленому використанні існуючих концептуальних розробок, які мали б доводитися до широких мас населення в адекватних для розуміння формах засобами масової інформації.

З першого погляду, ця оцінка виглядає цілковито об'єктивно і максимально відповідною підходам, притаманним українській політології. Однак надто часто тут зустрічається зміщення причинно-наслідкових зв'язків. Або наблизитися до істини та представити у вигляді завершеної і підтвердженої інформації більше слід розглянути проблему в іншому ракурсі, а саме: триваюча політизація бізнесу нищить паростки громадянського суспільства у його класичному західному сприйнятті. Відтак, пересічний український виборець часто, в умовах владного домінування олігархічних структур, просто змушений вибирати між революційною боротьбою і суспільною стабільністю. Перша, відкидається на, умовно кажучи, генетичному рівні внаслідок історичного досвіду, який переконує в тому, що російські і українські революції ніколи не приносили для народу стратегічно стійких позитивних результатів соціально-економічного і суспільно-демократичного характеру. Окремі наслідки помаранчевої революції тільки посилили таке ставлення народу, хоча сам факт її здійснення говорить про можливість нового вибуху масового невдоволення. Влада не має перебільшувати відомого висновку про те, що суспільна стабільність сприймається українцями більш важливою, ніж примарна перспектива прилучитися до благ західного варіанту і моделі розвитку. Насправді ж, індекс соціальної напруги у суспільстві вже сьогодні настільки високий, що подальше нагнітання негативів, як це, наприклад, вкрай кваліфіковано, але майже завжди провокаційно робиться в «*Свободі слова*», може виштовхнути показники цього індексу за розумні межі.

Нашим ЗМІ явно бракує позитиву. Ми ж навіть безсумнівні соціальні досягнення попередніх двох урядів зуміли подати в сенсі повного негативізму. Буквально все розчинено в зручній для цього тезі про популізм.

Чергова позиція західних політологів, коли йдеться про рекомендаційну частину, полягає в тому, що жодна з концепцій і програм економічного реформування в Україні не була доведена до логічного завершення. Остаточно не була обрана ні закрита, ані відкрита схема. Засилля груп інтересів та перетво-

рення економічних кланів у політичних монстрів позбавляє державу можливості стабільних трансформувань на політико-економічних принципах і засадах, максимально адекватних національним інтересам країни. Напевне, в даному випадку маємо найбільш адекватний висновок, з якими важко не погодитися за всієї критичності. Адже проблема тут набуває часом абсурдних вимірів в контексті стратегічних інтересів самих кланів та їх ключових представників. Не здійснюючи поетапних реформ за кращими світовими зразками, більше того стримуючи ці реформи, ця верства українського суспільства штучно віддаляє входження України в демократичну спільноту націй, гарантоване впровадження конкурентних відносин замість використання владного домінування кланів, а тим самим і позбавляє стійкості їх власний стан і перспективу. Але такий підхід і відповідне оцінювання у нас поступово втрачають свої впливи або й зовсім стають формою самоствердження окремих журналістів і експертів.

Далі відзначимо, що важливим є пошук причин відставання України у здійсненні економічного реформування саме у політичній сфері, зокрема, - політичної культури, традицій, особливостей світосприйняття тощо. Важко аргументовано сперечатися з тезою західних колег про безпосередній зв'язок між характером політичної системи, наявністю чи відсутністю консолідованої нації, ступенем національної свідомості управлінців всіх рівнів, з одного боку, та характером економічного реформування і ступенем його успішності, з іншого боку. Відтак, і базовий інформаційний інтерес України та українського суспільства на 15-му році незалежності залишається незмінним: сприяння формуванню громадянського суспільства та консолідованої політичної нації, масовому розумінню незаперечності прямої залежності між ступенем впливу громадськості на політиків і державних діячів та початком сталого економічного розвитку.

Протиборство у дусі холодної війни, як і попередні гарячі конфлікти, завершилися перемогою однієї із сторін. Фактичний перебіг подій показує, що Захід як переможець тривалий час діяв за традиційною схемою диктату стороні, яка потерпіла поразку. Україна опинилася у складі переможених. Згідно з авторською концепцією не варто ігнорувати інший елемент проблеми, яким є поведінка переможених. Оскільки ми віднесені до їх числа, то слід пригадати, що від самого початку життя в посткомуністичному світі громадяни незалежної України почувалися не переможеними, а переможцями. Більшість вважала, що західний світ сприймає перемогу над комуністичною системою і Радянським Союзом спільним здобутком — своїм і нашим. На рівні масового інформування не помітили, що такий підхід можна певною мірою віднести тільки до деяких постсоціалістичних країн Центрально-Східної Європи, а саме тих, які вважалися загарбаними Радянським Союзом. Можна пригадати хоча б Польщу, якій були списані гігантські зовнішні заборгованості або держави Прибалтики, котрим було одразу дано "*карт-бланш*" на приєднання до європейського співтовариства.

Відтак, і на міжнародній арені Україна, Росія, інші пострадянські нові незалежні держави почали діяти в межах концепції рівності, на яку внутрішньо не були згодні переможці, вбачаючи в нас недавніх опонентів з усіма відповідними наслідками. Для того, щоб переконати переможців у своєму праві приєднатися до них, переможеним слід було або стати, умовно кажучи, "*в позу*", обравши китайський чи в'єтнамський варіант суспільного розвитку, або ж, безумовно, виконувати вимоги, висунуті переможцями.

Формально було обрано другий варіант. Але з численних причин експеримент, спрямований на швидке здійснення ринкових реформ і демократизації, зазнав фіаско. Шлях до ринку і демократії виявися значно складнішим, ніж планувалося. У цій ситуації реальні переможці починають вважати себе обділеними: новий лад, який вони запропонували переможеним, не складається. Звідси – прагнення натиснути, змусити, підштовхнути. У відповідь – нерозуміння, розгубленість і навіть протидія.

Перефразовуючи відомі постулати мислителів минулого, слід зазначити: теорія мертва без практичного підтвердження, але й політичний та економічний процеси швидше зазнають деградації без активного людського пошуку на теоретичному рівні. З іншого боку, наука залишається вправою мислення окремого дослідника, допоки не знаходить реального замовника і споживача або не потрапляє в інформаційне поле, позитивно впливаючи на суспільство.

Сам характер політичної науки як специфічної галузі суспільствознавства обумовлює оцінку її ефективності. Якщо розробка і запровадження новітніх методологій і методів здатні привести до поглибленого розуміння своєї місії політиками і державними діячами, якщо у такий спосіб вдається підвищити вплив політології на рівень обізнаності мас, то таку спрямованість досліджень теоретиків можна і слід вважати доцільною, потрібною і корисною. Якщо ж, як це часто трапляється зі спробами математизувати політологію або механічно запровадити в неї апокаліптичні прогнозування, це робиться у формі данини тій чи іншій модній течії безвідносно до можливості сприйняття й практичного застосування тими, хто розробляє і впроваджує політичні рішення, а водночас і до впливу на масове світосприйняття, то висновок має бути протилежним. Політологію не слід плутати з тими чи іншими відгалуженнями філософської науки.

Мова йде про особливість політології, яка робить обов'язковим максимальне наближення її положень і висновків до потреб суспільного розвитку. Слід погодитися з політологами, які пов'язують рівень обізнаності й політичної активності громадян з характером політологічних розробок. Політолог М.Кундера ще в 1974 році писав, що "людина відповідає за свою необізнаність, необізнаність – це вада". Однак слід додати, що піднесення рівня політичної обізнаності мас належить до специфічних прерогатив і завдань представників саме політичної науки. Без такої спрямованості політологія

втрачає в ефективності, а самі політологи справедливо визначаються в контексті пошуку задоволення власних амбіцій. Якщо в Україні досі відзначається відносно негативне ставлення до європейського і особливо євроатлантичного вибору нашої держави, це рівною мірою є провиною політологів, істориків, філософів, журналістів, вітчизняного політикуму.

3.9. Медійні аспекти інформаційної безпеки України

Розгляд проблем інформаційної безпеки проводиться у складний для українських мас-медіа період. Наша країна давно перестала бути "*найбільш читаючою*". За рівнем насиченості періодичними виданнями на тисячу осіб населення вона значно відстає від інших країн світу. Ця ситуація є найбільшою загрозою інформаційній безпеці держави. У нас якось звикли з великою недовірою ставитися до всього, що містить слово "*безпека*". Багато хто в цьому відчуває якусь загрозу правам особи, демократичним свободам. Треба вже позбутися цього постсоціалістичного синдрому. В усьому світі інформаційна безпека визнана необхідною складовою нормального розвитку суспільства. У тих же Сполучених Штатах постійно діє Комітет з політики інформаційної безпеки, який очолюють заступник міністра оборони і директор ЦРУ. Зараз, згідно з директивою Президента США № 63 (1998 р.), розгорнута загальноамериканська система інформаційної безпеки. У грудні 1999 р. резолюцію з питань інформаційної безпеки прийняла Генеральна Асамблея ООН. Метою є вироблення міжнародних принципів, що спрямовані "на посилення безпеки глобальних інформаційних та телекомунікаційних систем" і сприяють "боротьбі з інформаційним тероризмом і криміналом". У червні того ж року була прийнята Концепція інформаційної безпеки держав-учасниць СНД.

У сусідній Росії була прийнята Доктрина інформаційної безпеки РФ. У лютому 2000 р. закон "Про інформаційну безпеку" був прийнятий у Бєларусі. Причому в Росії системи інформаційної безпеки будуються вже на регіональному рівні. В Новгородській області створена і працює Рада з інформаційної безпеки, у Хабаровському краї прийнята Концепція інформаційної безпеки краю, аналогічні кроки зроблені в Свердловській та Воронезькій області.

Важливість питання інформаційної безпеки чітко усвідомлюють представники інформаційного бізнесу. В липні 2000 р. компанія "Анна" запустила портал "Український центр інформаційної безпеки", що об'єднує біля 10000 тисяч ресурсів, присвячених цій проблемі.

Особлива увага саме до цієї складової загальної безпеки в Україні і світі обумовлена входженням суспільства у нову, інформаційну стадію розвитку. Зараз, завдяки вільним інформаційним потокам, світ перетворюється у своєрідне глобальне село, якщо говорити за Г.Маклюеном. Інформаційна революція, яка була викликана широким застосуванням комп'ютерної техніки

та інформаційних технологій, призвела до необхідності переглянути ряд ключових положень розвитку сучасного суспільства, в тому числі у сфері безпеки.

Ми звикли розуміти під захистом інформаційної безпеки перш за все якісь обмежувальні дії. Але це неправильно. Взагалі, під інформаційною безпекою прийнято розуміти стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. На жаль, законодавча база в цій галузі відстає від потреб практики. Ті закони та інші нормативні акти, які існують в цій сфері, мають, в основному, обмежувальний чи заборонений характер. Тобто безпека розуміється як захищеність інформації та інфраструктури, що її підтримує, від випадкових чи спеціальних втручань штучного або природного характеру, які можуть нанести шкоду власникам або користувачам інформації. Цей підхід явно застарілий. У наш час від держави потрібна не стільки заборона чи обмеження, скільки підтримка, організація та координація робіт. До речі, саме такий підхід превалює у цивілізованих країнах. У США вже більше десяти років діє Закон про комп'ютерну безпеку. Так от, наголос у цьому законі зроблений не на заборони, а на комплекс заходів з навчання користувачів, що мають справу з критичною інформацією, на підготовку роз'яснювальної документації тощо. Тобто це заходи для свідомого підтримання режиму безпеки.

До основних об'єктів інформаційної безпеки відносяться:

- особистість, її права та свободи;
- суспільство, його матеріальні та духовні цінності;
- держава, її конституційний лад, суверенітет та територіальна цілісність.

Які ж можуть бути загрози? Як зовнішні (недружня політика іноземних держав в області глобального інформаційного моніторингу, розповсюдження інформації та нових інформаційних технологій), так і внутрішні (протизаконна діяльність різних структур в області збору, обробки та передачі інформації, яка призводить до порушення прав громадян і організацій).

Для того, щоб побачити, які ж пріоритети мають інші держави у цій сфері, можна проаналізувати Доктрину інформаційної безпеки РФ. Першою з 4-х складових національних інтересів Росії в інформаційній сфері виділене дотримання конституційних прав і свобод людини, друге — це інформаційне забезпечення державної політики РФ, третє — розвиток сучасних інформаційних технологій і тільки четверте — захист інформаційних ресурсів. Як бачимо, наголос явно не на обмежувальні дії, а на розвиток.

Таким чином, інформаційна безпека держави буде забезпечена тільки у випадку ефективного та безперешкодного функціонування ЗМК. На жаль, якраз для цього у нас умови ще не створені. Українські газети абсолютно правильно у листопаді 2000 р. віднесли до найактуальнішої на той час загрози інформаційній безпеці дефіцит газетного паперу. А "Урядовий кур'єр" навіть виніс таке формулювання у заголовок.

Хоча й інших загроз вистачає. До них можна віднести ті значні фінансові труднощі, які зазнають регіональні газети, теле- й радіокомпанії, різке скорочення вітчизняного кіно- та відеовиробництва, погіршення матеріального стану журналістів, особливо, знов таки, в регіонах. Щорічно після закриття газет і журналів сотні журналістів залишаються без роботи. Одночасно посилюється тиск на журналістів економічними, політичними, судовими і адміністративними методами.

І одними законами чи іншими правовими актами тут нічого не вирішиш, бо треба відмітити, що в законодавстві України вже приділяється значна увага цій проблемі. Взагалі, Україна займає одне з перших місць в СНД за кількістю законів, присвячених діяльності мас-медіа. Але жоден із законів в інформаційній сфері не виконується у повному обсязі. Таким чином, справа не в законах, а в рівні їх виконання.

Тепер хотілося б конкретизувати загрози, які виникають в інформаційній сфері. Не секрет, що у ряді держав розробляються чи вже розроблені концепції інформаційних війн. Так, війну у Перській затоці чи в Югославії було виграно не тільки внаслідок бойових дій, але й спеціальних інформаційних операцій. Причому починалися вони задовго до початку бойових дій. Згадаємо, перед початком бомбардування Югославії міністр закордонних справ Великобританії Кук стверджував, що серби страчують по 2 тис. албанців на день. А коли Косово було захоплено, спеціальна комісія знайшла всього тільки трохи більше 2 тисяч трупів, причому ідентифікувати їх виявилося дуже важко. А у Перській затоці відразу після початку "*Бурі у пустелі*" на екранах американських телевізорів виникла заплакана арабська дівчина, нібито медсестра з кувейтського пологового будинку, яка розповіла жахливі речі про те, як іракські солдати викидали немовлят з барокамер і вбивали їх. Війна в Затоці була повністю морально виправдана в очах пересічних американців. А потім виявилося що та дівчина — донька кувейтського посла у Вашингтоні, а її слова — вигадка. Американці дуже пильно слідкують за тим, щоб журналісти висвітлювали події у вигідному для армії напрямку. Так, під час тієї ж війни з Іраком всі журналісти були зібрані у так звані пули і пересувалися тільки по затверджених американськими військовими коридорах. Тих же, хто випадав із загальної картини, відразу намагалися дискредитувати. Так, кореспондент ВВС Д. Сімпсон був звинувачений в тому, що піддався на сербську пропаганду за те, що він показав у репортажі сербів, які говорили про свої антинатівські настрої.

Складовою частиною інформаційних війн є кібервійни. Ще колишній президент США Б.Клінтон та Міністр оборони В.Коен підписали наказ про підготовку до кібервоєн. Вже зараз при цьому можуть використовуватися DdoS-атаки, комп'ютерні віруси, виведення з ладу комп'ютерів за допомогою електро- і радіоперешкод. Причому американське командування ставить ведення інформаційних воєн в один ряд із застосуванням балістичних ракет і контролем за космосом. До інформаційних воєн також активно готується і китайська армія.

Не можна оминати і такої загрози інформаційній безпеці особистості як психотронна зброя. Ми звикли ставитися до повідомлень про неї з недовірою, бо параноїків у нас і без всякої зброї вистачає. Але як сказав декан факультету інформаційної безпеки Московського інженерно-фізичного інституту А.Маланюк під час свого виступу у Державній Думі Росії на парламентських слуханнях, присвячених інформаційній безпеці: "останнім часом активно ведуться розробки методів і засобів комп'ютерного проникнення у підсвідомість людини і здійснення на неї глибокого впливу. Враховуючи безконтрольність розповсюдження комп'ютерних технологій, вплив яких на психіку має необмежені можливості, слід говорити про появу нової інформаційної зброї масового знищення".

Треба відмітити, що спецслужби розвинених країн світу активно використовують мережу Інтернет для моніторингу інформаційних потоків чи, простіше кажучи, відслідковування змісту веб-сайтів, електронної пошти, інформаційних запитів тощо. У нас широко критикувалося впровадження в Росії, а потім в Україні системи оперативно-розшукових заходів (російською – СОРМ –2), яка була спрямована на це. Але на Заході вже кілька десятиліть діє система "***Ешелон***", яка перехоплює повідомлення та аналізує їх зміст на предмет присутності підозрілих слів та висловів. За допомогою 120 супутників перехоплювалася інформація, що проходила телефонними лініями, радіо, супутниковим зв'язком. Існування цієї системи, яка була створена спецслужбами США, Великої Британії, Канади, Австралії та Нової Зеландії, приховувалося навіть від союзників по військовим блокам. Тільки після того, як 21 жовтня 1999 р. рух "Хактивісти" провів "*День боротьби з Ешелоном*" (вони пересилали якомога більше листів із словами "революція", "плутоній", "Північна Корея", "ЦРУ" тощо), Австралія визнала його існування. Євросоюз вже кілька разів розглядав питання діяльності Ешелону. З'ясувалося, що перехоплювалося навіть листування французьких та італійських дипломатів. Дані Ешелону активно використовувалися в економічному шпигунстві та допомозі вітчизняним фірмам. Так, в Європарламенті стверджувалося, що у 1994 р. в результаті того, що Агентство національної безпеки США прослухало та передав конкурентам зміст переговорів французької компанії "*Томпсон*" з бразильцями, був зірваний контракт на суму 40 млрд. франків. У 1995 р. Європейський консорціум Airbus Industry втратив контракт на поставку літаків у Саудівську Аравію після того, як його комерційна пропозиція була перехоплена і передана корпорації Boeing.

Але навіть масштаби Ешелону повністю не задовольняють потреб спецслужб. У Великій Британії був прийнятий закон, згідно з яким уряд отримав право відслідковувати електронну пошту громадян та декодувати криптовані повідомлення. Створена нова установа — Урядовий Центр технічної підтримки, яка буде діяти за схемою СОРМ-2. Тобто провайдери будуть зобов'язані протягнути виділену лінію в офіс цього центру. Різниця в тому, що уряд готовий відшкодувати провайдерам витрати на встановлення нового обладнання (на це

виділено 30 млн. доларів). Крім того, за поправкою Палати лордів, на перехоплення e-mail буде потрібна санкція на прослуховування. Але, якщо спецслужби самі не зможуть розшифрувати якесь повідомлення, новий закон зобов'язує користувачів надавати поліції паролі для розшифрування своїх листів.

Звичайно, Інтернет посилює загрозу до державних таємниць та конфіденційної інформації громадян (це з особливою гостротою ставить на порядок денний питання криптографічного захисту інформації). Неабияку, хоча і приховану, небезпеку являють собою обмін науковою інформацією через Інтернет. З одного боку, це прогресивний спосіб обміну думками про новітні досягнення науки, але, з іншого, таким чином через численні запити, анкети тощо можуть збиратися відомості, що становлять державну таємницю. Взагалі, слідуючи світовій практиці, таємна інформація має бути недоступна через Інтернет, тобто вона має циркулювати тільки у закритих локальних комп'ютерних мережах.

Часто права користувачів Інтернету порушуються з комерційною метою. Наприклад, багато компаній передають користувачам, коли ті відвідують їх сайти, так звані "cookies". Це невеликі приховані програми, які відслідковують інтереси користувача (до яких сайтів він звертається) і пересилають ці дані до своєї компанії, яка використовує їх для прямої реклами (тобто реклами певних товарів тільки тим людям, яких ці товари можуть зацікавити). У лютому 1999 р. офіційні національні представники від 15 країн Європейського Союзу прийняли рекомендацію щодо суворої секретності даних, що передаються. Згідно неї користувач має точно знати, які саме персональні дані про нього передаються у мережу. З 1 листопада 2000 р. США погодилися виконати вимогу Євросоюзу, і тепер американським компаніям заборонено розсилати "*cookies*".

З іншого боку, доцільно, щоб органи влади виставляли на своїх домашніх сторінках в Інтернеті інформацію про свою діяльність, організовували обговорення найважливіших документів, двосторонній зв'язок з рядовими громадянами. Крім того, держава має створити сприятливі умови для інвестицій у розвиток комп'ютерних мереж, виникненню нових компаній і конкуренції у цій сфері, бо це буде сприяти наближенню до рівня розвинених країн і переходу суспільства до інформаційної стадії розвитку. На це, зокрема, спрямований проект країн великої "сімки" "Держава он-лайн". У Данії всі рішення уряду мають бути доступні через Інтернет одночасно з їх публікацією в пресі. У Норвегії уряд пропонує через глобальну комп'ютерну мережу єдиний пакет інформації по найважливішим життєвим проблемам. У Великій Британії навіть створена книга "*Електронне надання державних послуг*". Аналогічні кроки роблять інші розвинені країни.

В Україні у рекомендаціях парламентських слухань "Свобода слова в Україні: стан, проблеми, перспективи" (квітень 1997 р.) зокрема говориться: "Інтернет може посилити загрозу для державних таємниць, особистої конфіденційної інформації громадян та збільшити залежність національного

інформаційного простору від закордонної продукції, чужої інформаційної політики". Вже в жовтні того ж 1997 р. Кабінет Міністрів України затвердив Концепцію технічного захисту інформації, тобто діяльності, яка спрямована на забезпечення інженерно-технічними засобами порядку доступу, цілісності та доступності (неможливості блокування) інформації, яка складає державну та іншу таємницю, що передбачена законом, конфіденційної інформації, а також цілісності та доступності відкритої інформації, що має важливе значення для особи, суспільства і держави. Для цього передбачена "обов'язковість захисту інженерно-технічними засобами інформації, котра складає державну та іншу таємницю, що передбачена законом, конфіденційної інформації, яка є власністю держави, відкритої інформації, що важлива для держави, незалежно від того, де ця інформація циркулює, а також відкрита інформація, яка важлива для суспільства і держави, якщо ця інформація циркулює в органах державної влади і органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, у державних установах і організаціях". Звичайно, реалізація цих планів може суттєво зменшити доступ до офіційної інформації, бо всі види інформації, крім державної таємниці, законом не передбачені і будуть визначатися, мабуть, через якісь галузеві інструкції. У лютому 1998 р. в Україні був прийнятий Закон *"Про Національну програму інформатизації"*. Причому однією з цілей цієї програми є забезпечення інформаційної безпеки України.

Ще одна проблема, яка виникає у зв'язку з розвитком глобальних комп'ютерних мереж — це проблема дотримання авторського права.

Взагалі, за кордоном все частіше постають питання, пов'язані зі зловживанням можливостями Інтернету. У Німеччині наприкінці 1995 р. баварський прокурор визначив, що більш, ніж 200 телеконференцій порушують німецьке законодавство з питань боротьбі з порнографією. Але заподіяти цьому не зміг, бо сервери, де були розміщені ці матеріали, знаходилися далеко за межами країни. У Канаді та Японії були заарештовані особи, які розміщували порнографічні картинки на своїх домашніх сторінках в Інтернеті. У Сінгапурі влада зобов'язала провайдерів послуг Інтернету контролювати зміст домашніх сторінок, звертаючи увагу на матеріали про секс, політику та релігію. Причому політичні партії аби відкрити свою домашню сторінку в Інтернет, мають отримати урядову ліцензію. Франція через небезпеку тероризму у 1996 р. навіть звернулася до уряду США, з тим, щоб було притягнуто до відповідальності ісламське угрупування, яке діяло в Каліфорнії і розповсюджувало через Інтернет інструкції по створенню саморобних бомб на зразок тих, що вибухнули у паризькому метро. До найрадикальніших засобів звернулися у Китаї. Там усі користувачі Інтернету мають бути обов'язково зареєстровані у кантонах та префектурах і повідомляти владу про всі зміни у своїй діяльності.

Деякі країни приймають спеціальні законодавчі акти щодо розповсюдження порнографії в Інтернет. Так, у жовтні 1998 р. в Ірландії було прийнято

закон, який забороняє використання дитячих образів при виготовленні аудіовізуальних матеріалів сексуального характеру, а також розповсюдження дитячої порнографії. Дітьми тут вважаються особи, що не досягли 17 років. Порушники будуть штрафуватися у розмірі до 25 тис. фунтів або засуджуватися до 14 років позбавлення волі.

Необхідність дотримання балансу між вільним інформаційним потоком і захистом громадських та особистих інтересів розуміють і в Європейській Комісії. Наприкінці 1996 р. Рада з телекомунікацій Європейської Комісії прийняла рішення, яке спрямоване на запобігання розповсюдження в Інтернеті порнографії, особливо дитячої. Треба відмітити, і це підкреслювалося неодноразово, Інтернет дуже специфічний засіб комунікації і через свій транскордонний характер важко піддається правовому регулюванню. Всі учасники Інтернет підлягають законам своїх країн. Але незаконний зміст може бути виявлений не на території тієї країни, де він зберігається на сервері. Тому для врегулювання правових відносин в Інтернет і необхідні міжнародні угоди щодо нього. А це в свою чергу ускладнюється різними підходами законодавства країн до тих чи інших порушень, наприклад, різний зміст вкладається у поняття "порнографія". Зараз загальний напрямок законодавчих ініціатив щодо Інтернету спрямований на встановлення відповідальності провайдерів хостових послуг за зміст інформації, що міститься на їх комп'ютерах. Звичайно, це дуже складно з технічної точки зору і тому в деяких законодавствах відповідальність провайдерів обумовлюється тим, що вони знали про зміст незаконної інформації. Мережеві оператори, як правило, не притягуються до відповідальності, але у них вимагають припиняти доступ до клієнтів, що розповсюджують незаконну інформацію. Цікаво, що у Великобританії вже працюють системи саморегулювання в роботі провайдерів Інтернет. Там прийнятий "Кодекс поведінки" і створений Фонд "Безпечна мережа", який допомагає провайдерам визначитися чи є та чи інша інформація незаконною. Канадська асоціація провайдерів послуг Інтернету також розробила Кодекс поведінки в Інтернеті. Його мета - допомогти членам Асоціації у дотриманні правових стандартів у роботі. У Франції існує Хартія Інтернет, у якій визначаються добровільні обов'язки користувачів і провайдерів в Інтернеті. У Німеччині провайдери Інтернет зорганізувалися у Freiwillige Selbstcontrolle Multimedia Dienstleanbieter (FSM) — Спілку добровільного саморегулювання служб мультимедіа. Ця організація створена, для того щоб вживати заходи по скаргам на зміст он-лайн потоків, але скарги мають стосуватися виключно інформації, що є пропагандою насильства чи іншим чином може зашкодити молодим людям. Кроки зі створення подібних організацій саморегулювання зроблені і в деяких інших країнах. Деякі неурядові організації у Великій Британії навіть організовують тиск на членів парламенту з вимогою забезпечити законодавчу підтримку приватності спілкування у *WWW*. Члени цього руху «Візьми шевство над депутатом» створили свою веб-сторінку, на якій всі бажаючі можуть взяти шефство над одним з депутатів парламенту і проводити з

ним через Інтернет чи пошту роз'яснювальну роботу з цього питання. У Бельгії в травні 1999 р. був заключений протокол між Асоціацією провайдерів Інтернет-послуг, Міністерством юстиції та Міністерством у справах телекомунікації. Мета цього протоколу — попередження злочинів за допомогою Інтернету: дитячої порнографії, пропаганди расизму, порушення законодавства про ігорний бізнес. У протоколі закріплений обов'язок провайдера інформувати виконавчу владу про порушення, які він помітив. Корисно те, що провайдери не зобов'язані перевіряти інтернет-ресурси та шукати порушення.

Але інколи спроби саморегулювання Інтернету набувають незаконних форм. У 1996 р. у Німеччині група хакерів "Організація спасіння Європи" за чотири місяці знищила більш, ніж 50 сайтів, на яких містилася інформація, що стосувалася нацизму. У 1997 р. у Франції відбулася ціла "*війна хакерів*". Хакери – прибічники нацизму до чергової річниці Гітлера намагалися наводнити Інтернет екстремістською інформацією, а антинацистські налаштовані хакери її активно знищували. Боротьба продовжувалася десь тиждень, а потім припинилася сама собою. Один з представників французької провайдерської компанії сказав: "Таке враження, що дітям набридло грати в одну гру і вони вирішили вигадати нову». У березні 1999 р. російською хакерською групою "*Антифашистський фронт Росії*" була проведена акція блокування серверу "*Руспатріот*", на якому були розміщені веб-сторінки таких націоналістичних об'єднань, як "*Чорна сотня*", "*Пам'ять*" тощо. Хакери викрали у власників серверу доменне ім'я ruspatriot.com, внаслідок чого всі відвідувачі серверу попадали на сторінку, де була розміщена карикатура Кукриніксів "*Фашизм не пройде*" і звернення "*Антифашистського фронту Росії*" до "презирливих фашистів". У зверненні говориться, зокрема, про те, що члени фронту не будуть чекати на рішення судових органів, а самі зроблять все для зменшення присутності наці в Інтернеті. Після цієї акції подібні проводили вже деякі провайдери. Так, компанія "BizLink" вилучила з свого серверу електронні версії газет "Завтра" і "Дуель". Американський провайдер "Hyper Mart" закрив три сайти письменника О. Дугіна, через те, що "його агітація не відповідає цілям та завданням діяльності серверу". За російськими законами діяльність "Антифашистського фронту Росії" є незаконною, бо порушує ч. 2 ст. 272 Кримінального кодексу РФ "Неправомірний доступ до комп'ютерної інформації, здійснений групою осіб за попередньою угодою, чи організований групою", згідно якої карається "неправомірний доступ ... до інформації на машинному носії, що охороняється законом, в ЕОМ, системі ЕОМ чи їх мережі, якщо ця дія призвела до знищення, блокування, модифікації, чи копіювання інформації, порушення системи ЕОМ чи їх мережі". Покаранням може бути від штрафу від 500 до 800 розмірів мінімальної заробітної плати до позбавлення волі терміном до п'яти років. Звичайно, за законодавством всіх перелічених країн заборонено розповсюдження інформації екстремістського толку, як воно, до речі, заборонено і Європейською конвенцією з прав людини, однак встановлювати законність чи незаконність

інформації — це справа суду. Так, у 1997 р. за рішенням судів Великої Британії було закрито два сайти за те, що там містилася інформація расистського характеру, бо було вирішено, що ця інформація "не відповідає інтересам людства".

Іноді війни у кіберпросторі набувають міждержавного характеру. Так, на початку 2000 р. біля місяця тривала війна між хакерськими групами з Азербайджану та Вірменії. Спочатку дві азербайджанські групи (Green Revenge і HijaK Team 187) зламали біля 25 вірменських сайтів, у відповідь вірменська група Liazor захопила майже всі найпопулярніші азербайджанські сайти, навіть сайти газет, телебачення та інтернет-провайдера. Після того, як вірменські хакери поміняли зміст цих сайтів, вони заявили, що не будуть опиратися поверненню їх законним власникам.

21 грудня 1998 р. Рада Європейського Союзу затвердила план дій щодо безпечного використання Інтернету, який був запропонований Європейським парламентом за місяць до цього. План діяв чотири роки (з 1 січня 1999 р. по 31 грудня 2002 р.), його бюджет складав 25 млн. євро. План передбачав створення різних "рівнів якості" Інтернету. Формуватися вони мали відповідно до "знаків Інтернет-якості" продукції. Ці положення мали бути найближчим часом закріплені як у національних законодавствах, так і в кодексах саморегулювання інтернет-провайдерів. У березні 1999 р. Європейська Комісія прийняла звіт про результати обговорення положень Доповіді про конвергенцію телекомунікацій, ЗМІ та інформаційних технологій (*"Зелена книга"*). Основний висновок такий: правове регулювання в Інтернеті має бути прозорим, ясним і пропорційним, а також бути різним по відношенню до передачі даних і до змісту повідомлень. Подібні заклики до обережності при спробах регулювання Інтернету лунають часто. Так, у Франції Вища Рада з аудіовізуальної політики організувала у 1999 р. міжнародну дискусію на тему регулювання інтернет-послуг. Сама Рада дотримується думки, що окремих спеціальних законів не потрібно, а надання радіо- чи телепослуг за допомогою Інтернету має регулюватися за вже існуючими законами щодо функціонування телерадіопростору.

Для захисту даних у глобальних комп'ютерних мережах широко застосовується шифрування, тобто криптографічні засоби. У різних країнах існують свої правила їх застосування. У Росії згідно із Законом *"Про державну таємницю"* та Указу Президента РФ № 334 від 3.04.96 забороняється діяльність фізичних та юридичних осіб, яка пов'язана з розробкою, виробництвом, реалізацією і експлуатацією шифрувальних засобів, а також захищених технічних засобів збереження, обробки і передачі інформації, наданням послуг в області шифрування інформації, без ліцензії, виданої Федеральним агентством урядового зв'язку та інформації при Президенті РФ. Таким чином, запроваджена фактична державна монополія на розвиток шифрувальних систем. В США навпаки спеціальний комітет Національної ради з досліджень Національної академії наук США прийняв рішення, що переваги

широкого розповсюдження криптографії дають суспільству більше гарантій, ніж заборона та обмеження шифрувальних засобів. Комітет закликав змінити офіційну політику США, щоб криптографія була доступна для всіх правомочних суб'єктів американського суспільства. Особлива увага надається розробці засобів криптографічного захисту інформації від перекручення, для підтвердження особи користувача і для захисту інформації в мережах зв'язку. У Франції 19 січня 1999 р., через рік після прийняття державної програми з розвитку інформаційного суспільства, прем'єр-міністр запропонував нові заходи з розвитку Інтернет. І найпершим були пропозиції щодо зміни механізму регулювання шифрування даних. Якщо раніше з міркувань державної безпеки всі були зобов'язані повідомляти у державні органи шифр будь-якого коду передачі транскордонних повідомлень, що перевищували 40 біт, то тепер верхня планка складає 128 біт. Відповідні поправки з питань розвитку технологій та введення електронного підпису запропоновані у Цивільний кодекс Франції.

З'явився і такий новий вид правопорушень, пов'язаний з Інтернет, як запуск сфальсифікованих повідомлень нібито від інформаційних агентств. Наприклад, у розпалі президентської компанії в Росії 1996 р. у західні країни прийшло повідомлення від імені агентства ІМА-ПРЕС про смерть президента Б.М.Єльцина. Агентство у випуску 6 мусило офіційно спростовувати це повідомлення і розцінило його як провокацію. Від імені цього ж агентства по московським ЗМК і банківським структурам було розіслано сфальсифіковане повідомлення про "*наїзд*" на один з банків. А за наступне втручання хакерів у мережу ІМА-ПРЕС довелося відповідати волгоградській газеті "*Молодежный курьер*". Справа в тому, що у сфальсифікованій інформаційній стрічці, яка надійшла до газети електронною поштою нібито від ІМА-ПРЕС, містилися наклепницькі відомості про астраханського губернатора А.П.Гужвіна. Газета мушена була виплатити губернатору 10 млн. карбованців і надрукувати спростування. Інший скандал був пов'язаний з сайтом "*Коготь-2*". На цьому сайті була розміщена інформація щодо "корупційних" зв'язків алюмінієвого магната А.Бикова. При цьому ніяких доказів подібних зв'язків не наводилося. Не дивлячись на це, скандал широко обговорювався громадськістю Красноярського краю і мав неабиякі наслідки. А.Биков втратив значну частку довіри населення на користь свого опонента, губернатора краю О.Лебедя. З одного боку, це може викликати подив. Адже кількість користувачів Інтернету залишається невеликою. Але з іншого, згідно з теорією багатосходинкового потоку комунікації саме "лідери думок" в основному формують громадські настрої. Таким чином, роль порівняно дешевих кампаній по пропаганді (часто дезінформації) в Інтернеті важко переоцінити.

Звичайно, підтримання інформаційної безпеки — це справа, насамперед, державна. Але не всі державні інституції розуміють її належним чином. Не можна вважати діяльність витісненню з інформаційного поля України російськомовних медіа захистом інформаційного простору України. Стандар-

ти інформаційної ери розвитку суспільства вимагають інших підходів до регулювання діяльності ЗМК [392-398].

Наївно думати нібито обмеження доступу закордонних мас-медіа на український ринок призведе до зменшення впливу тієї чи іншої країни. По-перше, транскордонні технології передачі інформації, на щастя, не дають можливості повністю ізолювати ту чи іншу країну від закордонного інформаційного впливу. По-друге, всі великі держави проводять свої інформаційні кампанії в тій чи іншій країні через національні ЗМК тих країн. Інформаційний вплив при цьому збільшується, бо населення не ідентифікує національні медіа-засоби з діяльністю із-за кордону. Наслідок проведення політики інформаційного ізоляціонізму може бути тільки один: інформаційний голод. В умовах переходу до інформаційного суспільства це означає відкидання власної країни на узбіччя розвитку. Бо зараз, як ніколи, треба створювати конкурентне середовище на медіа-ринку. Українські засоби масової комунікації мають нарощувати свої мускули в конкурентній боротьбі, тільки в цьому випадку вони зможуть протистояти інформаційним кампаніям з-за кордону. Конкурентне середовище означає відсутність будь-якої монополії у медіа-просторі, бо це забезпечить право доступу громадян до плюралістичної за своїм характером інформації, а це одна з найважливіших складових інформаційної безпеки. Таким чином, звуження власного інформаційного простору не тільки суперечить загальним тенденціям світового розвитку (ті ж США всіляко розширюють свій інформаційний простір, включаючи туди видання французькою, іспанською, іншими мовами), а несе реальну шкоду національним інтересам України. Російськомовна українська аудиторія у випадку переходу на 100-відсоткове українське мовлення переключиться на закордонні джерела інформації, що створить додаткові проблеми для інформаційної безпеки держави.

Необхідно чітко зрозуміти, що підтримувати україномовний інформаційний простір можна лише шляхом преференцій. Шлях же каральних санкцій призведе тільки до реального звуження інформаційного поля і, таким чином, нанесе реальну шкоду національним інтересам України.

Україна має бути відкрита для світових інформаційних потоків. І шлях преференцій допоможе включити їй свій голос до цих потоків. Шлях же обмежень призведе тільки до стагнації, що в умовах стрімкого розвитку інформаційного суспільства означає тільки одне: закріплення України серед нерозвинених, відсталих країн без всякої перспективи для розвитку.

У сучасних умовах самообмеження інформаційного простору країни може означати лише одне: усунення України з числа більш-менш розвинених країн без всякої перспективи до її повернення у цей табір. Тільки інформаційна відкритість, активна власна інформаційна політика, спрямована на створення пільгових умов для виробників власного інформаційного продукту (в широкому сенсі цього слова) можуть зробити Україну незалежною могутньою державою.

Загалом, Україна переживає складні часи свого становлення. Українські журналісти ще не користуються тими правами і свободами, як їхні ко-

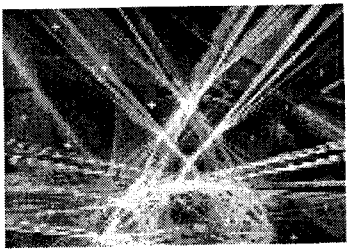
леги в цивілізованих країнах. Йде період становлення демократичної преси. Існування плюралізму думок в українських медіа не доповнені і не забезпечені незалежністю газет і телерадіоорганізацій.

Після приходу до влади нового президента медіа-товариство очікувало трьох речей: знищення політичної цензури, роздержавлення медіа та створення суспільного телебачення. Маємо ми тільки перше. Але цензура держави була замінена цензурою власника, а держава втручається у медіа-процес через державні та комунальні медіа. Крім того, не наведений порядок в медіасфері в частині дотримання антимонопольного законодавства. Власність масмедіа так і не стала прозорою.

Можна назвати кілька основних погроз свободи слова в Україні. По-перше, це неможливість для медіа бути прибутковими, тобто економічно незалежними, по-друге, убивства і побиття журналістів, по-третє, судові переслідування, особливо по справах про захист честі і гідності, по-четверте, адміністративний тиск (перевірки і санкції з боку податкової інспекції, пожежної охорони й інших служб). На жаль, приходиться констатувати той факт, що в Україні ще не існує таких важливих складових для створення громадянського суспільства, як свобода слова і незалежні медіа.

РОЗДІЛ 4

ПРИКЛАДНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



4.1. Інформаційна парадигма сучасної геополітики у контексті проблем міжнародної безпеки та глобального розвитку

Глобалізація або посилення взаємозалежності світу є однією з причин другого народження, яке зараз переживає геополітика. На сучасному етапі у зв'язку з розвитком міждержавних зв'язків, інформаційних технологій, формуванням універсальних загальнолюдських цінностей політичні процеси дедалі більше виходять за межі локальних. Як вважає російський політолог К.С.Гаджієв, нині починається етап формування нового типу світового співтовариства загальнопланетарного масштабу [399].

Глобалізація перетворилася на ключову тенденцію, що характеризує процеси світового розвитку на початку XXI ст. Російський політолог М. Іванов бачить сутність глобалізації в "різкому розширенні й ускладненні взаємозв'язків і взаємозалежності як людей, так і держав, що значною мірою впливає на процеси формування планетарного інформаційного простору, світового ринку капіталів, товарів і робочої сили, а також в інтернаціоналізації проблем техногенного впливу на природне середовище, міжетнічних та міжконфесійних конфліктів та безпеки" [400].

У політичній та передусім в економічній сферах, глобалізація проявляє себе в нарощуванні інтеграційних тенденцій. Інтеграцію можна описати як "процес руху й розвитку певної системи, у якій кількість та інтенсивність взаємодії її елементів зростає – посилюється її взаємний зв'язок, і зменшується відносна самостійність" [400]. Інтеграційні процеси на міжнародному рівні призводять до збільшення взаємозалежності й розширення сфери спільних інтересів. Ступінь участі будь-якої держави в міжнародних інтеграційних процесах є одним із показників її зовнішньоекономічної й зовнішньополітичної безпеки. Однак, глобалізація та процеси інтеграції мають наслідками не тільки позитивні результати.

Ідейно концепція "третьої хвилі" глобальної модернізації оформилася на початку 1990-х років та найвиразніше маніфестувалась у працях трьох авторів - О.Тоффлера, Ф.Фукуями та С.Хантінгтона [13; 401-402]. Майже незалежно один від одного вказані дослідники описали глобальний образ найближчого майбутнього. Евфемізми типу "modern societies" (*"сучасні суспільстві"*) не приховували, однак, суті того, що йдеться про "вирівнювання" всіх країн та народів на цивілізаційних взірцях *"золотого мільярда"*.

Отже, з одного боку, глобалізація є прогресивною тенденцією розвитку, що відкриває нові можливості та обіцяє великі вигоди сучасній цивілізації, зокрема, національним економікам. З іншого боку, змістовну частину й напрями глобалізації, що передбачає взаємозалежність економічних систем різних країн, визначає вузьке коло найбільш розвинутих країн (так званий *"Перший світ"*), які виступають вагомими суб'єктами процесу глобалізації. Цей факт,

як відомо, пов'язують з нерівномірністю розвитку країн, яка може призвести до перетворення на аутсайдерів глобалізаційних процесів великої групи країн, які неспроможні на радикальні перетворення з метою швидкого економічного зростання.

Сучасні процеси глобалізації зосереджуються не лише в економічній та фінансовій сфері, але й у політичній, соціальній тощо. За таких обставин намагання західної цивілізації спрямувати глобалізацію на реалізацію власних прагматичних інтересів, претендувати на загальнолюдський статус породжує відповідну негативну реакцію з боку різних суб'єктів міжнародних відносин, внаслідок чого посилюються суперечності між цивілізаціями різного типу (зокрема, між ісламською та західною).

Таким чином, розвиток процесів глобалізації та інтеграційних процесів, загострення глобальних проблем сучасності, які відображають тенденції світового розвитку й визначають сутність геополітичної ситуації у світі, містять у собі як позитивні так і негативні аспекти. У сучасних геополітичних реаліях "поствестфальського світу", пов'язаних із розвитком взаємозалежності держав у рамках глобалізації, на умовну одиницю перетворилося таке важливе поняття як державний суверенітет, адже цілковитої незалежності в сучасному світі просто не може бути [400].

Глобалізація породила конфлікт парадигм цивілізаторства або модернізації, з одного боку, та геополітики самобутності, з іншого, - що є цілковито закономірним та виправданим процесом. Проте, існує небезпека хронізації, коли цей конфлікт спричинить підміну цивілізаційної презумпції довіри протилежною презумпцією всезагальної недовіри з жорсткою дилемою міжнародної поведінки: або агресивний супротив, або глуха оборона ізоляціонізму. Тоді замість філософії відкритого й однорідного світового простору із чіткими та однозначними гарантіями партнерського обміну може сформуватися філософія закритих просторів [403].

Отже, нове XXI століття позначене зміною історично-часових орієнтирів, які стосуються геополітичного та культурно-історичного самоусвідомлення народів. Причому, ідеться не лише про Україну та інші пострадянські республіки, але й про більш розвинені регіони світу. Такий феномен породив у відповідь на виклики глобалізації цивілізаційний регіоналізм, який знаходить вияв в європоцентризмі, панамериканізмі, ісламському або православному фундаменталізмі тощо.

Водночас, у випадку з Об'єднаною Європою зміна світоглядних орієнтирів стосується не лише боротьби між глобалізмом та різноманітними виявами регіонального європеїзму, але також між ідеєю "*Об'єднаної Європи*" та ідеєю "*Європи Націй*", пов'язаною зі зростаючим національним самоусвідомленням ("націоналізмом"). Особливо загострилася європейська криза ідентичності на тлі останньої хвилі розширення ЄС (із прийняттям низки країн Східної та Центральної Європи). Ще потужніший виклик цій ідентичності кидає ймовірний вступ до ЄС Туреччини. Зокрема, маючи на увазі акту-

алізацію питання про "кордони Європи", у доповіді на "*Європейському форумі*" німецький канцлер ФРН Ангела Меркель сказала, що "*...потрібно визначитись з кордонами ЄС*" [404], а лідер правлячої у Франції партії "Союз на підтримку народного руху" Ніколя Саркозі зазначав: "Не всі країни мають можливість вступити до ЄС. Варто пригальмувати процес розширення, принаймні до того часу, коли не будуть оновлені всі його інституції. Європа повинна мати кордони" [405].

Загальна тенденція розвитку європейської геополітики протягом XX ст. характеризується переходом від геополітики простору до геополітики людини, яка оволодіває цим простором. Якщо європейські геополітики спочатку розробляли свої концепції, спираючись на природно-наукові фактори, то на сучасному етапі геополітика в Європі стала більш гуманітарною наукою, що досліджує "*дух і культуру*" людини, яка володіє простором.

Глобальні трансформації змушують дослідників заявляти про "геополітичний хаос", коли руйнуються старі геополітичні парадигми, в рамках яких вже нічого не можна пояснити у сучасній геополітичній боротьбі за простір. Класична геополітика була заснована на сакральних ідеях віри, ґрунту та крові, а посткласична картина політичного простору поставила питання про трансляцію цих символів у віртуальний простір у вигляді символічного капіталу національної культури.

В індустріальну епоху держава-агресор намагалася захопити територію, руйнуючи промисловий комплекс і засоби виробництва держави-ворога, в інформаційному суспільстві головним засобом контролю над простором стали контроль над особистістю, управління її світоглядом, а також картиною світу цілих народів [406].

У класичних геополітичних доктринах переважали спрощені – суто просторові – географічні підходи, які базувалися насамперед на аналізі географічних чинників у контексті протистояння континентальних та морських держав. Основний закон класичної геополітики зводився до фундаментального дуалізму, що базувався на ідеї споконвічної боротьби двох стихій – "*телурократії*" (суходільної могутності) і "*талассократії*" (морської могутності). Така "*войовнича*" геополітика припинила своє існування разом зі своїми авторами, але її основна тенденція – прагнення до поширення контролю над простором – залишилася актуальною. Виникла нова формула – "*захист національних життєвих інтересів*" [400]. Нині ця формула має бути істотно "переписаною", оскільки найбільш життєво важливим для нинішніх держав є інформаційний ресурс, адже інформаційна революція додала до сфер розуміння геополітики новий віртуальний вимір простору, змушуючи дослідників переосмислювати норми й правила геополітичної боротьби [406].

В інформаційному суспільстві інформація відіграє роль того стратегічного ресурсу, за оволодіння яким провадиться політична боротьба на різних рівнях – міжнародному, регіональному, локальному тощо. Відповідно, контроль над інформаційним середовищем, перетворився на важливу складо-

ву міжнародної, національної безпеки та геостратегії, яка передбачає використання інформаційної сфери для "досягнення власних стратегічних цілей" та попередження такої можливості для конкурента [407].

М. Лібіцкі зазначає в даному контексті: "*Контроль над інфосферою означає ситуацію, у якій актор має можливість контролювати інформацію та її рух, підкоряти дію цієї інформації у власних цілях*" [408]. Українська дослідниця С.В.Андрущенко стверджує, що інфосфера в сучасному світі виступає засобом для посилення традиційних інструментів геостратегії в досягненні державами національних та глобальних інтересів [407].

Зазначене обумовлює ту ситуація коли сучасна постмодерна (інформаційна) геополітика або геополітологія, на відміну від класичної, яка однозначно прив'язувалася до географічних образів світу, активно використовує проективні віртуальні геополітичні ансамблі медійних образів (іміджів, брендів тощо), "випробовуючи" їх у силових полях певних політичних чинників. Відтак, виникають ті геополітичні ансамблі, у межах яких перебуває й віртуальне буття навіть класичних "геополітичних паттернів" ("*хартленд*", "*рімленд*" тощо), із певною актуалізацією ad hoc інших інтенсивно експлуатованих мас медіа образів (відродження образів "Євро-Африки", "Євразії" тощо) з відповідними змінами й розширеннями, залежно від аудиторії призначення, спектрів можливих значень.

Відповідно, набуло поширення тлумачення геополітики як дискурсу, специфічного способу міркувань про світ, який не скутий "догмами". Згодом сюди додалося більш точне поняття "*геополітичних культур*" ("geopolitical cultures") [409].

Подібна ситуація призвела до того, що у 1992 р. Жеруа Туатайль (Gearoid У Tuathail) та Джон Егню (John Agnew) опублікували статтю "Геополітика та дискурс: практичне геополітичне обгрунтування американської зовнішньої політики" ("Geopolitics and discourse: practical geopolitical reasoning in American foreign policy") в науковому журналі "Політична географія" (Political Geography) [410]. Проведене ними дослідження прискорило концептуалізацію геополітики як форми політичного дискурсу на противагу спрощеному описовому поняттю, яким пояснювали вивчення зовнішньої політики та мистецтво керувати державою. Вищезгадана стаття разом з більш ранніми геоекономічними дослідженнями світової економіки (Егню та Корбрідж, 1989) змусили політичних географів вивчати не тільки політику географічного знання, але також географію світової економіки, що постійно змінюється [411]. Геополітика в цій праці була представлена не як описова наука, яка досліджує зовнішню політику та "*великі стратегії*", а як форма міркувань, навантажених різноманітними стереотипами метафоричного змісту.

Справді, у масовому геополітичному дискурсі можна зустріти чимало яскравих метафоричних формул на зразок "*вулкану, що прокинувся,*", "*храму ненависті*", "*ракової пухлини*", "*метастазів сепаратизму*", "*чорної діри*", "*вісі зла*", які виражають невизначеність або нерозуміння

специфіки певних країн та регіонів світу, які намагаються використати як підстави для прищеплення тій же масовій свідомості різноманітних фобій із відчуттями ірраціональної небезпеки [412].

Термін "критична геополітика" виник наприкінці 80-х рр. XX ст. завдяки новаторському дослідженню двох політичних географів Саймона Делбі (Simon Dalby) та Жеруа Туатайля. Стало очевидним, що "критична геополітика" вписується в групу досліджень в рамках дисципліни "міжнародні відносини" та підтримується пост-структуралізмом та політичною економікою [411]. На ранніх етапах наукові статті, присвячені "критичній геополітиці", намагалися радикально змінити предмет геополітики, що в принципі виправдовувалося вагомими змінами та "зламами", які відбувалися у геополітичному просторі під час "холодної війни".

У 90-х рр. XX ст. геополітика перетворилася на суто міждисциплінарну справу з оглядом на світосистемну теорію, кількісну течію у рамках теорії міжнародних відносин, дослідження гендерних проблем та пост-структурні дослідження світової політики, що змінили інтелектуальний вимір політичної географії (Тейлор, 2000; Егню та Корбрідж, 1995; Туатайль та Делбі, 1998; Шарп, 2000) [411].

"Критична геополітика" виходить з ототожнення реального (фізичного) і концептуальних "просторів", сполучаючи елементи політичної економії й геополітичної практики, культурології й народної (фольклорної) геополітики, видової ідентичності й геополітичного дискурсу, психоаналітики й геополітичної уяви, образів телекомунікаційних мереж і геополітичних кіберорганізацій, кібернетичних війн і віртуальної геополітики, глобалізації й реструктурування геополітичних регіонів.

За таких умов на зміну модерністській "географії" приходить постмодерністська "інфографія", оскільки дедалі все більше й більше великих груп людей інтегруються в глобальні мережі, тоді як пришвидшений простір інформаційних потоків розмиває традиційні поділи між місцевим, національним і глобальним. Зазначене означає стосовно регіонів колишнього Радянського союзу (Російської імперії) з Україною включно цілковиту недоречність сприймання цих регіонів ("*окраїн*") як російських іноетнічних "*периферій*", оскільки нині всі ці "периферії" охоплені єдиними транснаціональними процесами.

У 1990-і роки ця "багатопросторовість" країн та регіонів світу стала не тільки темою міжнародних ЗМІК і політичних дискусій, але й невід'ємним ідентифікатором державної та регіональної геополітики. Наслідком такої ситуації стало остаточне утвердження у свідомості політиків та науковців уявлень щодо існування принципово нового віртуально-географічного простору, який не вписується в традиційну бінарну логіку та суперечливі геополітичні образи, деформовані фольклорними кліше, згідно яких цілі регіони світу асоціюються з "відсталістю й недорозвиненістю" периферії, а інші - із незмінним прогресом. Згідно цієї викривленої логіки "Україна", наприклад, у

російській масовій свідомості асоціюється з *"Окраїною"*, а *"Малоросія"*, у тій же свідомості, - із меншовартістю на тлі більшовартості "Великоросії".

Отже, станом на кінець 1990-х рр. геополітика фактично перетворилася в специфічний міждисциплінарний дискурс або парадигму в межах теорії світо-системних взаємодій [413].

У контексті загальної тематики дослідження неокласичної геополітики можна виокремити чотири генеральних напрями (предметно-проблемних поля), представлені в західній літературі, які істотно відрізняються від класичної англо-американської геополітичної школи [409]:

- Геополітичні практики: дослідження шляхів та способів географічних та геополітичних міркувань, поширених у реальній практиці світової політики (Туатайль, 1994, 1996 [414]; Хеффернан, 2000 [415]);
- Геополітичні традиції: переосмислення історичного та географічного контексту ідей, які стосуються географії, політики й стратегії (Доддс та Аткінсон, 2000 [416]);
- Геополітика масової культури (popular culture): репрезентація світової політики на рівні образів масової культури [417];
- Структурна геополітика: осмислює зв'язок практичних проблем державності (statecraft) із процесами глобалізації, процеси творення інформаційних мереж та економічні трансформації [418].

Таким чином, ***"критична геополітика"*** складається з нових форм політичної географії, які ставлять під сумнів традиційне розуміння визначень "політичний" та "географічний". Так, британський дослідник Клаус Доддс зазначає, що політична географія статевих та особистісних формацій (sexuality and identity formation) представляє один з нових напрямів дослідження у рамках критичної геополітики. Відповідно, політична географія пройшла значну дистанцію від традиційних досліджень кордонів, могутніх держав та природних умов. В цілому, "критична геополітика" дозволяє відкрити нові підходи та напрями дослідження, робить вклад у дискусію гуманітарних (the humanities) та соціологічних наук (the social sciences) з приводу глобалізації, політики суверенності або "недосуверенності" (failed state) та ідентичності. Критична геополітика звертає увагу на абсолютно нові виміри: як нації в якості "уявних об'єднань" (imagined communities) виявляють себе у щоденному житті; як геополітика "працює" в щоденному житті людини, тощо. Такі географи як Девід Н'юман (David Newman), Анссі Паасі (Anssi Paasi) та Джеймс Сайдевей (James Sidaway) провели дослідження в рамках критичної геополітики з приводу того, як геополітичні кордони впливають та визначають життя тих людей, що мешкають в прикордонних місцевостях [411]. Джон МакКендрік (John McKendrick) продемонстрував як статистичний аналіз можна поєднати з теоретичною точністю в дослідженні нових форм націоналізму та демократичної політики [419].

Віртуалізації й медіатизації зазнають навіть класичні геополітичні образи "номоса Суходолу" і "номоса Океану" Карла Шмітта. Звідси виникають понят-

тя "геополітичного кодування", "геополітичної уяви" та "геополітичного бачення" ("візії"). Геополітичні образи ("візії") пантурецького, австрійського, німецького (пангерманського), російського (панслов'янського), англо-саксонського тощо "світів" гласно або негласно, навіть, слугують підставами творення сучасними державами та наддержавними утвореннями зовнішньої політики. Неважко, наприклад, збагнути контури колишньої Австро-Угорської імперії в такому утворенні як ЦЄІ (Центральноєвропейська ініціатива).

Важко ігнорувати, вибудовуючи практичну геостратегію, також ті "візії", які пропонує сучасна масова культура. *"Поп-геополітика"* (popular geopolitics) у цьому контексті є досить успішною практичною сферою знань, особливо в разі, коли вона вивчає перцепції та диспозиції масової аудиторії, які стосуються феноменів геостратегії та національної безпеки [409].

Особливо ефективною є "поп-геополітика" у випадку розуміння мотивів масової аудиторії, які вона використовує для виправдання або осуду сучасних війн. Геополітична риторика в 65-ти арабськомовних газетах (4 із них були іракськими) та в повідомленнях арабських інформаційних агентств з 17 країн світу стали, зокрема, предметом дослідження, яке переконливо показало причини неприйняття масовою арабською аудиторією американсько-союзницького вторгнення до Іраку в 2003 р. як "визвольного". Як виявилося, у масовій свідомості арабів відсутні "коди" моральних виправдань для такого вторгнення, й, навпаки, у цій свідомості присутності моральні виправдання тривалому опору "окупації" [420].

Саме інформаційно-комунікативні механізми мають причетність до предмету сучасної геополітики, яка постійно тримає в центрі уваги процеси ідентифікації та зміни, що відбувалися із цими процесами в минулому й відбуваються на сучасному етапі з поглибленим баченням можливих перспектив подальшого розвитку геополітичної ідентичності. Саме тому цілковито природною є необхідність розширити межі геополітики і поряд з географічним детермінізмом враховувати геоекономічні, соціокультурні та інші чинники [421]. Не дивно, що за подібних обставин геополітика виглядає як "когнітивний конгломерат, де науковий компонент співіснує з іншими складовими" [422].

У сучасному інформаційному суспільстві боротьба за простір розгортається в інформаційному полі — саме тут знаходиться "передній край" посткласичної геополітики, через це особливого значення набувають духовні, цивілізаційні й культурні фактори, роль і значення яких посилюється на кожному новому етапі сучасного розвитку інформаційного суспільства. Основна ідея інформаційних війн за простір у посткласичну епоху полягає в нав'язуванні потенційному супротивнику програмованого та керованого інформаційного образу світу. Г. Кіссінджер сформулював новий зміст геополітики наступним чином: *"Знання світогляду супротивника важливіше за об'єктивну реальність"* [406]. У центрі уваги сучасного геополітика не картографія географічного земного простору, а картографія людської душі, символічний капітал культури, віртуальний світ символів.

Отже, канали комунікації перетворюються на віртуальну силову арену геополітичної боротьби. Проміжні результати цієї глобальної геополітичної боротьби за простір стають реальними та помітними після чергових "гуманітарних антитерористичних операцій" в результаті яких на карті світу зникають цілі держави та народи, зображені в ЗМІК як "*вісь зла*" [406].

Предмети геополітики та геостратегії часто змішують, хоча в строгому розумінні цього терміну "геополітика" – вчення про політику в її просторових вимірах, про побудову таких дослідницьких моделей, які сполучають знання про соціоприродні простори – кліматичні, ландшафтні, геоморфологічні тощо - зі знаннями, придатними для ведення практичної політики й політичної організації в даних соціоприродних просторах. Водночас, геостратегія – це "обґрунтований геополітикою напрям діяльності держави на міжнародній арені" [400] або "розробка механізму реалізації геополітичних інтересів суб'єктів геополітики (держав, груп держав, інших транснаціональних угрупувань) на глобальному, регіональному, локальному рівні в існуючій геополітичній структурі світу" [407]. Геостратегічними гравцями є держави, що володіють національною волею, мають змогу впливати за межами своїх національних кордонів та стають лідерами не тільки регіонального масштабу, а й глобального.

Отже, геостратегія, яка обов'язково містить вольову компоненту, включає до розуміння свого предмету та методів інформаційну парадигму. Звичайно, поряд з іншими компонентами – національно-державним, ідеологічним та цивілізаційним. Саме зростанням ролі та значення геостратегії в геополітичному аналізі, сучасна геополітика зобов'язана надзвичайно істотним розширенням уявлень щодо сфер просторових відносин між державами, перемістивши основну частину уявлень по політичну боротьбу з реального простору у віртуальний і погодившись із думкою про те, що в реальному геополітичному середовищі з національно-державними та ідеологічними тісно взаємодіють фактори цивілізаційні та інформаційні [406].

Нова інформаційна парадигма геополітики означає, що в XXI ст. доля просторових відносин між державами визначається, передусім, інформаційним переважанням (гегемонією) у віртуальному просторі. І в цьому сенсі розробка геополітичної стратегії (геостратегії) – це створення оперативної концепції, що базується на інформаційній перевазі у віртуальному просторі й дозволяє досягнути зростання бойової могутності держави за допомогою інформаційних технологій. Таким чином, питання про роль символічного капіталу культури в інформаційному просторі набуває не абстрактно-теоретичного, а стратегічного геополітичного значення [406].

На думку В.Гречанінова на тлі глобальних процесів відбуваються значні зміни в співвідношенні так званої "*високої*" ("high politics") та "низької" ("low politics") політик. Проблеми "високої" політики – це проблеми загальної воєнної безпеки (оборона держави та її кордонів, досягнення воєнно-політичних угод тощо). Характеристикою сучасного етапу розвитку світового

співтовариства стало зменшення загрози світової війни, внаслідок чого аспекти співробітництва у військовій сфері, аспекти воєнно-політичного протистояння стали програвати економічним, соціальним і культурним зв'язкам, взаємодія в галузях яких і почала називатися "низькою" політикою [423].

Геополітичними "вісями" або "стрижнями" є держави, значення яких випливає не з їхньої могутності (суб'єктивні причини, сфера мотивації), а із суто об'єктивних причин географічного розташування та можливого впливу на геостратегічних гравців.

З огляду на вищенаведене розуміння поняття геостратегії можна звести до такої форми міжнародної взаємодії (співпраці), яка адекватна геостратегічним інтересам суб'єктів міжнародних відносин. Однією з позицій у такій взаємодії є відносини стратегічного партнерства, які передбачають масштабний і взаємовигідний спосіб взаємодії в багатьох різноманітних сферах [400].

Саме геостратегія складає основу зовнішньополітичної концепції будь-якої держави. Геополітика (та геополітичний аналіз), як основа геостратегії, формується державними інституціями (в сфері академічних та стратегічних досліджень, зовнішньополітичними органами держави, недержавними дослідницькими інституціями), а також виступає в якості ідеології – формування геополітичної національної ідеї. З.Бжезинський вважає, що сутність геостратегії полягає в стратегічному управлінні геополітичними процесами [424].

Зв'язок інформаційної сфери та геополітики й геостратегії виявляється в тому факті, що інформація існує в певному політичному просторі, що може належати суб'єкту політики, але водночас вона існує як окреме середовище, що дозволяє застосовувати маніпулятивні технології [407].

Алгоритм перемоги в інформаційному протиборстві за М. Маклюеном передбачає наступну схему: щоб бути "*агресивно ефективними в сучасному світі інформації*", необхідно активізувати у свідомості людей національну систему пріоритетів (як внутрішньо-, так і зовнішньополітичних (геополітичних), прим. автора дисертації), створити яскравий образ національної ідеї, адаптувати народні традиції до нових засобів комунікації [425].

На думку російської дослідниці І.О. Василенко, джерелом перемоги в будь якому інформаційному протиборстві може бути тільки символічний капітал національної культури, посилений сучасними інформаційними технологіями [406].

Василенко формулює головний геополітичний закон епохи інформаційної революції: "*Той, хто володіє символічним капіталом культури, – володіє вирішальними перевагами в інформаційному просторі, – а, отже, і на геополітичній карті світу*" [406].

До інформаційного виміру геополітики звертаються й українські дослідники. Так С.В.Андрущенко вважає інфосферу "п'ятим виміром сучасного геополітичного середовища" (поряд із землею, морем, повітрям та космосом), одним з "визначальних процесів сучасного геополітичного середовища,

що характеризують предмет геополітики на сучасному етапі" [407]. Визначною характеристикою інфосфери як певного виміру геостратегії є той факт, що різні форми стратегічної сили проектуються через і в межах саме цього середовища [426].

У XXI ст. геополітики почали достатньо вузько трактувати поняття "інформаційна війна". Л.Г. Івашов дає наступне визначення інформаційного протиборства – "інформаційне протиборство як форма геополітичного протиборства є сукупністю відносин інформаційного захисту та інформаційного суперництва протидіючих геополітичних суб'єктів" [427]. І.О. Василенко дає більш широке визначення інформаційної війни – "це планомірний інформаційний вплив на всю інфокомунікаційну систему супротивника та нейтральних держав із метою формування сприятливого глобального інформаційного середовища для проведення будь-яких політичних і геополітичних операцій, що забезпечують максимальний контроль над простором". У контексті інформаційного протиборства як форми геополітичного протиборства перемогти здатна така держава, яка запропонує та побудує в інформаційному просторі яскравий символічний образ національної ідеї, який для більшості громадян виявиться більш значущим, ніж будь-які інформаційні впливи [406].

Домінування інформаційної складової в структурі сучасної цивілізації якісно змінило стратегії міжнародної та національної безпеки, воєнну стратегію й тактику у боротьбі за простір. Зникають чіткі межі між різними рівнями воєнних дій, здійснюється розширення простору воєнного впливу й скорочення його часу (зникає географічно заданий традиційний театр воєнних дій), оперативні й тактичні дії в інформаційному просторі випереджають чисто фізичні дії [428]. До того ж "інформаційна агресія" може у деяких випадках запобігати початку воєнних дій. Як слушно зауважив В. Андреєв (Росія): "Активне застосування "жорстких" невоєнних засобів у поєднанні з "*м'якими*" нетрадиційними (у першу чергу, інформаційними) становить головну особливість протікання першої фази війни в сучасних умовах... Неможливість вирішення протиріч без застосування воєнних засобів знаменує перехід політичного процесу до другої фази війни" [429]. Таким чином, друга фаза є фактично війною, оскільки саме тут застосовується збройне насильство, ллється кров та відбувається руйнування життєвого середовища людини.

Більшість сучасних дослідників розглядають інформаційний вплив на психіку та свідомість військовослужбовців і цивільного населення інших країн як один із ключових елементів військової могутності. При цьому інформаційно-психологічний вплив стає відносно самостійним видом геополітичного протиборства, до складу якого входять:

- концептуально-методологічна зброя – інформація світоглядна, філософська, методологічна, яка дозволяє виокремити загальний і частковий хід речей. На базі цих знань формується філософський погляд на світ та приймаються рішення по основних напрямах розвитку народів і держав;

- хронологічна (історична) зброя — інформація щодо хронологічного порядку слідування фактів та явищ, їхнього взаємозв'язку між собою. При володінні методологією вона дозволяє розглядати явище як складову глобального історичного процесу і точно визначити вектор своєї політики.

Саме знання фактичної історії дає в руки людині зброю цього пріоритету. У взаємопов'язаному процесі минуле пояснює сучасне, а, відповідно, правильне усвідомлення сучасного дає можливість прогнозувати майбутнє. Інверсія на цьому рівні швидко спричиняє спотворення майбутнього:

- фактологічна (ідеологічна) зброя — інформація прикладного характеру: релігія, ідеологія, виборчі технології тощо.

Застосування інформаційної зброї має на меті досягнення політичних або воєнних переваг. Тому провідні у цьому відношенні держави світу визначили інформаційну війну як елемент геополітичного протистояння XXI століття. Підготовку та розробку стратегій захисту від неї розгорнуто в країнах НАТО, Росії, Китаї та в інших країнах на концептуальному, інформаційно-технологічному, організаційному рівнях.

Як слушно зауважив О. Литвиненко: "Нове покоління силових засобів, що їх отримує керівництво розвинених країн у результаті вдосконалення інформаційної зброї, найближчим часом може досягнути могутності та ефективності найновіших видів зброї масового знищення" [430].

На думку вітчизняних дослідників, інформаційне протиборство у безконтактних війнах треба розуміти як нову стратегічну форму боротьби сторін, де використовуються спеціальні способи й засоби для досягнення стратегічних цілей, і кваліфікувати їх можна як війни сьомого покоління [431]. Досвід локальних війн та збройних конфліктів кінця XX - початку XXI століть дозволяє зробити припущення, що силові маневри держав доіндустріальної та індустріальної цивілізації все ще будуть пов'язані з веденням *"гарячих та холодних війн"*, які розгортатимуться в геополітичному та геостратегічному просторах [428]. В основі цих війн лежатимуть прагнення до панування на певних життєвих просторах інших національних утворень, бажання підтримувати свій вплив не лише дипломатичними, але й воєнними засобами, політичними інтригами шляхом маніпуляції сіткою державних кордонів, апелюючи до *геополітичної пам'яті свого народу, відновлюючи ознаки давно минулих епох*, вплітаючи у підсвідомість теперішніх та наступних поколінь геополітичний менталітет мислення.

Силові маневри держав постіндустріальної цивілізації, міжнародні відносини яких грунтуються на геоекономічній парадигмі, вже не пов'язані ні із завоюванням територій, ні навіть з прямим підкоренням економічного простору противника. Вони швидше націлені на нав'язування світу своєї політичної волі і свого бачення майбутнього, на встановлення і досягнення власних стратегічних горизонтів, які визначаються геоекономічною конкуренцією й масштабами управління ризиками, на зміцнення чи підрив тієї чи іншої системи соціально-економічних орієнтацій [428]. При цьому пряме застосування

військової сили пов'язано з геополітичною функцією дестабілізації простору, який готується до геоекономічного засвоєння.

Таким чином, основною метою проведення операцій з використанням як традиційних, так і нетрадиційних засобів геополітичного протиборства, є здійснення дестабілізації політичної ситуації у регіоні, країні, проти яких спрямована експансія, створення умов для досягнення певної мети, наприклад, зміни курсу держави.

Нові реалії інформаційного суспільства в епоху глобалізації поставили перед дослідниками нове нетрадиційне з точки зору класичної геополітики завдання – проаналізувати роль та вплив інформаційного виміру (в усій його багатоманітності) на геополітичні процеси. Канали комунікації всього світу перетворюються на віртуальну силову арену геополітичної боротьби. Проміжні результати цієї глобальної геополітичної боротьби за простір стають реальними та помітними після чергових антитерористичних операцій.

Але потрібно зазначити, що геополітика тільки підходить до розуміння та освоєння інформаційної парадигми (поряд з національно-державною, ідеологічною та цивілізаційною) у геополітичному аналізі, оскільки геополітика розширила значною мірою сферу просторових відносин між державами, перемістивши основну частину боротьби з реального простору у віртуальний. Слід зазначити, що в реальному геополітичному середовищі діє і взаємодіє велика кількість факторів – національно-державних, ідеологічних, цивілізаційних, інформаційних тощо [432].

Отже, інформаційна парадигма сучасної геополітики явище досить нове і маловивчене, динамічне і таке, що стрімко розвивається. Формування п'ятого геополітичного виміру – інфосфери (поряд з традиційними геополітичними чинниками, детериторизацією держави, ретериторизацією та появою нових територіальних ідентичностей, геоекополітикою тощо [433]) є одним з визначальних процесів сучасного геополітичного середовища, що характеризує предмет геополітики XXI століття, та потребує детального наукового та практичного вивчення й подальшої розробки з урахуванням нових реалій розвитку світової спільноти.

4.2. Сучасні міжнародно-політичні стратегії США як модифікації доктрини стримування

В оцінках головних стратегій США до приходу Дж.Буша-молодшого в Білий дім досить часто можна помітити жорстку критику, що була узагальнена в монографії Е.Креймера "Великі дебати". Він робить це таким чином: "Тепер вже стало труїзмом, що у нас відсутній консенсус стосовно головної стратегії. Відбуваються жваві дебати, але відсутні видимі фаворити як серед зовнішньополітичних еліт, так і серед загальної публіки, хоча кожен, здається, міг би посприяти адміністрації Клінтона".

Виходячи з тону дискусії, надто багато зосереджено на специфічних виборах, що мають швидко бути реалізовані. Існують нарікання на те, що Сполучені Штати пливуть за течією, не мають стратегії, розігруючи поведінку в кожній кризі, що відбувається. Дехто вважає, що США можуть впасти жертвою "владної самовпевненості". Для інших Сполучені Штати — винятково толерантні стосовно інших держав. Деякі оглядачі прогнозують на основі прискорення американської винятковості й, згідно з незаперечними законами природи, появу антитези, або нової великої держави, або ворожого альянсу. Чимало й таких, що попереджають про перенапругу, імперську чи іншу, наслідком якої стане вичерпаність, поетапна чи інша. Ці дебати відбувалися переважно у 1990-ті, показавши ознаки триваючого одужання щонайменше в новому десятилітті. Ще один аспект відсутності головної стратегії є особливо очевидним тим, хто працює в міністерстві оборони. Незважаючи на номінальну зв'язаність Національної військової стратегії і Національної стратегії безпеки адміністрації Клінтона, військовий істеблішмент та адміністрація, схоже, не дотримуються однакових поглядів. Пріоритетними показниками цього розколу є поточні загострення в питаннях, які становлять життєвий інтерес, а також стосовно того, що виправдовує застосування військової сили" [434].

Далі він подає найбільш суттєві елементи головної стратегії:

- Визначення цілей для США.
- План використання американської сили для просування цих цілей.
- Справжній головній стратегії мають бути притаманні глобальний погляд (включаючи концепцію функціонування міжнародної політики і сподівань на майбутнє) та образ того, якою роль Америки в світі є або має бути.
- Головна стратегія має будуватися винятково на прагматичних засадах.
- Головна стратегія має бути більш загальною — переважно стратегічною концепцією.

Відтак, напередодні приходу Дж.Буша до влади в країні створилася ситуація, за якої переважна більшість аналітиків критично оцінювала міжнародно-політичну стратегію адміністрації Б.Клінтона як ситуативну, позбавлену фундаментальних ознак справді головних стратегій. Національна стратегія безпеки 1993 року, в основу якої було покладено мету розширення, за активного сприяння Сполучених Штатів демократичної спільноти націй через включення до неї недавніх сателітів Радянського Союзу із Східної Європи має достатні підстави називатися предтечею справді головної. Вона набула нових ознак внаслідок приходу до влади Дж.Буша та під впливом терористичних актів 11 вересня 2001 року, які сколихнули прихильників обмеженого ізоляціонізму, показавши неможливість такого підходу для єдиної глобальної держави світу.

Наразі ж подамо визначені цілі, які представив Е. Креймер, демократизація. Чітко визначені цілі відповідають критеріям глобальних стратегій демократизація міжнародної системи через демократизаційний

вплив на держави, чиї політичні системи викликають сумнів з цього погляду, а також подолання міжнародного тероризму як одного з базових чинників дестабілізації міжнародних відносин і завдання шкоди національним інтересам Сполучених Штатів. Передбачено масштабне використання всього комплексу американської могутності, включаючи військову сферу, для досягнення поставлених цілей. Окреслено прагматичний підхід, який полягає в тому, що застосовані механізми мають стабілізувати ситуацію в світі і забезпечити подальший розвиток американської політичної системи й економічний поступ. Врешті, Стратегія містить ознаки концепції, оскільки розробка конкретних механізмів реалізації затверджена за відповідними інститутами влади, починаючи від Ради національної безпеки, Державного департаменту, міністерства оборони і завершуючи спеціальними службами держави.

Повною мірою це відноситься і до відповідного документу РНБ, прийнятого навесні 2006 року.

Своє вступне слово на презентації нової Стратегії національної безпеки США Дж.Буш-молодший 16 березня 2006 року розпочав так: "Америка перебуває у стані війни. Ця стратегія національної безпеки воєнного часу спричинена серйозним викликом, перед яким ми опинилися — піднесенням тероризму, обурюваного агресивною ідеологією ненависті і вбивства, що повною мірою проявилася для американського народу 11 вересня 2001 року. Ця стратегія відображає наш урочистий обов'язок: захистити безпеку американського народу".

Інші ключові елементи Стратегії — захист свободи, демократії і людської гідності у всьому світі; просування свободи як альтернативи тиранії і відчаю; недопущення розповсюдження небезпечних озброєнь; стабільні і кооперативні відносини з головними потугами світу; підтримка економічного розвитку з наголосом відповідних зусиль на сприянні реформам і результативності.

Основними засобами її реалізації названо: відмову від ізоляціонізму і протекціонізму як таких, що ведуть тільки до наростання викликів і втрати можливостей; курс на лідерство як альтернативу ізоляціонізмові; реалізація такої мети, як вільна і чесна торгівля та відкриті ринки на противагу протекціонізмові; формування нового світу; вплив на події замість слідування за ними.

У контексті авторського дослідження суттєве значення відводимо словам 43-го президента США про те, що обрана нова Стратегія вписується у велику традицію американської зовнішньої політики, зокрема, тієї, яку проводили Гаррі Трумен і Рональд Рейган, ідеалістичну стосовно національних цілей і реалістичну на ниві засобів їхньої реалізації.

Відповідно до інших інтервенціоністських стратегій США повоєнної епохи стратегія передбачає підтримування і нарощування національної могутності, збереження і зміцнення збройної сили на основі економічного процвітання і демократії, міцних союзів, дружби, міжнародних інститутів, що допомагають розвивати демократію, процвітання і мир як спільну мету.

Відтак, наріжним каменем Стратегії окреслено:

- Сприяння свободі, справедливості і людській гідності, до чого веде весь комплекс міжнародно-політичної діяльності, спрямованої на припинення тиранії, підтримування ефективних демократій, поширення процвітання шляхом вільної і чесної торгівлі та мудрої стратегії розвитку, становлення вільного врядування на засадах підзвітності народам, ефективного управління територіями та відповідності благополуччю громадян, забезпечення міжнародного миру і стабільності через верховенство свободи і глобальне лідерство Америки.
- *Такий фундаментальний підхід базується на концепції критичної* геополітики, оскільки у першу чергу включає в себе використання всіх відомих форм американського впливу з метою зміни політичних і економічних систем у державах, на які він спрямовується. При цьому застосування воєнної сили також здійснюється не для територіальних завоювань, а з тією ж метою, що полягає у силовому примусі до демократизації. Тим самим такий концепт виразно відрізняється від позиції "батьків-засновників" Америки як цілями і способами їхнього досягнення, так і ставленням до ролі європейських союзників США. Так, у своєму найпопулярнішому історичному прощальному зверненні перший президент США Джордж Вашингтон безумовно заперечував зв'язок миру та процвітання Сполучених Штатів з долею Європи. Дж.Буш, котрий став президентом майже через двісті років по тому, щоправда, також стверджував, що вільна торгівля та комерція мають заохочуватися, але, на відміну від Дж.Вашингтона, політичні зв'язки називав небезпечними, закликаючи уникати постійних політичних союзів. Логічне обґрунтування настанов Дж. Вашингтона у цілісному вимірі виглядає повністю *протилежним текстові згаданої на початку розділу* Стратегії національної безпеки США від 16 березня 2006 року.
- Адаптація існуючих і розробка нових головних стратегій зовнішньої політики з кожним днем, що віддаляє нас від розпаду Радянського Союзу, посідає дедалі значиміше місце у діяльності політикуму і експертів Сполучених Штатів Америки. Завершення "*холодної війни*" буквально продиктувало пошук нових фундаментальних підходів, які могли б бути покладені в основу міжнародно-політичного курсу єдиної глобальної держави сучасності. Новий виток пошуків у цьому напрямі розгорнувся після трагічних подій 11 вересня 2001 року. Якщо під час президентської кампанії 2000 року і одразу з приходом до влади (січень 2001 р.) Джорджа Буша-молодшого американська адміністрація перебувала у стані невизначеності в цьому питанні, то терористичні акти в Нью-Йорку і Вашингтоні спричинили реставрацію ідеї "*нового світового порядку*", що її спробував актуалізувати до постбіполярного світу батько нинішнього президента США.
- "Вояжем навколо батька" назвав таку ситуацію один із творців неоконсерватизму Джон Подгорець у своїй монографії "Країна Буша" [435].

Нагадавши, що в Америці вже був один випадок президентств батька і сина (Харрісони, відповідно в 1841 і 1889–1893 рр.), він проводить умовну аналогію з сучасною ситуацію у тому сенсі, що "інший син" Бенджамін Харрісон привів країну до глибокої економічної депресії наприкінці 19-го століття.

- Мозкові центри неоконсервативного характеру запропонували оновле не бачення такого порядку, виходячи з того, що основою для нього могло б стати заснування міжнародної коаліції на чолі із Сполученими Штатами для розв'язання проблем Перської затоки як "джерела міжнародного тероризму". Перебуваючи в "тіні" свого батька, Буш-молодший у своїй передвиборній книзі написав, що головною помилкою батька на президентських виборах 1992 року був "дозвіл" своїм суперникам "визначити" його президентство, водночас подавши свій власний підхід: "У ході кампанії 1988 року мій батько зміг самовизначитися. У 1992 році його визначили Білл Клінтон, Росс Перо і Пет Б'юкенен... Я переконаний у тому, що об'єктивна історія судитиме про його президентство значно м'якше, ніж це було зроблено в ході передвиборної кампанії 1992 року" [436]. Разом з тим, команда Буша-молодшого не ризикнула розігрувати в президентській кампанії ідею повторення і/чи продовження курсу Буша-старшого. Взірцем для наслідування було представлено Рональда Рейгана. І саме цьому була по суті присвячена цитована вище передвиборна книга.
- Ідея "*нового світового порядку*" як би "*зависає*" ще й тому, що американська неоконсервативна школа політології міжнародних відносин так і не зуміла дати чітке, зрозуміле і адаптивне тлумачення "нового світового порядку" у розумінні Буша-старшого, щораз збиваючись в русло неоімперіалізму. Висунута паралельно концепція американського лідерства в багатосторонній коаліції також зазнала гострої критики всередині країни, у тому числі з боку республіканців, стурбованих тим, що нова адміністрація США надто тісно прив'язує національні інтереси і безпеку до багатосторонності, зокрема, в рамках ООН. Зі свого боку, ліберали і прогресисти стверджували, що сам концепт нового світового порядку неминуче стимулює воєнні акції як основний принцип захисту національної безпеки, що, однак, зовсім не вписується у пост біполярну систему міжнародних відносин [437].
- Таким чином, Буш-молодший прийшов до влади без чіткого бачення власної великої стратегії як всередині країни, так і на міжнародній арені. Натомість була обрана досить розмита теза "продовжити курс" Рейгана в економіці (обіцянка Буша не піднімати податки) [436] і актуалізувати ідею багатосторонньої коаліції на чолі з Америкою, що нагадувало експертам велику стратегію, яку запропонувала Клінтону державний секретар в його адміністрації М. Олбрайт під назвою "*догматична багатосторонність*". Її суть, як відомо фахівцям, полягала в "*конструктивній задіяності*", котра передбачала посилення спільних диплома-

тичних акцій і, особливо, економічних зв'язків, полегшених глобалізацією [437]. Відтак, малося на увазі робити ставку на дипломатію і економіку як ключові механізми досягнення стабільності, миру і безпеки. Паралельно 1990-ті роки визначали в рамках великої стратегії "гуманітарних інтервенцій", що практично проявила себе в акціях в Сомалі (Буш-старший) і в Боснії, Косово та Гаїті (Клінтон).

Аби виглядати іншим, Буш-молодший ще під час президентської кампанії обіцяє гнучку і зрозумілу зовнішню політику, котра більшою мірою відображатиме ідею захисту національних інтересів США як основи зовнішньої політики і дипломатії, зовнішньоекономічної діяльності і міжнародної торгівлі. Але вже перші дії нового президента на чолі адміністрації США показали, що вона, де-факто, вирішила стати на шлях "assertive анти-багатосторонності", оскільки передбачалося безумовне американське лідерство у розробці, прийнятті й реалізації міжнародно-політичних рішень.

Події 11 вересня 2001 року "допомогли" Білому домові чіткіше визначити свою велику стратегію через покладення в її основу боротьби з міжнародним тероризмом, превентивних воєн, агресивної односторонності за такої обов'язкової умови, як незаперечна перевага Америки у військовій сфері. Відтак, насправді була здійснена спроба "реставрації" рейганівської великої стратегії знищення комунізму та його втілення в особі Радянського Союзу як "імперії зла". Звичайно, формальні об'єкти знищення та відповідні пріоритети були адаптовані до посткомуністичної епохи, але суті це серйозно не міняло. Приміром, місце СРСР було віддано так званим "державам-паріям" як розсадникам тероризму, джерелам наркотиків та інших загроз людській цивілізації, від яких врятувати її може тільки могутня Америка.

Пріоритети міжнародно-політичної діяльності, традиційно визначені в рамках всіх великих стратегій США у парадигмі забезпечення національних інтересів США, будувалися на працях неоконсервативних ідеологів і політологів. Беручи витоки в давніх працях У.Ліппмана про союзи і альянси у зовнішній політиці [438], вони актуалізуються і адаптуються до позицій сучасності авторами монографій "*До однополюсного світу*" Ч.Краутхеммером [439] і "*Свобода від страху*" Д.Кеннеді [440], відомим політиком і дослідником Р.Золіком [441], на той час доктором політичних наук та майбутнім помічником президента з питань національної безпеки і державним секретарем К.Райс [442] тощо.

Безумовно, інтервенціоністська, наступальна і амбітна велика стратегія першого терміну президентства Буша-молодшого більше відома під назвою доктрини Буша. Війна в Іраку розширила коло її критиків. На правому крилі розмістилися ізоляціоністи, а на лівому – прогресисти, але вони єдині у загальному підході, оскільки визначають міжнародно-політичний курс нинішнього президента США як імперіалістичний. Повну підтримку і схвалення, якщо не брати до уваги адміністрацію, він знаходить в таборі неоконсерваторів. Але й вони виглядають критичними, бо вважають практичні дії

президента своєї країни у справі реалізації великої стратегії недостатньо агресивними з погляду впровадження американської гегемонії.

І все ж центральною ідеєю критики з початком і стагнацією війни проти режиму Хусейна залишається односторонність у розробці й прийнятті рішень за подальших спроб знаходити і всіляко *залучати* до союзників. Тут лідирують демократична партія і ліберали.

Отже, можемо говорити, що по суті велика стратегія Буша-молодшого викристалізувалася незадовго до початку президентських виборів 2004 року. Так, зокрема, вважає президент неоконсервативного Центру безпекової політики Ф.Гаффні, котрий відверто називає дії адміністрації США такими, що "визначають незаперечний тріумф американських цінностей" [443]. Він підтверджує "*спадкоємність*" великої стратегії Буша-молодшого у сенсі походження від стратегічних позицій Рейгана за його першого президентства, наголошуючи, що у такий спосіб 43-му президентові США вдалося "втілити моральні цінності американської безпекової політики на засадах і в обсягах, незнаних від часу першого терміна Рейгана". Ключовими виконавцями великої стратегії Буша-молодшого Гаффні визначив Д.Рамсфілда, Д.Чейні, Е.Абрамса, П.Волфовітца і Полу Добрянську. Відзначимо, що йдеться про творців і засновників Проекту за новий американський вік (ПНАВ).

Впадає в око, що від самого початку неоконсервативного руху, що припадає на другу половину 1970-х років, він пропонував базувати зовнішню політику на міцній оборонній і наступальній здатності Збройних сил, а також певних моральних цілях. "Заява про принципи", прийнята ПНАВ у 1997 році стала своєрідною предтечею великої стратегії Буша. Вона, зокрема, закликала до "*рейганівської політики, основаної на силі і моральній чистоті*". За твердженням Гаффні, президент чітко визначив "остаточну (верховну) моральну цінність – свободу, вважаючи її наріжним каменем своєї стратегії, метою якої є нанесення поразки ісламо-фашистським ворогам".

Маємо підстави стверджувати, що підготовка такої стратегії велася неоконсерваторами від 1970-х років, коли було створено широку мережу спеціальних мозкових центрів та інститутів політології, що "асоціюються з радикальною зовнішньою і військовою політикою, яка стоїть на порядку денному традиційних іудео-християнських цінностей" [443]. Серед них особливо значимою є активність і рольова функція Інституту релігії і демократії, Американського підприємницького інституту, Центру державної політики й етики, організації "*Велич Америки*" (Empower America), а також вказаного вище Центру безпекової політики. Принагідно відзначимо, що у вітчизняній політології міжнародних відносин вони мало відомі й, як наслідок, розробка великої стратегії Буша помилково приписується популярнішим мозковим центрам, скажімо, Раді зовнішньої політики США, Фонду "Спадщина" чи Міжнародному республіканському і Національному демократичному інститутам.

Це закономірно, оскільки, як свідчить проведений нами аналіз, ці солідні установи з "*дипломатичних*" причин не можуть собі дозволити твер-

дження, притаманні означеним, мало відомим не тільки в Україні, неоконсервативним центрам. Приміром, закликів змінити політичні режими у Північній Кореї й Ірані, здійснити нову реформу Збройних сил і навіть "відбудувати людську здатність мислити у процесі бойових дій, які веде Америка у Четвертій світовій війні", та розмістити додаткові оборонні ракетні комплекси у морі та космосі, не допускаючи, щоб була реалізована програма Франції і Німеччини створити єдину Європу як потенційну противагу американській могутності [443]. Окреслені центри та організації відверті також у своїх планах покінчити з "наростаючими" "фашистською торгівлею Китаю і його воєнною політикою", а також "внутрішнім тоталітаризмом Путіна і його агресивністю стосовно колишніх радянських республік". Кожного разу в таких судженнях і рекомендаціях присутня фундаментальна ідея – зупинити "світове поширення ісламо-фашизму" та "появу агресивно антиамериканських режимів у Латинській Америці". Наголошується з помітним задоволенням, що президент Буш частину з таких ідей включив до своєї великої стратегії, спрямованої на запобігання війни, культурного (цивілізаційного) конфлікту та недопущення зміни міжнародного режиму.

Загалом же велика стратегія Буша, за спільним визнанням американської політичної думки, спрямована на перетворення 21-го століття у ще один "американський вік". Зробити це, на думку Гаффні, можна тільки через конфронтацію з Росією і Китаєм, меншими державами Латинської Америки, націленими на вихід з-під американської демократичної гегемонії.

Відповідне наповнення характерне і згаданій вище праці Ч.Краутхеммера [6], який трохи пізніше, тобто упродовж другої половини 1980-х усіх 1990-х років грав центральну роль у консолідації неоконсерваторів навколо ідеї нової зовнішньої політики для посткомуністичної доби. Тут слід врахувати, що розпад комуністичної системи та її ключового представника, яким був Радянський Союз, на перших порах став шоком для стратегічних планів неоконсерваторів, оскільки всі їхні заклики до агресивності мали на меті знищення "*комуністичної імперії зла*". З її зникненням з політичної карти світу їм довелося шукати нового ворога.

Слід враховувати, що у цей час рішуче активізуються неореалісти від неоконсерватизму, скажімо, Джін Кіркпатрік, яка закликала обмежити прив'язування зовнішньої політики США до національних інтересів. Зі свого боку, відомий політичний експерт Дж.Муравчик, що відстоює ідеали "глобалістського" крила демократичної партії, з ідеалістських засад пропонував стати на шлях реалізації зовнішньої політики, яка б скористалася неперевершеною могутністю США для поширення демократії, вільної торгівлі і американських цінностей у світових масштабах.

Втім, для Буша і його команди таке переважно методологічне та частково ідейне протиборство з практичного погляду було другорядним, оскільки не виходило за рамки наукової дискусії. Звертати увагу доводилося переважно на вихідців з Американського підприємницького Інституту, до якого причетна ро-

дина віце-президента США Діка Чейні. Поки неоконсервативний політологічний дискурс здійснювався у контексті суперечок між ідеалістами і неореалістами, експерти, а також позбавлене методологічних обмежень прагматичне відгалуження неоконсерваторів зайнялися побудовою форми, методів і механізмів реалізації великої стратегії нового президента. На чолі цієї групи опинилися П. Волфовітц, І.Льюіс Ліббі та З.Халілзад. На рівні політичного інстинкту вони, де-факто, протиставили свої розробки неореалістському баченню, основаному на принципах міждержавного протистояння як головного чинника захисту і реалізації національних інтересів. З їх погляду, такий підхід був абсурдним в ситуації тотальної переваги США над всіма іншими акторами міжнародної системи. Прагматикам прийшов на допомогу теоретик Краутхеммер. Як прихильник демократизаційної парадигми односторонній глобальній політиці Сполучених Штатів він по суті стимулював ідеї згаданої вище прагматичної трійки науковою аргументацією постулату про те, що головне для великої стратегії глобальної держави полягає у якості і темпах здійснюваних за кордоном операцій. Для нього безперечна військова перевага США була основою не стільки для традиційного попередження і стримування зовнішніх загроз, скільки для сприяння прискореному переходові нових незалежних держав до статусу ринкових демократій. Де-факто, саме Краутхеммер запропонував цілковито нову велику стратегію США, яка, з одного боку, увібрала в себе елементи ізоляціонізму та ліберального інтервенціонізму (інтернаціоналізму) як найбільш сталих основ зовнішньополітичного курсу США , а з другого боку – представив дивовижну для багатьох дослідників суміш теорії і методології неореалізму з так званим демократизаційним глобалізмом, який у вітчизняній політології визначено як вершину односторонньої політики адміністрації Буша.

Не відкидаючи ізоляціонізму по суті (в рамках особливостей географічного розташування США), тобто формально залишаючись в межах Доктрини Монро, він доводить його обмеженість в умовах технологічних складових глобалізації та поширення міжнародного тероризму, який вводить у життя громадян окремих держав і світового суспільства тотальний страх.

Стосовно ліберального інтервенціонізму, тут для Краутхеммера все значно простіше. Він просто називає його політичною ідеологією демократичної партії, яка відстоює традиційну багатосторонність, незважаючи на домінуючу роль Сполучених Штатів у світовому співтоваристві націй. Відомий творець неоконсервативної ідеології переконаний, що у такий спосіб (багатосторонність) Америка обмежує можливості поширювати свободу і демократію вже самим фактом врахування інтересів, ідей і пропозицій інших учасників міжнародної системи. Такий ідеалізм, за його визначенням, вже самим прагненням запровадити верховенство права у міжнародні відносини ігнорує можливий наслідок у формі хаосу світ-системи.

Врешті, неореалізм у Краутхеммера також набуває своєрідних особливостей. За його тлумаченням, сучасний неореалізм починається тоді, коли йо-

го адепти розглядають світ таким, яким він є насправді. Замість поняття "*хаос*", яке є постійним у традиційному реалізмі та неореалізмі, він запроваджує своє визначення міжнародної системи як "*какофонії обмежених амбіцій і розділених цінностей*". Головний же його "неореалістський" постулат полягає у повному запереченні балансу сил як форми підтримки міжнародної стабільності з огляду на відсутність відповідних претендентів на участь у ньому за умов безумовної переваги США у світ-системі. Односторонність для Краутхеммера, а відтак і для Буша, належить до політологічних категорій, які в сучасних умовах заперечувати неможливо. Не баланс сил, а незаперечне домінування Америки, стверджує він, здатне не допустити подальшого падіння міжнародних відносин у прірву хаосу і глобальної анархії. Врешті, тут він зовсім відвертий, стверджуючи, що в сучасному світі остаточно визначилися два ключові елементи міжнародних відносин, якими є сила та інтерес. Та було б одностороннім вже з нашого боку подавати "неореалістську" парадигму Краутхеммера винятково в рамках односторонності. Він кожного разу додає до своїх міркувань тезу про неможливість для Америки в умовах глобалізації здійснювати неореалістську політику наодинці. Адже існує інша складова американської позиції в рамках великої стратегії епохи глобалізації і глобалізму: відстоювання спільних цінностей євроамериканської цивілізації. Тобто "*воля і сила*" та можливості США тут потрібні для реалізації ідеї "європеїзації" та "американізації" політичних систем всіх національних акторів системи міжнародних відносин як єдиного реалістичного чинника збереження стабільності і миру у світі. Як узагальнення такого "неореалізму" звучать дотичні заперечення Краутхеммером верховної ролі норм, договорів і багатосторонності як їхнього наслідку.

Переходячи до великої стратегії Буша-молодшого, відзначимо, що в її основу покладено одну з ключових ідей Краутхеммера: демократизаційний глобалізм. Тобто для 43-го президента США головними у всьому наборі постулатів цього дослідника міжнародних систем виступають не сила і влада, а вищі людські цінності, зокрема, свобода як вирішальна спонука цивілізаційного поступу. У цьому сенсі Буш мав би виглядати продовжувачем і практичним виконавцем філософських ідей великих європейських і американських мислителів різних історичних епох. Своєрідне розуміння сили (могутності) полягає у цьому випадку в постулаті про те, що вона потрібна не для завоювань і територіальних розширень в рамках класичної геополітики, а для поширення демократичних свобод у світовому вимірі. Демократизаційний глобалізм у такому сенсі покликаний розглядати неореалістський принцип верховенства сили як політично привабливий для всіх народів і суспільств. Поширення демократії для Буша в рамках політологічної парадигми Краутхеммера є водночас метою і засобом, що нерідко призводить до плутанини в оцінках великої стратегії першої американської адміністрації 21-го століття.

Безсумнівним пріоритетом великої стратегії Буша-молодшого виступає повсюдна підтримка демократичних змін і перетворень, яка має свої обмежен-

ня в рамках винятково стратегічних потреб американської держави. Готовність адміністрації проливати кров американських солдатів, за Бушем, виправдана тільки тоді, коли без цього неможливо стримати ворога від нанесення такого удару по Америці і світовому демократичному поступові, який може бути непоправним.

Для України як держави, яка перебуває на етапі становлення і розвитку власної зовнішньополітичної стратегії, дуже важливо враховувати окреслені нами постулати Краутхеммера, високою мірою запроваджені у велику стратегію Буша. Найважливішим поміж них бачиться заперечення тоталітаризму та попередження можливості його розростання у загрозу світовій стабільності і поступові демократії. Саме у цьому сенсі сьогоднішні американські неоконсерватори в рамках представленого вище оновленого неореалізму досить часто представляють перспективу розвитку політичної системи і міжнародних амбіцій Російської Федерації.

Але кожного разу на перше місце виноситься загроза арабо-ісламського тоталітаризму, а звідси – й ідея визволення арабських народів з-під політико-ідеологічного "гніту" місцевих режимів. При цьому потенційні наслідки такої боротьби американців часто-густо прирівнюються до тих, що мали місце внаслідок нанесення поразки німецькому нацизмові і японському мілітаризмові в епоху Другої світової війни. Американців переконують у тому, що "антиамериканізм" ісламських фундаменталістів близький до "антиамериканізму" нацистів і японських агресорів. За словами Краутхеммера, як і у випадку з "Німеччиною і Японією те, що ми робимо, є гігантською справою... Це війна, а у війні арешти вбивць – це прекрасно. Але ви виграєте не просто захопленням території, а залишенням чогось після себе" [439]. Як би у продовження Джордж Буш-молодший, презентуючи нову Стратегію національної безпеки США навесні 2006 року, розпочав словами про те, що "*Америка перебуває у стані війни*".

11 вересня 2001 року для таких неореалістів не є ні кінцем старої, ні початком нової історії. Це всього лише історичний поворот, що знаменується запереченням основної парадигми міжнародних відносин 20-го століття, базованої на радикальних політичних ідеологіях і наявності сутнісних ворогів суспільної демократії і відкритим ринковим відносинам. За великим рахунком, "неореалістська" велика стратегія адміністрації США, яка перебуває при владі у перші вісім років 21-го століття, фокусується на протидії арабо-ісламському тоталітаризмові. Але стратегічно значимими розглядаються також перспективи надмірного піднесення Китаю, демографічного колапсу Європи і (меншою мірою) становлення і зміцнення авторитарного режиму в Росії зі спробою відтворення єдиного імперського простору на пострадянських теренах.

Немає достатніх підстав і аргументів для того, щоб стверджувати, що можлива перемога демократичної партії на президентських виборах 2008 року спричиниться до рішучих змін у великій стратегії США. Адже близьким за своєю глибинною суттю до неореалістського (за Краутхеммером) бачення ве-

ликої стратегії є так званий "прогресивний інтернаціоналізм", розробником якого став також мало відомий і практично не представлений в українській міжнародно-політичній думці Інститут прогресивної політики, що діє в рамках опіки з боку Національної демократичної фундації. Будучи мозковим центром Ради демократичного лідерства, він пропонує так званий "третій шлях" реалізації великої стратегії США, що мав би враховувати позиції лівого, центристського і правого спектру американського політикуму. За очевидної схожості з неоконсерватизмом та високим рівнем використання адміністрацією США він має і свої особливості. Перша серед них полягає в тому, що, як і "холодна війна", нинішнє протистояння сил демократії і тоталітаризму триватиме десятиліттями [444]. На цьому аналогії з епохою системного протистояння соціалізму і капіталізму не вичерпуються. Приміром, війну з режимом Хусейна, яку інститут обґрунтовував і, відповідно, підтримував, там тлумачать як вимушену внаслідок невдачі політики стримування. Оскільки іракський режим підривав колективну безпеку і спричиняв деградацію міжнародних відносин аналогічно до того, як це свого часу робили держави радянського блоку, він мав бути ліквідований.

Радикалізм розробок інституту не викликає сумнівів хоча б з огляду на різкі закиди на адресу адміністрації Буша, яка, на погляд "прогресистів", не надто амбітна і позбавлена потрібної уяви про реальну ситуацію і загрози світовій стабільності. З іншого боку, привертає до себе увагу така особливість позиції представників інституту, що працюють на демократичну партію США, як заперечення доцільності ракетної оборонної системи США у якості базового інструменту забезпечення національних інтересів.

Чи не вирішальною відмінністю "*прогресивного*" демократичного глобалізму слід вважати певну орієнтацію на багатосторонність як ключовий інструмент. Тільки у такий спосіб, вважають експерти інституту, можна використати американську могутність для реформування ООН, міжнародних валютно-фінансових інституцій та СОТ. Тільки у випадку невдачі дипломатичних зусиль за доцільним є використання потенціалу Збройних сил США. Згідно з доповідями цього дослідницького центру, тільки "прогресивний інтернаціоналізм" спроможний узгодити позиції правих прихильників неоімперіалізму та лівих прибічників повного невтручання у світові справи. Так, зокрема, вважає президент Інституту прогресивної політики В.Маршалл.

Але це має бути не так званий "*беззубий*" (пасивний) інтервенціонізм, що ставить під питання консенсус між американськими союзниками і веде до хаосу у відносинах між ними. Такий інтервенціонізм "прогресивного" ґатунку мусить орієнтуватися на виявлення реальних ворогів і конфліктів та їх рішуче подолання.

Вочевидь сутнісною ознакою такої версії великої стратегії США виступають заперечення антиглобалістської парадигми і неприйняття антиглобалістів. Цікавим нам видається пояснення, до якого вони вдаються при цьому: мовляв, антиглобалізм прирікає країни, що розвиваються, на міжнародну

ізоляцію, а їхні народи — на довічну бідність. За такого підходу має місце логічне продовження у формі повного заперечення західного протекціонізму стосовно держав третього світу.

Прогнозуючи поки що гіпотетичний міжнародно-політичний курс демократичної адміністрації у разі перемоги на виборах 2008 року, слід брати до уваги наявність у рядах партії демократів «ліберальних яструбів», на думку яких, слід відмовитися від курсу на обмеження бюджету Пентагону та стати на шлях військових втручань у різних регіонах планети.

Особливий підхід до формулювання головної стратегії США належить прибічникам так званого ліберального реалізму, серед яких вирізняються Г.Ікенберрі та Ч.Купчан. У статті на цю тему [445] вони наголошують, що Сполучені Штати фактично втрачають статус світового гегемона внаслідок односторонності, яку сповідує адміністрація Буша. Його головна стратегія, з їхнього погляду, помилкова, оскільки кладе в основу неоконсервативну ідею, взяту на озброєння від 1979 року, про міжнародну систему як побічний продукт американського верховенства. Виходячи з того, що американська військова перевага та безсумнівне лідерство в технологічній сфері є гарантією збереження домінуючої ролі в умовах однополярності, адміністрація США бачить нинішню міжнародну систему в рамках винятково свого верховенства, не помічаючи таких її вад, як розмежування і безладдя, виклики американській однополярності, руйнівні економічні протистояння, міжнародний тероризм і порушення принципів нерозповсюдження зброї масового знищення.

На противагу такому підходові властей дослідники й пропонують головну стратегію на засадах ліберального реалізму, яка б базувалася на таких концептуальних складових:

- Реставрація багатосторонності, повернення обличчям до міжнародного права, реальна відданість вільній торгівлі, сприяння інтегруванню новостворюваних центрів сили на правових принципах.
- Комплексний підхід як форма одержання вигод від американського гегемонізму.

Не заглиблюючись у саме поняття "реалізму", Ікенберрі та Купчан різко критикують зовнішню політику Буша за одновимірне світосприйняття в чорно-білих тонах, що спричиняється до розбалансування міжнародної системи. Пропонуючи натомість застосування м'якої сили і дипломатичних механізмів як засіб легітимації ефективного американського лідерства, вони вже з суто неоконсервативних позицій аргументують свої висновки та пропозиції тим, що інакше Сполучені Штати втратять здатність впливати на плани і дії міжнародного співтовариства націй та визначати форми й механізми майбутнього керованого світового порядку. Орієнтація винятково на військове домінування врешті-решт, на їхню думку, може стати самоціллю без видимих здобутків для американської нації і суспільства.

Автори парадигми ліберального реалізму виходять у своїх оцінках з того, що за нинішнього підходу до розробки й реалізації головної стратегії вже в

ближчі десятиліття американське верховенство відійде в минуле під тиском нових центрів сили. До їх числа ними відносяться Євросоюз, Китай, Бразилія, Індія та, можливо, Японія. При цьому Росія виноситься за ці рамки без особливих пояснень. З метою убезпечення американських національних інтересів від згубних впливів односторонності Ікенберрі і Купчан пропонують налагоджувати кооперативне партнерство з цими державами та інтеграційним формуванням. Метою оновленої зовнішньої політики США вони бачать становлення міжнародної системи, в якій союзники діятимуть так, як це прийнято серед акціонерів великих корпорацій.

Стосовно міжнародного тероризму їхня позиція також особлива у сенсі "*надмірностей*", які йдуть від нинішньої головної стратегії США. Чорно-біла картина світу, взята на озброєння офіційним Вашингтоном після трагедії 11 вересня 2001 року, не розділяється більшістю світового співтовариства націй, що означає перспективу самотності Америки у майбутній міжнародній системі. Зосередившись на подоланні арабо-ісламського тоталітаризму і екстремізму, адміністрація Буша не помічає інших стратегічно значимих аспектів світової політики, що базуються на міжнародному праві, відповідних нормах, затверджених у міждержавних договорах і багатосторонніх домовленостях. Тим часом, ліберальні реалісти, пропонуючи повернутися до ліберального інтернаціоналізму епохи антигітлерівської коаліції, додають до списку пріоритетів захист навколишнього середовища. Екологічна проблематика для них не просто значима, але першочергова у загальній системі ціннісних координат. У цьому сенсі зовнішня політика адміністрації Буша видається їм такою, що веде країну до маргінального курсу і відповідного місця у майбутній світ-системі. Уникнути такої ситуації, на їхню думку, неможливо поза рамками діяльності, базованої на правилах та інститутах міжнародної системи як цілісної інфраструктури. Врешті, навіть вільна торгівля як складова головної стратегії оцінюється ними негативно у поданні Буша та його команди, оскільки практично нічого не робиться для захисту інтересів американських трудящих, які зазнають втрат від глобалізації.

Кліффорд Купчан подає специфічне визначення демократизаційної складової у великій стратегії США як віце-президент помірковано консервативного дослідницького Центру імені Ніксона [446]. Він представляє своє бачення нової головної стратегії демократичної партії, що, на його погляд, може повернути її і, власне Америку, в сприятливе русло співробітництва з міжнародною спільнотою. Це, за його словами, може відродити демократів, які дещо розгубилися внаслідок гуманітарних акцій в Сомалі, де вони вдалися до віджилих підходів минулого, не зумівши належним чином скористатися велетенською могутністю Америки.

Як і К.Купчан та Г.Ікенберрі, він відстоює власний варіант реалістської парадигми. Його суть у тому, що саме реалізм диктує врахування у головній стратегії США того факту, що сучасний міжнародний порядок останніх кількох десятиліть позначений безпрецедентною однополярністю Америки.

Такий підхід, за його висновком, "нормативно сприятливий і емпірично неминучий". Дискусія навколо війни в Іраку не може, як він вважає, реально змінити цю оцінку. Демократам же пропонується скористатися однополярним світом, аби продовжити і навіть вдосконалити такий стан речей у міжнародній системі, водночас підтримуючи і забезпечуючи "*ключові інтереси США*".

Головну стратегію Буша він, як і його колеги з табору ліберальних інтернаціоналістів, критикує не за невдале верховенство у світових справах, а радше за надмірну односторонність і брак легітимності. Адже така позиція по суті провокує інші держави докладати максимум зусиль для прискорення процесу ліквідації однополярної епохи, утруднюючи захист життєвих інтересів Сполучених Штатів.

К.Купчан не надто стурбований тим, що інші великі держави чи міждержавні союзи могли б всерйоз розбалансувати американський варіант однополярного світу, вважаючи, що створена при первинній ролі США безпрецедентна стабільність і система міжнародної торгівлі приносить дивіденди якщо не всім, то більшості учасників міжнародного співтовариства націй. Стосовно відновлення балансу сил ідея К.Купчана базується на впевненості в тому, що ближчим часом Америка не матиме вагомих конкурентів у світові й політиці. Водночас, на його думку, американський глобалізм сам по собі не стимулює однополярності міжнародної системи. Не будучи надмірним прихильником багатополюсності, К.Купчан просто переконаний у тому, що головна стратегія має представити широкий простір для багатосторонніх рішень: "Граючи за спільними правилами міжнародних інститутів, на зразок ООН і СОТ, гегемон знаходить ще одну лазівку для прив'язування інших держав і запевнення їх у тому, що його повноваження будуть поміркованими і навіть до якоїсь міри відносними". Що ж стосується гіпотетичної перспективи відновлення багатополюсного світу, то для Г.Купчана вона є такою, що не відповідає життєвим інтересам США.

Такий варіант реалізму уможливив відповідне узагальнення: "Як і у випадку з альянсами, інститути за умов однополярності зазвичай будуть відображати політичні преференції Америки". Метою ж головної стратегії США дослідник називає якомога довше пролонгування однополярності та переваг у питаннях жорстких політичних рішень. Бушівський варіант однополярності він окреслює як обмежений і такий, що веде до безпрецедентного хаосу замість формального балансу. Внаслідок цього прогнозується заперечення американського лідерства багатьма учасниками світової політики. На противагу ізоляціоністам і багатьом реалістам традиційного ґатунку, К. Купчан відстоює тезу про те, що Real Democratik не може бути стриманий економічними і безпековими інтересами у їх вузькому розумінні. Тим самим підводиться висновок про те, що головна стратегія США має залишатися вірною моральним принципам американської зовнішньої політики.

З цих причин і міркувань пропонується приділяти більше уваги слабким державам, сприяти розвиткові країн Африки та інших країн, що розвивають-

ся, на засадах добре продуманого сприяння демократії і правам людини, допомоги у подоланні хвороб, організованої злочинності, протидії кліматичним змінам, торгівлі наркотиками і людьми.

Детальніше еволюція суперечливих головних стратегій США після Другої світової війни може бути зрозуміла тільки в рамках так званого наступального чи оборонного реалізму. Тут ми згодні з американськими дослідниками, які подають саме таку картину становлення і прийняття таких стратегій [447].

Але найбільш загальну і, безумовно, фундаментальну ідею щодо наповнення всіх без винятку головних стратегій зовнішньої політики США дав керівник глобальних програм Центру міжнародних відносин Дж.Гершман як один з ключових учасників доповіді, що була ним підготовлена спільно з експертами з Інституту політичних досліджень під промовистою назвою "*Безпечна Америка у безпечному світі*" [448].

Вона присвячена ключовій проблемі бушівської головної стратегії боротьбі з міжнародним тероризмом, і в концептуальному сенсі серйозно відрізняється від ідентичних розробок представників інших шкіл. Сам же Гершман, будучи близьким до ліберально-інтернаціоналістської традиції, пропонує справді радикально нову парадигму боротьби з окресленим злом в рамках прийнятих у світі політико-правових норм. Більше того, автор пропонує і надалі зайнятися зміцненням і розширенням міжнародних домовленостей з питань подолання тероризму. Заперечуючи ідею тотального домінування як вирішальну у головній стратегії США, він натомість висуває ідею формування за участю Америки гнучкої мережі глобальних, регіональних і двосторонніх альянсів як основи для гарантування такої безпеки всього світу, яка забезпечить безпеку США.

Втім, доповідь дещо відходить від ліберально-інтернаціоналістської традиції в сенсі критики зусиль уряду США розширити свої торговельні відносини і максимально лібералізувати світову торгівлю. Автори вирізняються низкою інших особливостей у своїх концептуальних підходах. Для них значно важливіше, ніж для адміністрації Буша, виявити спонуки, причини і джерела міжнародного тероризму в соціальній та інших сферах життєдіяльності людей, суспільств і держав. Виходячи з того, що тероризм не відповідає інтересам переважних громадян, незалежно від того, де вони мешкають, вноситься ідея створення ворожого економічного, соціального і політичного клімату для терористів, маючи на увазі позбавлення їх будь-якої підтримки з боку населення країн, на яких розташовані терористичні центри.

Фактично погоджуючись з відомою ідеєю неоконсерваторів про те, що головним джерелом тероризму є арабо-ісламський тоталітаризм і екстремізм, колектив авторів доповіді на чолі з Гершманом виступає за різке зниження залежності Америки від поставок близькосхідної нафти за рахунок реалізації спеціальної програми енергозбереження і відновлення енергоресурсів.

Конкретно до методів боротьби з тероризмом віднесено такі два ключових моменти, як постійна готовність і попередження через посилення міжна-

родного співробітництва в рамках багатосторонньої акції та захисту громадянських прав.

Оригінальна версія головної стратегії міститься у доповіді військового аналітика з консервативної Фундації за вільний конгрес В.Лінда [449].

Погоджуючись з традиційною для консерваторів США ідеєю про те, що "головний симптом" міжнародного тероризму лежить у сфері його походження від ісламського екстремізму, що вносить хаос у міжнародні відносини, ним у журналі згадуваного вище П.Б'юкенена "Американський консерватор" пропонується повернутися до стримування в рамках однієї з двох базових головних стратегій США – ізоляціонізму якнайбільш ефективного способу подолання і попередження хаосу, що входить у міжнародну систему від держав, які перестають виконувати свої місії, або від недержавних озброєних акторів.

Кращим і найбільш ефективним засобом боротьби з тероризмом він визначає відмову від нападів на інші держави та перехід до оборонної стратегії. При цьому вона має бути, за словами військового аналітика, такою, що "знищує" ворога. Робити це, на його погляд, можна справді ефективно у випадку розвитку зв'язків з партнерами та ізолювання від ворожого оточення.

Відтак, новий ізоляціонізм для 21-го століття відрізняється від Доктрини Монро, у першу чергу, підтримкою і розвитком трансатлантичного альянсу, що має постійно розширюватися. Важливими учасниками антитерористичної кампанії він називає також Китай, християнство і бізнес.
Стосовно ж територій, які мають бути ізольовані, то на першому місці стоять: "значна частина Африки, Месопотамія, Афганістан, частина колишнього Радянського Союзу і західний Берег Йордану".

За висновком і аргументацією Лінда головна стратегія Буша у її нинішній формі і з застосуванням механізмів воєнного наступу стимулює хаос у міжнародній системі. Більше того, він вважає, що такі напади і вимоги демократичного реформування тільки розширюють коло зовнішніх загроз і підштовхує прихильників тероризму до об'єднання. Замість цього експерт вважає доцільним посилити ефективність роботи спецслужб і блокувати центри поширення хаосу.

Інший аспект безладдя і хаосу для Америки вбачається у цьому випадку в неконтрольованій імміграції, яку слід зупинити з огляду на те, що вона вже стала причиною культурних конфліктів.

У теоретико-методологічному вимірі найбільш чітко сформулював головні ідеї для американської головної стратегії на 21-ше століття відомий політолог із Йєльського університету Джон Льюїс Геддіс [450]. На його думку, доволі успішна головна стратегія Буша періоду першого президентства тепер має зазнати змін. Аби не допустити реалізації існуючих загроз, він пропонує вдаватися не просто до попереджувальних акцій, але й відповідних воєн. Такий підхід, на погляд знаного фахівця, не має залежати від того, яка партія домінує в конгресі і від якої політичної сили обраний президент. Що стосується "поправки" на другий термін президента Буша, то Геддіс вважає

доцільним частіше вдаватися до переконання і активнішого роз'яснення суті головної стратегії на міжнародній арені.

Для професора Геддіса така головна стратегія включає в себе ліберально-демократичні ідеали як базовий засіб формування загальної безпеки. Першим об'єктом демократизації має стати, знову таки, Близький Схід.

Ще одна "поправка" Геддіса зводиться до необхідності "збирати до купи частини нового порядку", для чого "*шокової терапії*" недостатньо.

Загалом же, проведений автором аналіз дозволяє стверджувати, що від січня 1993 року до весни 2006 року в Сполучених Штатах відбувався процес формулювання головної стратегії, яка має всі підстави так називатися. При оцінюванні цієї стратегії слід виходити з того, що США є державою, котра упродовж своєї історії фактично реалізувала всі фундаментальні цілі, які ставилися владою у формі доктрин і стратегій національної безпеки, що є виразом більш загального бачення. Повною мірою можемо говорити про те, що стратегія Дж.Буша-молодшого концептуально є продовженням наступальної стратегії демократизації світу, представленої переважно на регіональному рівні президентом від демократичної партії Біллом Клінтоном. Його наступник у Білому домі вніс суттєві уточнення, головні з яких полягають у наданні цій стратегії глобальних вимірів та застосуванні всього потенціалу американської держави для завдання поразки учасникам "осі зла", від яких йде нині найбільша загроза національним інтересам США, стабільності і мирові у формі міжнародного тероризму.

4.3. Політика культурної експансії США в міжнародних відносинах

Теоретично концепцію культурної експансії було обґрунтовано у наукових працях відомих фахівців-політологів С. Хантінгтона, З. Бжезинського, Ф. Фукуями, С. Сміта та ін., які вважають її важливою складовою зовнішньополітичної діяльності країни з метою забезпечення глобального політичного лідерства США. Ці праці розвинули головну зовнішньополітичну ідеологію Америки XX століття – ідеологію гегемонізму, запропоновану в дослідженнях К. Шмітта та А. Грамші.

Так, на думку К. Шмітта, сутність імперіалізму полягає не тільки у військових завоюваннях та економічній експлуатації народів, а й у м'якому тиску, яким є культурна експансія, тобто "імперіалізм" у сфері культури або тиранія "нав'язування цінностей". Культурний імперіалізм може дорівнювати військовому вторгненню, або, якщо розвинути думку К. фон Клаузевіца, вторгнення ідей американської політичної теології, подібно до дипломатії, є "продовженням війни іншими засобами", засобами ідеології. Такий імперіалізм є надзвичайно небезпечним, оскільки він руйнує прагнення до національного самовизначення. Американська гегемонія базувалася і продовжує базуватися на геополітичній гегемонії США, яка визначає і нав'язує

структуру нового міжнародного порядку на основі глобалізації відомої доктрини Монро, тобто заперечення міжнародного плюралізму.

Концепція природного права американського імперіалізму викладена у теологічних настановах універсалізму, де американська гегемонія визначається як довічний і природний стан світового суспільства, оскільки категорія абстрактного співтовариства є ідеологічним прикриттям конкретних національних інтересів США. Саме універсалізм розвивав ідею абсолютної влади однієї країни (монополярність політики), прикриваючи її ідеологічними поняттями природного стану світового співтовариства [451].

Ф. Фукуяма підтвердив необхідність монополярної гегемонії США, вважаючи що американізм є кінцевою метою і заключною стадією ідеологічної еволюції людства, найдосконалішою формою державної влади, а його прихід знаменує кінець історії [452].

С. Хантінгтон, аналізуючи американську стратегію "доброчинного гегемона", робить висновки, що існують суттєві розбіжності між образом "носія демократичних цінностей, свободи і стабільності" та справжніми намірами США у геополітичних процесах. Зокрема, культурна складова зовнішньої політики країни, включає примусове запровадження американських цінностей та інститутів демократії в інші політичні системи; фактично порушення принципів державного суверенітету і втручання у внутрішні справи окремих держав, в яких США намагаються реалізувати американську модель демократії та економіки, свої моральні і культурні цінності. С. Хантінгтон також звертається до зворотного боку політики гегемонії США, вважаючи, що ілюзія гегемонії, яку створюють США, не має реальної основи в самій Америці, оскільки правляча еліта діє незалежно від громадської думки, а ухвалені рішення є дедалі більше втаємниченими [453].

С. Сміт звертає увагу на те, що демократична модель, яку поширює США, є моделлю демократії для еліти, коли зберігається значний відрив між елітою та рештою суспільства. В цій моделі не враховуються культурні та історичні традиції інших країн, неприйняття американських цінностей та пріоритетів в іншому суспільстві. Він вважає, що концепція глобального лідерства, яку реалізують США через доктрини зовнішньої та внутрішньої політики, характеризується як "культурний імперіалізм" [454].

Х. Овада зазначав, що після закінчення другої світової війни США проводили політику "однобічного глобалізму", опонуючи комунізму та підтримуючи тенденції створення відкритої світової економіки, яка сприяє економічному розвитку та зміцненню міжнародних фінансових організацій. З розпадом СРСР з'явилася нова стратегія США – "глобальної уніполярності", тобто просування американських інтересів у глобальному світі, що, на його думку, може призвести до ізоляції США на світовій арені. Зазначимо, що аналогічного погляду дотримуються англійські фахівці з міжнародних відносин, які переконані, що тільки у США пишуть про бажання решти світу бачити Америку світовим лідером, а за межами Сполучених Штатів вважають

зовнішню політику наддержави як "американську жорсткість, прагнення єдиновладдя" та "*примусовий колективізм*" [455].

З. Бжезинський у відомій праці "*Велика шахівниця*" наголошував на тому, що культурна перевага є недооціненим аспектом американської глобальної сили, оскільки американська масова культура є надзвичайно потужним чинником впливу на світову спільноту: американські телевізійні програми та фільми складають майже три чверті світового ринку інформаційних продуктів та послуг; американська популярна музика панує у глобальних масштабах, американську модель життєдіяльності та мотивацію поведінки дедалі більше наслідують спільноти в різних країнах; інформаційні ресурси Інтернету також англомовні; врешті, Америка перетворилася на "Мекку" для тих, хто прагне отримати сучасну освіту та зробити успішну кар'єру. З. Бжезинський наголошує, що ідеали, пов'язані з американськими політичними традиціями, дедалі більше сприймаються у міжкультурному співробітництві як прояв "культурного імперіалізму", а американська перевага зумовлює новий міжнародний порядок, який не тільки копіює, а й відтворює у міжнародних відносинах модель американської політичної системи [197].

Відомий російський дослідник О.С. Панарін, розглядаючи проблеми глобалізації світу, звертається до ролі США у цьому процесі. Зокрема, він вважає, що в основі американської державної моделі закладена своєрідна культурофобія: 1) на індивідуальному рівні обтяженість культурними "комплексами" заважає досягати успіху в досягненні цілей, за допомогою засобів, які були засуджені "старими" культурами; 2) на колективному, національно-державному рівні ця обтяженість спричинює феномен подвійного громадянства і заважає формуванню безумовно лояльних, "стовідсоткових" американців. Такий прийом "приручення до Америки" за рахунок розриву зі "старими культурами" американські гегемоністи почали використовувати у світовому масштабі, формуючи армію прозелітів, які з тих чи інших причин виявилися готовими до розриву зі своїми національними культурами. Дискредитація культурної спадщини, на думку науковця, зумовлена самою програмою глобалізації світу як американоцентричної та американоподібної моделі, яка вимагає рішучої дискредитації інших культур як несучасних або недостатньо сучасних з погляду реалізації політики.

Ставлення Америки до решти світу, на думку О.С. Панаріна, можна порівняти зі ставленням перших відкривачів та колоністів до "*туземної культури американських індійців*". Під впливом американоцентричного лібералізму статус стародавніх культур на всіх континентах безперервно знижується, і всі вони потрапляють під підозру як бар'єри на шляху до економічної та політичної революції, яку несе світові американський авангард. Боротьба "економіки з антиекономікою" як кредо даної революції означає зростання знецінення культурної спадщини та культурних цінностей порівняно з матеріальними ресурсами. Народи — носії застарілих культур внаслідок історичної випадковості, стверджує О.С. Панарін, виявилися власниками

природних багатств, якими вони не вміють розпоряджатися. Така "антитоталітарна" критика чужих культур розкриває свої підтексти, пов'язані з планетарним перерозподілом ресурсів на користь наддержави [456].

Феномен "культурного імперіалізму" з позиції економічного та інформаційного домінування США у світі розкривається у дослідженнях Г. Шіллера, Дж. О. Бойда-Баретта, А. Метлеарта, К. Роача, Д. Смайті та ін., які вважають концепцію культурного імперіалізму відображенням культурної потужності та популярності американської маскультури і ефективних ринкових стратегій впливових американських компаній і транснаціональних корпорацій.

Проблема трансформації культурного імперіалізму в умовах глобалізації та становлення інформаційного суспільства посіла центральне місце у наукових дискусіях 70-х рр. XX ст. Обґрунтування змін політики міжкультурного співробітництва, на думку К. Роача, пов'язане з іменами А. Пасквалі, Л.Р. Белтрана та М. Каплана, наукові розвідки яких стали основою світового руху за Новий міжнародний інформаційний та комунікаційний порядок, політичну доктрину якого підтримала спеціалізована установа ООН з питань освіти, науки, культури та комунікацій ЮНЕСКО в рамках програми свободи вираження та вільного обміну ідеями між націями. Головні дослідження були присвячені проблемі "*медіаімперіалізму*", як важливій складовій "культурного імперіалізму". Зокрема, медіаімперіалізм характеризувався як глобальне домінування західних націй у сфері засобів масової комунікації, яке здійснюється за рахунок потужного впливу на культури країн "третього світу" шляхом нав'язування їм західної ментальності, світогляду і водночас руйнування їх самобутніх культур [457].

Так, англійський дослідник Дж. О. Бойд-Баретт визначав медіа імперіалізм як процес зовнішнього тиску та забезпечення інтересів корпоративних медіагруп без дотримання пропорційності взаємообмінів та інформаційних взаємовпливів [458]. Визначення дослідника, на нашу думку, є занадто вузьким і недостатньо висвітлює проблему розмаїття форм, яких набувають політичні відносини між різними культурами.

На думку Г.Шіллера, який вважається засновником теорії культурного імперіалізму, розвинуті західні країни (західна цивілізація) виробляють більшу частину світової медіакультурної продукції, яка виступає чинником політики культурного імперіалізму, оскільки решта світу споживає через неї західний стиль життя, погляди та спосіб мислення. Таким чином відбувається імплементація культури західних країн у культури інших держав за рахунок руйнування їх самобутності. Культурно-комунікаційний сектор, вважає науковець, розвивається відповідно до цілей і завдань політики американського культурного імперіалізму. Односторонній у своїй основі потік інформації — від США до інших частин світової капіталістичної системи — є одним з атрибутів американського лідерства. Іншим атрибутом є нав'язування саме англомовної культури з використанням високошвидкісних та всеохоплюючих інформаційно-телекомунікаційних технологій, розробка яких тісно пов'язана зі

структурою і потребами провідних елементів системи. Ще одним важливим чинником культурного імперіалізму є його ринкова сутність, пов'язана з ідеологічними особливостями світової економіки, яка ефективно рекламує цінності західної цивілізації: медіа, наприклад, вважає Д. Огілві, засновник відомого рекламного агентства "Огілві енд Матер", здійснюють культурну дипломатію не менш ефективно, ніж ЮСІА політичні акції на рівні ідеологічного протистояння.

Досліджуючи діяльність багатонаціональних медіакорпорацій, Г. Шіллер робить висновок, що їх діяльність призводить до "культурної колонізації суспільства". На думку автора, важливим провідником культурної експансії західних країн, зокрема, США, виступає місцева правляча еліта. Г. Шіллер посилається на дослідження Е. Дапіно, який, аналізуючи механізми культурного контролю в Латинській Америці, відзначає той факт, що наслідки культурної залежності у цьому регіоні є результатом культурного "вторгнення" за сприяння правлячого класу латиноамериканських країн в інтересах "національного розвитку". В результаті такого вторгнення національна культура зводиться до знеособленої однорідної форми як необхідної умови функціонування політичної системи міжнародного співтовариства. Відбувається "культурна та ідеологічна гомогенізація світу, якої прагне і на якій наполягає не певна країна, а об'єднана система різних національних секторів, що базується на специфічній соціально-економічній формі відносин" [275].

Український дослідник В.В. Багацький вважає, що американська культура, яка сформувалася і розвивалася як національна, з другої половини XX століття за допомогою масової культури перетворилася в наднаціональну, підпорядковуючи духовне життя народів та країн світу ідейному впливу США, що дає підстави визначити ще один вид імперіалізму — культурний, сутність якого полягає у прагненні встановити панування у сфері культури в глобальному масштабі [459].

Критики теорії культурного імперіалізму — Дж. Томлінсон, Ч. Оген, Т. Лібс, Е. Катц, Р. С.-Н. Лі, Дж. Сінклер, С. Канінгем та ін. — вважають процес глобалізації чинником посилення американського лідерства, перерозподілу політичного впливу від урядів (у тому числі й США) до інших суб'єктів міжнародних відносин (ТНК), а власне культурний імперіалізм США — фантомом, бо експансія американської масової культури, на їхню думку, має поверховий характер і жодна нація не відчула на собі "асимілюючої" американізації.

Серед недоліків теорії культурного імперіалізму дослідник Ф. Фейджес називає відсутність концептуальної визначеності самого терміну "культурний імперіалізм". Водночас Р. С.-Н. Лі, аналізуючи тлумачення терміну, додатково визначає "культурний імперіалізм" як "комунікативний імперіалізм". Так, Дж. Томлінсон, аналізуючи праці з проблем культурного імперіалізму, виокремлює декілька головних підходів до визначення цього феномену: 1) культурне домінування, 2) медіаімперіалізм, 3) націоналістичний дискурс, 4) критика гло-

бального капіталізму, 5) критика модерніті. Зокрема, Дж. О. Бойд-Баретт "ототожнює культурний імперіалізм" з "медіа імперіалізмом", Дж.Гелтанг – із "структурним імперіалізмом", Дж.Лінк та Е. Мохаммаді – з "культурною залежністю та домінуванням", Дж.Хемелінк – з "культурною синхронізацією", Т. Макфейл – з "електронним колоніалізмом", Р. Суі-Нам Лі – з "комунікаційним імперіалізмом", Е. Метлеарт – з "ідеологічним імперіалізмом" та "економічним імперіалізмом", а І. Сейд – з колоніалізмом. Така розбіжність у підходах до визначення обумовлена тим, що кожен з дослідників намагався знайти джерело досліджуваного явища у різних сферах, аналізуючи різноманітні прояви процесу культурного імперіалізму [458; 460-468].

На думку Дж. Томлінсона, ототожнення культурного імперіалізму з медіаімперіалізмом є неправомірним, оскільки це робить поняття "*культура*" і "*медіа*" синонімами. Прибічники цієї теорії ставлять феномен медіа на перший план, приписуючи їм головну роль у культурному імперіалізмі, а терміном "*медіа*" замінюють термін "*культура*". Однак дослідник вважає, що слід ретельніше дослідити зв'язок медіа з іншими аспектами культури, апріорі не надаючи їм (медіа) центрального значення [462]. Натомість Ч.Оген, вважає, що теорія культурного імперіалізму має цілу низку недоліків, зокрема, не має обґрунтувань та пояснень і не виходить за межі суто описових підходів; культурний компонент, на відміну від економічних та статистичних показників, потребує іншого виміру досліджень [469].

Польові дослідження проявів культурного імперіалізму медіа (досліджувалося сприйняття різними етнічними групами Ізраїлю – арабським населенням, іммігрантами з Марокко, членами кібуців та іммігрантами з Росії – культового американського телесеріалу "Даллас") та наслідків його впливу на культурні цінності різних спільнот, які проводили американські науковці Т.Лібс, Е. Катц та Й. Енг свідчать, що існуючі концепції "культурного імперіалізму" не враховують здатність аудиторії інтерпретувати зміст відповідно до специфіки соціально-цивілізаційного досвіду і протистояти культурній експансії [470-471].

Австралійські дослідники Дж. Сінклер, Е. Джейк та С. Канінгем також вважають, що висновки прибічників культурного імперіалізму не мають системного характеру у випадках і явищах, які вони намагаються пояснити. Прикладом для них слугує телеіндустрія таких "периферійних націй", як Індія, Бразилія, Мексика, Середній Схід, в яких продукція вітчизняних телекорпорацій в національному інформаційному просторі становить близько 80% – показник, який залишається недосяжним для більшості англомовних ринків [472].

Таким чином, феномен культурного імперіалізму залишається дискусійним в теоретичному плані, а прикладні дослідження виявляють суперечливі характеристики цього явища в сучасному політичному та соціокультурному глобальному середовищі.

Американське політичне та ідеологічне лідерство із закінченням "холодної війни" трансформувалося у глобальне економічне, інформаційне та куль-

турне домінування. Наявність ефективного політичного, економічного та силового механізму зовнішньої політики у поєднанні з високим рівнем технологічного розвитку дали США унікальну можливість стати глобальним лідером і впливати на політику більшості країн світу. Важливим інструментом встановлення такого домінування є особлива політика міжкультурного співробітництва і американська культурна дипломатія.

Особливість політики міжкультурного співробітництва США базується на геополітичних стратегіях двох політичних сил країни – концепції "*жорсткої*" гегемонії (Республіканська партія) та концепції "м'якого впливу" (Демократична партія), які сповідують різні підходи, проте однаковий політичний результат домінування американських цінностей і американського способу життя у світі. Концепція "*жорсткої*" гегемонії виражає ідею американської обраності та месіанства і передбачає здійснення політики необмеженого глобального лідерства, для якого у США, з погляду ідеологів, політиків і практиків, є всі підстави. Республіканські сенатори Р. Лугар, Д. Армі та Б. Доул, аналізуючи американську зовнішню політику, підкреслювали, що здійснення зовнішньополітичних акцій повинно відповідати національним інтересам і підтримувати їх на всіх рівнях міжнародної взаємодії [473]. Відомий американський політолог З. Бжезинський виокремлює чотири показники унікального статусу глобального лідерства США: 1) глобальний характер воєнної могутності; 2) глобальний економічний потенціал; 3) технологічне лідерство; 4) універсальний характер і глобальний вплив американської політики "культурної експансії" [197; 455].

Концепція "м'якої" гегемонії враховує у політиці міжкультурного співробітництва статус глобального лідера США і практику створення наднаціональних механізмів врегулювання світових процесів задля реалізації месіанських ідей культурного американізму, проте здійснення такої політики спирається на культуру, ідеали та політичні стратегії за американським зразком і досягається через "*Soft Power*" ("*м'яку владу*"), тобто заохочення політичної еліти та світової громадськості до сприйняття привабливих демократичних і культурних цінностей США, бо, за висловом колишнього міністра закордонних справ США М. Олбрайт, Америка спонукає світ до ефективних дій, від яких неможливо відмовитись. [455]

Відомий дослідник політики "Soft Power" Дж. Най вважає, що значна політична і культурна привабливість цінностей Америки впливає не тільки на реалізацію зовнішньої політики держави, а й на діяльність більшості міжнародних інститутів, які відображають американські інтереси, та на світову політику міжкультурного співробітництва. Американська позиція у світі унікальна, зазначає Дж. Най, оскільки жодна інша країна в історії людства не досягала подібного. Інший погляд на культурну складову зовнішньої і внутрішньої політики висловлює С. Хантінгтон, який вважає, що міжнародна практика США демонструє розбіжності між задекларованою стратегією "м'якого гегемона" і справжніми намірами досягнення монопольного лідерст-

ва у світі на основі примусового впровадження американських цінностей та інститутів демократії. Політолог С. Сміт також звертає увагу на те, що демократична модель, яка поширюється на всі напрямки міжнародного співробітництва, – це модель демократії для політичних еліт інших країн, коли зберігається значний розрив між елітою та рештою населення і не враховуються національні культурні та історичні традиції і ставлення до американських цінностей і норм. Він характеризує таку концепцію глобального лідерства як "культурний імперіалізм" [453; 474-475].

Проте обидві концепції сприяють утвердженню монопольних позицій США у світі і доповнюються факторами союзницької та економічної допомоги США, на яку розраховують окремі держави – регіональні лідери, що належать до різних культур, мають різні геополітичні інтереси у конкуренції за лідерство на регіональному рівні і проблеми у виробленні спільних позицій і дій у міжнародних відносинах. Політику Америки підтримують й інші актори міжнародних відносин, оскільки усвідомлюють неможливість створення коаліцій провідних та "*другорядних*" держав, які зацікавлені в послабленні перших і шукають підтримки у глобального лідера.

Виклики XXI століття, прагнення забезпечити глобальне лідерство через привабливу ідеологію сприяння демократизації світу зумовили появу концепції "*американського інтернаціоналізму*", яка, на думку ідеологів такої концепції (К.Р. Холмс), спирається на людські цінності, глобальні за своїм змістом та загальні за своїми гуманістичними принципами. Ця концепція декларує можливість надати кожній державі і кожній спільноті інструменти для реалізації національного потенціалу на основі культурних, етнічних і релігійних традицій, а не прагнення нав'язати світові певні культурні стандарти, при цьому підкреслюючи, що жодна країна світу не в змозі забезпечити такі можливості, крім США. Дж. Буш – молодший, демонструючи багатосторонню політику держави, зазначив, що вона буде спрямована на поширення цінностей і можливостей за американським зразком. Прихильники концепції вважають "*американський інтернаціоналізм*" ні протекціоністським, ні експансіоністським, а таким, що забезпечує свободу, сприятливі можливості розвитку економіки, культурні права, людську гідність та добробут. При цьому стверджується необхідність через політику американського інтернаціоналізму просувати національні інтереси в країнах, яким США надають гуманітарну допомогу. В реалізації концепції "*американського інтернаціоналізму*" задіяні такі інструменти міжнародного співробітництва, як публічна та культурна дипломатія, які водночас виступають елементами культурної експансії держави [476].

Політичний розвиток США не раз доводив той факт, що культурний потенціал, полікультурна спадщина держави відігравали не менш важливу роль у формуванні статусу світового лідера, ніж інші складові глобального лідерства. Використовуючи позитивний досвід у сфері зовнішньої культурної політики Франції та Великої Британії, які започаткували ідеологію культурного колоніалізму та розробили культурний механізм тиску на інші держави,

США визначили культурну дипломатію ефективним засобом впливу на зовнішню та внутрішню політику інших держав. Сучасна зовнішня культурна політика США – це екстраполяція американських цінностей на культурне середовище інших країн, хоча на рівні міжкультурних відносин декларативно пропагуються демократичні принципи поваги до різноманіття, вільного вираження поглядів та переконань; збалансованого обміну культурними цінностями [477].

Основні засади американської зовнішньої культурної політики були розроблені на початку XX ст., коли адміністрація президента В. Вільсона почала впроваджувати нові принципи зовнішньої політики, зокрема, провідний принцип поширення американської присутності в країнах особливих політичних інтересів США. Цей принцип трансформувався у політику природного культурного імперіалізму, яку політолог З.Бжезинський характеризував пізніше як ідеологічну діяльність політичних інститутів Америки, визначальними рисами якої були авторитарне нав'язування культурних стандартів, культурна гегемонія та місіонерська ідея домінування масової американської культури [478].

Стратегію і тактику американської зовнішньої культурної політики на міжнародній арені до середини XX ст. визначали три політичні доктрини –доктрина ізоляціонізму (в Північній Америці та Західній Європі), "доктрина Монро" (в Латинській Америці), доктрина "*відкритих дверей*" (в Азії), які мали на меті забезпечити інтереси США в трьох важливих геополітичних регіонах світу [479].

Саме в Європі та країнах Азії культурні цінності Сполучених Штатів безпосередньо почали впливати на спосіб життя і цивілізаційний розвиток. Проте тиск культурної експансії США, зумовлений "швидким зростанням її могутності і поступовим руйнуванням міжнародної системи, в центрі якої була Європа", викликав протести навіть в англомовній Британії, де було створено спеціальний урядовий центр "противаги" діяльності Америки в культурному середовищі країни [480].

Це змусило США створити державні структури, до компетенції яких було віднесено реалізацію програм співробітництва з країнами західного світу в контексті забезпечення національних інтересів. Як зазначав К. Хейс, "*кордони Америки – це кордони європейської, чи західної культури, і ця культура, нехай модифікована чи пристосована до конкретних географічних і суспільних умов в Америці, чи деінде, завжди залишається з принципової точки зору західною культурою, і цим обумовлений постійний зв'язок культур та регіональна єдність народів з обох боків Атлантичного океану*" [481].

Друга світова війна стимулювала плюралізацію цілей американської зовнішньої політики, оновлення її доктрини, форм і методів забезпечення національних інтересів у всіх сферах міжнародного співробітництва. Зокрема, це стосується формування доктрини "Pax americana", тобто світу за амери-

канським зразком, глобальної американської моделі світового порядку, де американське панування було б беззаперечним. Так створився феномен "великої держави", за висловом З.Сардара та В.М.Девіс, яка потужно впливає на життєдіяльність світового співтовариства [482]. Культурна політика, яка була створена за американськими стандартами і пропагувала американський спосіб життя, перетворилася на стрункy і гнучку систему ідеологічного впливу інститутів США в різних регіонах світу. Це були перші активні спроби Державного Департаменту використати культурну дипломатію для американізації Західної Європи, подолання економічних, політичних і морально-психологічних бар'єрів проти американської економічної і політичної експансії, що, у свою чергу, призводило до порушення традиційних історичних і культурних зв'язків між європейськими країнами (у багатьох випадках на шкоду розвитку національних культур). Культурна складова "Плану Маршалла", який втілював ідею про атлантичну єдність з політичною монополією США, полягає у наступному: 1) роз'яснювати і представляти громадськості інших країн політику уряду Сполучених Штатів; 2) показувати "можливими способами взаємозалежність між політикою США і розумними прагненнями інших народів світу"; 3) викривати і протидіяти "ворожим спробам викривлення політики Сполучених Штатів", а також 4) визначати "ті найважливіші аспекти життя і культури спільноти Сполучених Штатів, які переконують у правильності політики і цілей уряду" [481].

Реалії біполярного світу та гостре ідеологічне протистояння під час "*холодної війни*" визначили пріоритетним інструментом американської зовнішньої політики задля поширення національних інтересів у пріоритетних країнах. Координаторами цих програм стали Інформаційна Агенція Сполучених Штатів (USIA) – головний центр пропаганди американських цінностей у світі (за межами США відома як Інформаційна служба Сполучених Штатів (U.S. Information Service, USIS), Програма освітніх обмінів Фулбрайта, яка згодом стала складовою Міжнародної програми освітніх обмінів (International Educational Exchange Program), головною метою якої, з позиції американського уряду, було визначено протистояння комуністичній пропаганді та залучення інтелектуальних ресурсів країн світу для розвитку американської гегемонії, Агентство з питань міжнародного розвитку Сполучених Штатів (U.S. Agency for International Development, USAID), яке також підтримувало програми культурних і освітніх обмінів та ініціювало освітню програму для регіону Карибів і Латинської Америки (Carribean and Latin American Scholarship Program, CLASP, 1985) з метою антирадянської пропаганди в регіоні тощо [480; 483].

Саме на Інформаційне агентство Сполучених Штатів (ЮСІА), яке було створене 1953 р. за ініціативою президента Д. Ейзенхауера як незалежне зовнішньополітичне інформаційно-пропагандистське відомство у системі виконавчої влади, була покладена місія поширення спрямованої інформації про США та просування привабливого образу американської політики, ідеології і культури, зокрема, через телерадіомережі "*Голос Америки*", "*Радіо Марті*",

"*Свобода*", "*Вільна Європа*", "*Вільна Азія*" та "*Уорлднет*", щоквартальник "*English Teaching Forum*", та реалізація програм міжкультурного співробітництва у 143 країнах світу. Діяльність ЮСІА розглядалася як один з основних інструментів інформаційно-пропагандистського забезпечення міжнародної діяльності держави щодо реалізації зовнішньополітичних інтересів та активного формування позитивного іміджу США за кордоном [484].

Завдання діяльності ЮСІА передбачали: 1) встановлення і розвиток контактів між США та іншими країнами на інституційному і неформальному рівнях задля міжнародного взаєморозуміння і стабільності, допомогу в демократизації та формуванні відкритого громадянського суспільства за зразком "американської демократії"; 2) політичний консалтинг для адміністрації президента і уряду США, членів Ради національної безпеки та інших високопосадовців з питань ефективного здійснення зовнішньої політики і динаміки світової громадської думки; 3) інформування владних структур про реакцію світової спільноти та політичних лідерів на зовнішньополітичні кроки США практично в усіх країнах світу; 4) сприяння партнерству американських організацій у міжнародній взаємодії; 5) роз'яснення політики Сполучених Штатів задля переконання в її легітимності у прийнятній для зарубіжної спільноти формі; 6) представлення політичного та культурного різноманіття американського суспільства шляхом поширення інформації про офіційну політику, національні цінності та інститути США, які впливають на здійснення такої політики та її розуміння у міжнародному середовищі; 7) обмін інформацією та здійснення освітньо-культурних програм для забезпечення національних інтересів [484-485].

Біля витоків ЮСІА стояв Комітет з питань публічної інформації (The Committee on Public Information), який в роки першої світової війни фактично започаткував ідеологічну інформаційно-роз'яснювальну роботу уряду Сполучених Штатів за кордоном. Після першої світової війни, коли було сформовано Міждепартаментний комітет наукового співробітництва як відповідь на ведення німецької та італійської пропаганди нацизму в країнах Латинської Америки, Сполучені Штати активізували культурні відносини з іншими американськими республіками, включаючи в реалізацію програм культурного та освітнього обміну пропагандистський компонент. В повоєнний період, коли Європа стала полем ідеологічної боротьби, Держдепартамент з питань зовнішньої політики сформулював основне завдання для ЮСІА – забезпечити позитивний імідж політики Сполучених Штатів з іншими націями. Як зазначав президент Дж. Картер, "*у наших інтересах – а також в інтересах інших націй – знати історію, культуру і проблеми одне одного, щоб зрозуміти надії, сприйняття світу та бажання його змінити*" [484].

Представництва ЮСІА у складі дипломатичних установ стали провідниками культурної та ідеологічної пропаганди американських цінностей. Вони формулювали політичну лінію щодо ключових міжнародних подій, роз'ясню-

вали політику Сполучених Штатів та діяльність посольства, забезпечуючи, зокрема, через відділи культури, прямі, незалежні та постійні контакти з політичними лідерами і громадськістю в країнах перебування, висвітлюючи проблеми американської зовнішньої політики для ЗМІК та закордонної спільноти, залучаючи зарубіжну аудиторію до програм ЮСІА. Серед них — різноманітні програми допомоги побудови демократичних інститутів у нових демократіях у всьому світі, які підтримуватимуть демократичні реформи, зокрема, в країнах Центральної та Східної Європи, Росії, нових незалежних державах колишнього СРСР. Наприклад, стажування новообраних парламентарів Боснії в США допомогло в успішному переході країни до демократичної і незалежної форми державного управління; в Африці спеціальний акцент було зроблено на програмах, пов'язаних з демократизацією влади, торгівлею та інвестиціями, більше того, відносини США з африканськими країнами перейшли від програм допомоги до реального партнерства. ЮСІА також фінансує програми розвитку національного права та права інтелектуальної власності (на культурну продукцію у Китаї, Бразилії та В'єтнамі). Останні програми культурної дипломатії ЮСІА стосуються роз'яснення глобальної політики США, включаючи розширення НАТО і його майбутню роль в європейському регіоні та у світі [485; 486].

Водночас представництва ЮСІА в країнах перебування здійснювали пошук, обробку і аналіз інформації для вдосконалення політики співробітництва урядових інститутів США, охоплюючи загальні проблеми міжнародного співробітництва та спеціалізовані напрями міжнародної взаємодії — погляди на політику Америки у сфері демократизації, лібералізації ринків, діяльності ЗМІК, щодо конфліктів, миротворчих процесів, тероризму тощо. Так, у 1997 р. Представництва ЮСІА підготували для Білого дому, Національної ради з безпеки, Держдепартаменту та дипломатичних установ США за кордоном 150 оглядів по 74 країнах, серед яких можна виокремити такі основні типи: персональні дос'є високопосадовців, які відповідають за здійснення ідеологічної роботи та гуманітарно-культурного співробітництва, аналітичні дослідження про ставлення до стратегічної і поточної практики міжкультурних зв'язків, прогностичні рекомендації та пропозиції щодо міжкультурної взаємодії на перспективу [478].

ЮСІА реалізують різноманітні програми, завданням яких є переконання внутрішньої і зарубіжної спільноти, впливових політичних лідерів та представників інтелектуальних і ділових кіл у правильності внутрішньої і зовнішньої культурної політики США щодо підтримки культурного різноманіття, уникнення конфліктів культурно-цивілізаційного характеру та впровадження ідеології культури миру в сучасних міжнародних відносинах на противагу звинуваченням в культурному імперіалізмі та експансії масової культури. Визначальну роль у просуванні культурної дипломатії відіграють тематичні електронні публікації ЮСІА (*Economic Perspectives, Global Issues, Issues of Democracy, U.S. Foreign Policy Agenda, U.S. Society and Values*), в яких подається докладний аналіз усього спектру життєдіяльності Сполучених Штатів.

Проблематика електронних видань охоплює дискусійні проблеми національної культурної політики, які стосуються усвідомлення американської ідентичності, релігійної свободи у багатокультурному американському середовищі та етики расової культури. Так, в основі тематичного електронного дослідження „Сполучені Штати в 2005 році: хто ми, як ми усвідомлюємо і розуміємо себе" – ідея перевірки і підтримки американських цінностей у світі, що трансформується, полеміка щодо єдності американської культури у поліетнічному та полірасовому суспільстві, яке динамічно розвивається і потребує зміни внутрішньої культурної політики. Дослідження „До єдиної Америки: загальнонаціональна дискусія щодо расових питань" визначає погляди, параметри та невирішені питання фундаментальних аспектів проблем рас, культурного різноманіття та міжрасового діалогу і примирення, оскільки швидкоплинна сучасна імміграція, яка впливає на етнічний склад населення США, спричинює нове усвідомлення американської культурної самобутності та американського громадянства, що виходить за етнічні межі. Дослідження „Свобода релігійної совісті як право людини" підкреслює свободу релігійних культур в США у порівнянні з розвитком релігійної культури в країнах світу [487;489].

Позиційними можна вважати тематичні електронні дослідження щодо реалій і перспектив зовнішньої політики у сфері міжкультурного співробітництва, які підкреслюють роль Америки в утвердженні демократичних ідеалів та розвитку глобальних цінностей, пропагують ідею „американського інтернаціоналізму" як політику заохочення свободи демократії та розвитку, аналізують практику і перспективи сучасної американської зовнішньої політики. В дослідженні „На шляху до співтовариства демократичних держав" обстоюється ідеологія демократії в контексті прав людини, міждержавного діалогу та формування нового світового порядку; в дослідженні „Формування зовнішньої політики США" розглядається проблема забезпечення національних інтересів у сфері міжкультурного співробітництва за допомогою засобів масової інформації, *„мозкових центрів"* і глобальної мережі [490; 491].

Після закінчення "холодної війни" у зовнішній політиці Сполучених Штатів превалювала концепція "жорсткої" гегемонії, яка призвела до відходу від концепції "війни ідей" та зменшення масштабів американської культурної присутності, що створило проблему заповнення глобального культурного простору ідеями, кардинально протилежними американським політичним інтересам. Як підкреслює Р.Т. Арндт, така ситуація була зумовлена відмовою від активної культурної дипломатії, руйнування якої відбулося непомітно, що залишило націю вочевидь беззахисною перед культурною агресією *"третього світу"* [492].

Функції ідеологічних структур США із закінченням "холодної війни" були передані Бюро з питань освіти та культури Держдепартаменту, до якого було інтегровано ЮСІА, що трансформувало систему державного контролю політики спрямованого міжкультурного співробітництва і стратегію офіційної американської культурної присутності за кордоном. Ця стратегія полягала у реалізації програм культурних заходів, які б сприяли взаєморозумінню між

народами США та інших країн, посилювали увагу до відкритості, свободи і демократичності американського суспільства та ролі культурного різноманіття у динамічних досягненнях Америки і водночас готовність до сприйняття самобутньої культури народів світу [486].

Програми, якими опікується Бюро з питань освіти та культури Держдепартаменту, повинні сприяти, за задумом організаторів, поглибленому взаєморозумінню американських та зарубіжних учасників, формуванню нового міжнародного партнерства, забезпечувати потреби політики міжкультурного співробітництва дипломатичних установ США в країнах перебування з метою представлення релігійного і культурного різноманіття, що впливає на демократизацію, економічний розвиток та розв'язання конфліктів на всіх рівнях взаємодії американського суспільства. Зокрема, культурна дипломатія помітно вплинула на позиції країн (Китай, Росія, Південна Африка тощо), з якими у США складалися напружені відносини. Культурні події стали символічними посередниками дипломатичних ініціатив [493].

Проблеми трансформації зовнішньої культурної політики та програм міжнародного співробітництва були в центрі дискусій першої представницької конференції "***Культура і дипломатія***" адміністрації США і Бюро з питань освіти та культури Держдепартаменту (2000 р.), в якій взяли участь Президент США Б.Клінтон, Держсекретар М.Олбрайт, члени Конгресу, представники американської адміністрації, міністри культури з усього світу, американські посли, керівництво приватних фондів, представники неурядових організацій і транснаціональних компаній, майже 200 відомих діячів культури і мистецтв Америки та світу. Головна мета – з'ясувати роль культурного чинника у зовнішній політиці США та спрогнозувати подальший розвиток американської культурної дипломатії. Серед основних проблем конференції, які мали практичне значення для реалізації зовнішньої політики США, підкреслення пріоритетності культури в сучасних дипломатичних відносинах; важливість захисту культурного розмаїття; підтримка культурної самобутності у країнах, які розвиваються; транспарентність культурного обміну; презентація досягнень полікультурності американського суспільства, потенціал Інтернету у здійсненні культурної дипломатії; поширення англомовних культурних ресурсів, заохочення до програм культурної дипломатії транснаціональних корпорацій та неурядових організацій. Як зазначав у своєму виступі президент Б. Клінтон, „культура – це головний елемент відносин між людьми, і культурна дипломатія здатна просувати взаєморозуміння між націями, знаходячи спільні культурні елементи, та формувати контекст для офіційних відносин". Функції американської культурної політики Б. Клінтон вбачає у тому, що багаті розвинені суспільства, які мають економічні та технологічні засоби, щоб просувати свої культурні інтереси у світі, повинні допомагати менш розвиненим суспільствам зберегти самобутнє культурне розмаїття та представити їхні культурні надбання на міжнародному рівні. Головною американською культурною цінністю він вважає демократію, що завжди присутня в культурних

контактах США с іншими країнами. Повага до дотримання універсальних прав людини пов'язана з повагою культурного розмаїття. За словами Клінтона, культурний обмін повинен бути „вулицею з двостороннім рухом". Б.Клінтон також вказав, що у контексті світової політики спостерігаються дві протилежні тенденції: з одного боку, збільшення кількості расових, етнічних, релігійних конфліктів на основі культурних розбіжностей, з іншого — проблеми впливу глобалізації на культурну самобутність та ідентичність. Він сподівається, що американська культура, збагачена іншими культурами світу, стане позитивною силою для міжнародних відносин, підтвердить спільні гуманні цінності, до яких належить і культурна дипломатія [494].

Зазначимо, що бюджетні витрати Держдепартаменту на зовнішню культурну політику в 2003-2004 рр. становили 600 млн. дол. США, 40% з яких було витрачено на освітні та культурні програми, що у порівнянні з фінансуванням інших напрямів зовнішньої політики уряду США становить 4% від коштів, призначених для діяльності Держдепартаменту у сфері міжнародних відносин і 1% від щорічного бюджету Пентагону. Іншим джерелом фінансування є інвестиції урядів інших країн та приватного сектору, зацікавлених у міжкультурному співробітництві. Наприклад, Програма Фулбрайта у 2001 р. отримала з бюджетів зарубіжних урядів близько 27,9 млн. дол., приватний сектор надав фінансову підтримку в розмірі 18,4 млн. дол., а внески американських університетів, які забезпечують виконання програми, становили понад 46,4 млн. дол. США [477; 493].

Саме на ефективність зовнішньої культурної та інформаційної політики, з огляду на динаміку глобалізації світових цивілізаційних процесів, які зумовили космополітизацію національних культур, уніфікацію культурних цінностей і стандартів, поширення стереотипів масової культури, покладають надії розробники зовнішньої політики США, вважаючи, що вона є складовою успішної глобальної стратегії держави з поширення американської моделі світового розвитку. Враховуючи, що цей інструмент зовнішньої політики США відзначався тісним історичним зв'язком з пропагандою та ідеологічним протиборством, характерними для періоду "холодної війни", і ототожнювався з політикою культурної експансії, трансформація культурної дипломатії США сприймалася в інших регіонах та країнах світу як продовження політики гегемонізму.

Політологи відзначали потужність світового лідерства Америки, яка спирається не тільки на значний військовий, а й економічний та культурний потенціал, що зумовило після розпаду біполярної політичної системи ідеологічне панування американського ідеалу ліберальної демократії у світі. Поєднання військового, економічного, політичного та інформаційно-ідейного потенціалу дає США можливість встановити систему тотального глобального впливу на світову спільноту. Тобто, месіанська ідея імперської всемогутності, яка передбачає готовність до жорстких дій, повинна знайти підтримку у громадськості Сполучених Штатів та змінити пріоритети і цінності американського суспільства. Однак відсутність масового поширення ідеології монопольного панування США

як глобального блага для світу потребує використання колосальних національних ресурсів для утвердження такої ідеї американізму [495-498].

Ця позиція Сполучених Штатів наражається на критику як всередині країни, так і серед зарубіжної спільноти. Так, політичні аналітики С. Хоффман та А. Лівен зазначають, що сьогоднішній варіант США пояснюється як вид радикального республіканства, тобто „бушизму", утопічно-імперського у зовнішній політиці та реакційного і антиліберального у внутрішній: „Настане той день, коли американці зрозуміють, що їхні цінності, якими вони так пишаються, несумісні з імперською практикою, яка підриває авторитет США на світовій арені, а всередині країни руйнує основи демократичних інститутів" [499-500].

Політика "бушизму" виявилася у пріоритетності жорстких підходів до забезпечення національних інтересів і значних перевагах у фінансуванні військового бюджету порівняно з іншими сферами міжнародного співробітництва.

Зовнішня культурна політика Держдепартаменту США за часів Дж. Буша переважно здійснювалася неурядовими організаціями і ТНК, які стали самостійними акторами міжнародних відносин, та за наглядової позиції Держдепартаменту США. Особливо це стосується діяльності ТНК, інформаційно-культурні продукти та послуги яких і політика міжнародної конкуренції набули характеристик культурної експансії та культурного імперіалізму як чинника зовнішньої політики Сполучених Штатів. Така тенденція викликала дискусії серед політичної еліти і фахівців з питань міжкультурного співробітництва, в рамках яких виявилися різні підходи до ролі приватного сектору у зовнішній політиці держави. З одного боку, підкреслювалося, що Держдепартамент повинен контролювати програми в рамках публічної і культурної дипломатії, оскільки державна політика традиційної дипломатії використовує культурний, освітній та інформаційний обмін в національних інтересах, а фінансовий та урядовий контроль за здійсненням зовнішньої культурної діяльності дасть змогу уникнути формування однобічного негативного іміджу Америки, який складається на основі американської теле- та радіопродукції, акцентуючи увагу на таких характеристиках, як примітивізм, вульгарність, сексуальне та кримінальне насильство. З іншого боку, прибічники роздержавлення культурної дипломатії і збільшення ролі приватного сектору США у міжнародних культурних обмінах вважають: держава контролює занадто велику кількість програм, що в добу глобалізації, розвитку Інтернету та глобального поширення американської масової культури і англомовних культурних продуктів і послуг є недоцільним [478; 501].

Однак, залишається неспростовним той факт, що міжнародна культурна діяльність США сьогодні здійснюється переважно приватним сектором, а американська масова культура є однією з найпотужніших чинників впливу на світову спільноту. В такій ситуації Бюро з питань освіти та культури Держдепартаменту США виступає лише як координуюча структура, яка узгоджує принципи партнерства між приватним і громадським секторами держави і

відіграє важливу роль у налагодженні культурних зв'язків в самій країні та за її кордонами. Загалом нараховується близько 1500 організацій, що представляють приватний сектор, академічні інститути та неурядові організації, які керують більшістю наукових, освітніх та культурних обмінів і формують сприйняття Америки через індустрію масової культури [477].

Упродовж другої половини XX ст. тенденція концентрації власності у межах кількох транснаціональних корпорацій привела до переваг приватного сектору в реалізації зовнішньої культурної політики. Більш того, культурна індустрія стала частиною широкої системи взаємопов'язаних структур, які, наприклад, у США, включають урядові інституції (Федеральну комісію з комунікацій, Федеральну комісію з торгівлі); групи промислового лобіювання (Американську асоціацію газетних видавців, Національну асоціацію мовлення, Асоціацію американських кіновиробників і дистриб'юторів, Асоціацію журнальних видавництв); постачальників національної та міжнародної інформації, зокрема, телеграфні компанії; компанії та синдикати з виробництва телевізійних програм, представників музичної індустрії, власників радіо-телевізійних та кабельних мереж; рекламних компаній, незалежних видавництв, супутникових систем; дистриб'юторів аудіовізуальної продукції, виробників комп'ютерної техніки та програмного забезпечення, провайдерів Інтернет-послуг, регіональних телефонних компаній тощо. Усі ці інституції безпосередньо зацікавлені у підтримці політичного, економічного та культурного домінування США у світі через культурну експансію і забезпечення комерційних інтересів [502].

У поєднанні з високоефективною промисловою, військовою, транспортною і технологічною присутністю США у глобальному міжнародному середовищі така система взаємопов'язаних структур створює і підтримує сприятливі умови для агресивного просування американських національних інтересів, є важливим інструментом культурного імперіалізму. Використовуючи сучасні комунікаційні технології для ведення бізнесу та захисту власних економічних пріоритетів і культурних цінностей у глобальному масштабі, Сполучені Штати стали єдиною світовою державою, яка домінує в міжнародних інформаційних потоках і впливає як на світову, так і зовнішню політику. Такий культурний імперіалізм є, на думку Г. Шіллера, невід'ємним наслідком політичних, військових та індустріальних амбіцій Сполучених Штатів, оскільки американські образи, продукти та послуги "заполонили світ, поширюючи вірус споживацького ставлення до культурних надбань". Мас-медіа та численні продукти і послуги, які вони рекламують, забезпечують панування культурної експансії США. Найбільш вразливими в цьому процесі виявилися країни, які розвиваються, і в яких через ЗМІК насаджуються чужі культурні цінності, спосіб мислення та мотивація поведінки [501].

За даними Британської асоціації телевізійних дистриб'юторів США у 2001 р. контролювали 60% глобального ринку телевізійного експорту, що оцінюється у 4 млрд. дол.; Голівуд монополізував глобальний кіноринок (вісім найбільших кіностудій Голівуду виробляють 85% кінопродукції) та контролює

90% ринку Європи; майже 93% повнометражних фільмів на британському телебаченні у 2001 р. повністю належали США або були створені спільно [503]. Прибуток від американського культурного експорту конкурує з виробництвом літаків (наприклад, надходження від продажу за кодоном кінофільмів, знятих лише у Голівуді, становить понад 60% річного прибутку галузі) [504].

Таб. 3.1

Рейтинги найбільш касових фільмів за всю історію кінопрокату

Місце у рейтингу	Назва фільмів	Рік	Країна-виробник	Валовий прибуток (млн.дол.)
1	"Титанік"	1997	США	1235
2	"Володар перснів: повернення короля"	2003	США	696
3	"Гаррі Поттер і потаємна кімната"	2001	США	651
4	"Гаррі Поттер і філософський камінь"	2002	США	604
5	"Володар перснів: дві башти"	2002	США	581
6	"Парк Юрського періоду"	1993	США	563
7	"Володар перснів: Братство кільця"	2001	США	547
8	"У пошуках Немо"	2003	США	513
9	"День незалежності"	1996	США	505
10	"Зоряні війни. Епізод І: Прихована загроза"	1999	США	491
44	"Віднесені привидами"	2001	Японія	254
86	"Чотири весілля і похорон"	1994	Велика Британія	191
96	"Щоденник Бріджет Джонс"	2001	Велика Британія	183

У країнах, які розвиваються, місцева культурна індустрія перебуває в критичному стані через монополію масової культури США. Така політика ТНК, материнські компанії яких розміщені переважно на території США, призводить до системних негативних культурних наслідків у світовому масштабі. Це стало причиною радикальних заходів з боку Канади та країн ЄС, які забезпечують доктрину внутрішньої культурної політики шляхом протекціонізму, державних субсидій та квотування імпорту/експорту культурної продукції [502].

У перспективі торговельної політики США культурний сектор економіки розглядається як потенційно прибутковий вид комерційної діяльності. Водночас, превентивні заходи інших акторів міжнародних відносин, спрямовані на пропаганду і захист національної культури, негативно сприймаються у США і розглядаються як порушення принципів вільної торгівлі. Така позиція враховує як можливі комерційні втрати для економічних інтересів США, так і використовується для впливу на країни, які застосовують подібні обмеження для доступу продукції США на внутрішні ринки. Як зазначає американський

політолог У.С. Меркін, "скільки б США не говорили про повагу до принципів культурної ідентичності національних спільнот зарубіжних країн, комерційні інтереси та культурний імперіалізм переважають задекларовані принципи політики міжкультурного співробітництва. Більш того, така політика майже нездатна на компроміси" [504].

Найбільш гостру дискусію політика культурного імперіалізму США викликала в міжнародних економічних організаціях, зокрема, в Організації економічного співробітництва та розвитку (в рамках обговорення Багатосторонньої угоди про інвестиції) та Світовій організації торгівлі (в рамках обговорення Генеральної угоди з тарифів і торгівлі). Предметом дискусії стали різні підходи до визначення сутності культурної продукції. З одного боку, культурна продукція розглядається як комерційна продукція і тому повністю регулюється правилами міжнародної торгівлі. З іншого боку, вона розглядається як інтелектуальне надбання нації, що відображає культурну ідентичність та культурне різноманіття певного співтовариства, тому вона повинна бути виключена зі сфери дій міжнародних угод з торгівлі [504; 505].

Позицію "вилучення культури" з торгівельних угод про інвестиції і розвиток міжнародної торгівлі підтримали Канада, Франція і більшість латиноамериканських та африканських країн, які виступили за прийняття спеціального міжнародного документу, що надав би урядам право захищати національну культуру в умовах конкуренції та вільного ринку, застосовуючи політику прямого протекціонізму. Така політика американської культурної індустрії змушує інші держави виробляти відповідні механізми захисту національної культури та мови і вдаватися до політики квотування на ввезення культурної продукції для підтримки національної кіноіндустрії та розвитку національного телерадіомовлення [504].

Проти такої позиції виступили країни – головні лідери-експортери культурної продукції, зокрема, США, Бразилія, Мексика, Японія, Індія та деякі країни, які розвиваються, і які не в змозі задовольнити внутрішній попит національною культурною продукцією і для яких необмежений доступ до маскультури є комерційно вигідним, незважаючи на проблему культурної експансії. Позиція США полягає у тому, що повне вилучення культурної продукції з міжнародних торговельних угод може призвести до необґрунтованого обмеження культурного обміну з винятково комерційною або ідеологічною метою [504].

Події 11 вересня 2001 р. і початок широкої антитерористичної кампанії як складової політики „бушизму" негативно вплинули на просування американських цінностей у світі. Здійснені Zogby International, Pew Research Center та Gallup (CNN/USA Today) дослідження громадської думки демонструють зменшення позитиву у сприйнятті американської зовнішньої політики та її складової – культурної дипломатії. Так, громадська думка в Єгипті, Марокко та Саудівський Аравії визначає США як значно більшу загрозу світовому порядку, ніж терористичні рухи та угруповання. Більш позитивно оцінюють

зовнішню політику США в Туреччині, Пакистані, Йорданії та країнах Південно-Східної Азії, але і в цих країнах з 2002 р. по 2004 р. спостерігається критичне ставлення до діяльності адміністрації Дж. Буша. Навіть у традиційних країнах-союзниках США по НАТО, а також Австралії, Японії, Південній Кореї, Мексиці, Ізраїлі та Росії негативно оцінюють діяльність адміністрації Дж. Буша і тенденційну пропаганду політики антитероризму [506]. Враховуючи неоднозначне ставлення до стратегії зовнішньої політики держави, Сполучені Штати після подій 11 вересня 2001 р. витратили на культурну дипломатію в мусульманських країнах 150 млн. дол.; загальні витрати Держдепартаменту США в цій сфері складали понад 1 млрд. дол., проте воєнні витрати перевищували витрати на культурну дипломатію у 450 разів [493].

Стало зрозуміло, що культурний імперіалізм ТНК не гарантує забезпечення американських національних інтересів у сфері міжнародного співробітництва, а пасивна роль урядових структур виявила проблему неефективності культурної складової зовнішньої політики держави.

Попри економічний тиск та демонстрацію військової сили, перед урядом США постала проблема активізації зовнішньої культурної діяльності, повернення довіри до американської політики як ідеології глобальної демократії. Першочерговим завданням зовнішньої культурної політики США було визнано нейтралізацію негативного сприйняття американських ідей та цінностей у світі. Здійснені дослідження громадської думки показали, що 80% населення, зокрема, мусульманських країн, які висловлювали своє незадоволення американською політикою, виявили зацікавленість у запозиченні американського досвіду демократизації суспільства та поширенні здобутків західної культури, науки і технологій [507].

Так, за ініціативою Ради з питань телерадіомовлення та Конгресу США, Радіо "*Sawa*" ("разом" – арабською) транслювало передачі арабською мовою та місцевими діалектами на території Середнього Сходу, в тому числі в Іраку, а також музичну продукцію арабського і західного походження, новини спорту тощо [508]. Телеканал "Al-Hurra" ("вільний" – арабською), метою заснування якого, за словами Дж. Буша, є протиставлення "ворожій пропаганді, що заповнює медійний простір ісламського світу" і прагнення "донести правду про цінності і політику Сполучених Штатів", здійснює мовлення арабською мовою і фарсі на аудиторію ісламських країн [509].

У 2004 р. Держдепартамент США збільшив фінансування програм культурних, академічних та професійних обмінів, виділивши на їх реалізацію 316,633,000 дол. У рамках програми School Internet Connectivity Program до США прибуло 26 тис. студентів для навчання у школах та коледжах з країн Середнього Сходу, Південної Азії, Південно-Східної Європи, Центральної Азії та Кавказу. За програмою American corner у 2003 р. було відкрито понад 100 американських культурно-освітніх ресурсних центрів у різних країнах світу, у 2004 р. відкрито ще 194 у 64 країнах, з яких 58 – у країнах Середнього Сходу та Південної Азії, у тому числі 10 – в Афганістані і 15 – в Іраці.

Фінансування Програми вивчення англійської мови у цей період становило $1 573 000 у 2004 р. [477].

Однак, існуючі інструменти формування світової громадської думки, які використовують сьогодні США, проявили себе не достатньо ефективно і створили протилежний ефект в ісламських країнах. Серед ісламських політичних лідерів зростає скептицизм щодо прихованих намірів культурної політики США, а ісламські ЗМІ, незважаючи на комерційну прибутковість, відмовилися демонструвати передачі, створені за сприяння Держдепартаменту про життя мусульман у США.

Тому більшість представників дипкорпусу вважають, що необхідно активізувати саме культурну дипломатію задля позитивних змін у ставленні до США, покращення образу країни та розуміння базових цінностей американської нації. Але така дипломатія повинна здійснюватися упродовж тривалого часу, більш глибоко та грунтовно, щоб досягти позитивного ефекту та потужного впливу [510].

Геополітичні стратегії двох політичних сил країни – "*жорсткої*" гегемонії (Республіканська партія) та "*м'якого впливу*" (Демократична партія), спрямовані на однаковий політичний результат – домінування американських цінностей і американського способу життя в світі. Стратегія "жорсткої" гегемонії виражає ідею американської обраності та месіанства і передбачає здійснення політики необмеженого глобального лідерства. Стратегія "м'якої" гегемонії враховує у політиці міжкультурного співробітництва статус глобального лідера США та практику створення наднаціональних механізмів врегулювання світових процесів задля реалізації месіанських ідей культурного американізму, проте здійснення такої політики спирається на політику, культуру та ідеали за американським зразком і досягається через "Soft Power" ("*м'яку владу*"), тобто через заохочення політичної еліти і світової громадськості до сприйняття „привабливих" демократичних та культурних цінностей США. Проте обидві стратегії сприяють утвердженню монопольних позицій США у світі і доповнюються факторами союзницької та економічної допомоги США, на яку розраховують окремі держави – регіональні лідери, що належать до різних культур, мають різні геополітичні інтереси у конкуренції за лідерство на регіональному рівні і проблеми у виробленні спільних позицій і дій у міжнародних відносинах.

4.4. Брендінгові стратегії міжнародних організацій в контексті інформаційної безпеки

Процеси глобалізації посилили необхідність того, що не лише товари прагнуть виділитися поміж конкурентами. Необхідність грамотно позиціонувати себе в міжнародних відносинах усвідомлюють країни, уряди та міжна-

родні організації. Своєрідними орієнтирами в умовах глобальної конкуренції виступають саме бренди товарів, послуг, осіб, фірм, організацій, країн та їх об'єднань. «У технократичні та бліді часи бренди приносять тепло, обізнаність та довіру, вважає — голова ради директорів компанії Nestle» [511]. Асоціації, які викликає та чи інша назва, логотип, лозунг тощо і, відповідно, об'єкт, позначуваний цими елементами, є дуже важливими, оскільки вони відносяться до емоційної сфери і формують емоційне, а не раціональне сприйняття об'єкта, причому таке сприйняття є дуже стійким.

Сучасний стан та перспективи брендінгової політики ЄС. Нещодавні заворушення у Франції та провали референдумів щодо європейської конституції в декількох країнах навели багатьох на думку про кризу, що назріває в Євросоюзі. Економічну й політичну складові цієї можливої кризи досліджують відповідні спеціалісти; ми ж можемо стверджувати про наявність деякого кризового стану в інформаційно-комунікативній сфері. Він визнаний також і самим Євросоюзом, а саме Єврокомісією в нещодавно опублікованому стратегічному документі «*Біла книга з європейської комунікативної політики*» [512]. Ця криза полягає в тому, що європейське населення надто мало знає про ЄС, його цілі, політику, недостатньо усвідомлює себе саме європейським, а не населенням певної національної країни, недостатньо залучене в процес прийняття політичних рішень на європейському рівні. В документі, зокрема, наголошується на необхідності постійного вивчення громадської думки, активізації різноманітних форумів, конференцій з метою залучення населення до здійснення політики, а також роботи зі ЗМІ з метою збільшення питомої ваги загальноєвропейської інформації в порівнянні з національними питаннями.

У серйозності намірів Єврокомісії переконує також те, що вона залучила до ребрендування ЄС Саймона Анхольта, одного з найбільш впливових спеціалістів з брендінгу в світі [513]. Раніше він працював з компаніями Microsoft, Unilever та Coca Cola, а також консультував уряди Британії, Німеччини та Словенії щодо їхньої брендінгової стратегії. Зараз він продовжує займатися проблемами державного брендінгу і регулярно складає рейтинг брендів країн світу. Стосовно своїй співпраці з ЄС Анхольт каже, що розглядає це завдання як найбільший виклик після Нігерії та США. Складність завдання, на думку Рольфа Анненберга, комісара ЄС з комунікації, полягає в тому, що «ЄС має свій бренд, однак він конкурує з 25 національними брендами».

Інший спеціаліст з брендінгу зі світовим ім'ям Оллі Уоллінс, який займався ребрендуванням Португалії, вважає, що основана проблема бренду ЄС — не любов, або ж нелюбов до нього, а байдужість. Подолати таке ставлення, точніше, відсутність ставлення, можна, на його думку, за допомогою брендінгу, оскільки бренд передбачає емоційне ставлення до нього, а саме цього ЄС бракує. Стосовно інформаційного наповнення бренду експерт за-

значив, що «люди ставляться позитивно до місцевих асоціацій, села, міста. ЄС не повинен заміняти цього, він повинен існувати поруч. Перш за все слід визначити, чим є ЄС, а потім можна вирішувати, як його брендувати» [511].

У необхідності оновлення й активізації європейської комунікативної політики переконані й інші дослідники. Пітер Ван Хам, заступник голови відділу наукових досліджень Нідерландського інституту міжнародних відносин, м. Гаага, та професор Коледжу Європи, м. Брюгге, Бельгія, а також член Дорадчого комітету з міжнародних питань голландського уряду, пише в своїй статті «*I "heart" Europe*», опублікованій в журналі Foreign Policy [514]: «ЄС більше не може покладати завдання «продажу» себе на країни – члени. Він має сам докласти зусиль до подолання емоційних бар'єрів, що все ще існують між ним та його населенням».

В іншій своїй статті Branding European power [515] голландський дослідник розвиває своє бачення європейської брендінгової політики. Він акцентує увагу на силовому аспекті, а саме на пасивності європейської зовнішньої політики та політики безпеки, а незначні успіхи, стверджує автор, недостатньо «розкручені» і не усвідомлені громадськістю. Найбільшою загрозою для Європи у військовій сфері, як і в економічній, є недостатня упевненість в собі, що призводить до скромного іміджу ЄС на світовій арені.

Серед успіхів ЄС, на яких варто сконцентруватися при його просуванні, Ван Хам називає стиль європейської політики – не якість, не напрямки, а саме *стиль* як сукупність правової, громадянсько-суспільної та комерційної систем забезпечення реальної політики. Саме це на думку дослідника має стати unique selling point – унікальною торговою пропозицією.

Європі потрібно віднайти своє нове «я», сформулювати новий смисл існування – *raison d'etre*. На сьогоднішній день вже не діє міф, яким озвучувалося створення першого прообразу ЄС після Другої світової війни («європейська інтеграція принесе мир»), оскільки зараз імовірність війни між Францією та Німеччиною, як і між будь-якими іншими країнами – членами ЄС, *видається смішною*. Цікавим є те, що бачення ЄС населенням країн, що не входять до його складу, суттєво відрізняється від сприйняття Союзу його мешканцями. Так, якщо перші асоціюють ЄС в першу чергу з економічним добробутом і процвітанням, то для других така орієнтація бренду «не спрацює». Для них найбільш важливою є відповідність їх цінностям, відміна смертної кари чи заборона доступу на ринок генетично модифікованих продуктів.

Однак брендінг – це не стільки знання про об'єкт, скільки любов до нього. Один із співробітників агентства Saatchi & Saatchi Кевін Робертс винайшов термін «lovemark» – марка, яку люблять, улюблена марка; похідне від trademark – торговельна марка. Робертс називає три складові «lovemark»: таємниця, чуттєвість та приватність.

Отже, ЄС має перетворитися на таку «lovemark». Очевидно, це потребуватиме значних зусиль та тривалого часу. Однак, як викладено вище, Європа має потенціал для досягнення мети – економічний, політичний, соціаль-

ний. У проекті Конституції ЄС вказується глобальне завдання об'єднання: сприяти миру, безпеці, стабільному розвитку та захисту прав людини в світі. Внутрішньо-європейська політика сьогодні більше нагадує внутрішню політику держави, де панує порядок та солідарність, аніж класичну міжнародну політику із характерними для неї анархічністю та недовірою. «Європейською мрією» (за аналогією з американською) може стати «удомашнення» світової політики.

Бренд ЄС на сьогоднішній день є дзеркальним відображенням іміджів країн – членів, однак потрібен новий систематизований підхід, метою якого було б створення якісно нового бренду ЄС не як простої суми брендів окремих країн. Водночас оптимальним інформаційним наповненням бренду є культурна різноманітність і неоднорідність Євросоюзу. Так, після початку переговорів з Туреччиною про вступ, ЄС міг би претендувати на роль політичного, культурного та, навіть, релігійного містка між Християнством, Юдаїзмом та Ісламом, а унікальні історичні умови (демонстрація обмеженості дієздатності ООН щодо врегулювання конфліктів та гарантування безпеки в поєднанні зі зниженням авторитету США у зв'язку з їх агресивною зовнішньою політикою на Сході) створюють додаткові можливості для формування бренду ЄС як альянсу демократій. При цьому акцент має робитися не на мультилатералізмі як такому, а на унікальному досвіді європейських країн, які спромоглися здійснити перехід від відвертого протистояння до взаєморозуміння, консолідації та об'єднання і тепер виступають на світовій арені в якості єдиного актора. Закріплення образу сили, що несе добро, призведе до підвищення самооцінки європейців та зростання довіри та поваги до ЄС за кордоном.

Для успішної реалізації програми ребрендування Європи, на думку Ван Хама, слід створити робочу групу, до складу якої увійшли б теоретики і практики. Вони мають розробити брендінгову стратегію ЄС. Потрібно провести фокус-групи та референдуми для визначення сподівань внутрішньої та зовнішньої громадськості; переглянути й активізувати діяльність публічної дипломатії для покращення зовнішнього іміджу ЄС і завоювання довіри в країнах, що розвиваються.

З тим, що європейці мають занижену самооцінку, погоджуються і інші дослідники, зокрема, автори статті «Europe, Inc.» (журнал Business Management) Люсі Уайт, Марк Пурді та Ліз Педмоур, співробітники консалтингового агентства Accenture [516], однак такий погляд на власну історію та сучасні досягнення не є на їх думку виправданим. У своїй статті експерти звертають увагу на економічну складову бренду ЄС і доводять великий потенціал Союзу. Європейські комерційні та урядові структури є світовими лідерами в суспільній та природоохоронній, а також в деяких комерційних сферах. Європа має деякі надзвичайно успішні глобальні компанії: наприклад, Royal Dutch/Shell та BP займають відповідно четверте та п'яте місце в рейтингу найбільших компаній світу, датська компанія Royal Ahold, що займається

торгівлею харчовими продуктами, є другою в світі в своїй галузі, а три з чотирьох найбільших в світі комерційних банків – європейські. При цьому в багатьох випадках громадськість не усвідомлює, що має справу з європейськими компаніями – лідерами своєї галузі. Наприклад, Vodafone – це не лише лідер бездротового зв'язку в тих країнах, на ринках яких ця компанія працює; вона також володіє 45% акцій найбільшого американського оператора мобільного зв'язку Verizon Wireless.

Однак, не лише комерційні компанії є прикладами економічних успіхів Європи. Північноєвропейські країни відомі тим, наскільки успішно вони поєднують високий рівень соціального та екологічного захисту із стабільним економічним зростанням. Згідно з оцінками World Economic Forum, *Фінляндія та Швеція займають відповідно перше та третє місце за конкурентоспроможністю* та потенціалом до зростання, а також друге та сьоме відповідно за показником інноваційності економіки.

Заслуговує на увагу також Франція, яка, маючи надзвичайно високий рівень продуктивності праці, встановила 35-годинний робочий тиждень, а також деякі центрально- та східноєвропейські країни – нові члени ЄС. Вони пережили надзвичайно бурхливий розвиток в останнє десятиліття і за деякими показниками навіть випередили розвинуті західноєвропейські країни. Наприклад, Естонія займає лідируючу позицію щодо впровадження електронного врядування, зокрема, проводяться віртуальні наради кабінету міністрів, впроваджується безпаперовий документообіг та в найближчі 5 років планується перейти на систему електронного голосування на виборах.

Попри ці очевидні досягнення, Європа все ще не повністю усвідомлює свій потенціал, і, в першу чергу, це проявляється у невикористаних можливостях спільного ринку та сприятливих умов для інновацій та підприємництва. Саме з цими двома аспектами пов'язують найбільш оптимістичні перспективи розвитку Європейського Союзу. Так, подальша інтеграція європейського ринку матиме значні позитивні наслідки: розширення товарної пропозиції для споживачів, сприяння конкуренції та ін. Згідно з оцінками агентства Accenture, об'єднання європейських фондових ринків гуртової торгівлі створить прибуток у 130 млрд. євро (1,1% ВВП ЄС) протягом наступних 10 років. Також інтеграція ринків сприятиме налагодженню транс-секторальних партнерств в різних галузях промисловості завдяки полегшенню обігу капіталу та пересування робочої сили.

Що ж стосується інновацій та підприємництва, то в цій сфері ЄС має значні потенційні переваги завдяки високому рівню розвитку систем освіти. Так, ЄС має більшу, ніж США, кількість науковців із ступенем PhD в сфері науки та технологій, однак на європейських підприємствах працює менша кількість таких спеціалістів, ніж в США. Подальше інвестування в цю сферу є шляхом до оновлення європейської економіки. Так, за даними 2003 року три країни з найбільш конкурентоспроможною економікою в світі були серед найбільших інвесторів в сферу наукових досліджень.

Ці два аспекти (спільний ринок та інноваційність), доповнюючись ще однією характеристикою — різноманітністю — є найбільш визначальними та найбільш цінними характеристиками для Європи; це її унікальні переваги. Дослідження громадської думки свідчать про те, що європейці не усвідомлюють цього: відповідаючи на запитання агентства Accenture, 80% американських управлінців погодились з тим, що їх країна є найбільш підприємницькою, і лише 3% європейців висловили аналогічну думку щодо своєї країни. На мою особисту думку, це пояснюється тим, що кожен з європейців усвідомлює себе, в першу чергу, як громадянин тієї чи іншої країни і, відповідаючи на запитання, керується уявленнями про свою країну. Формування у мешканців Євросоюзу бачення себе в першу чергу як європейців значно підвищило б їх самооцінку.

Отже, найбільшою проблемою залишається на сьогодні відсутність поінформованості населення ЄС про його сутність, цілі, політику і, відповідно, відсутність самоідентифікації мешканців як європейців. Для створення справді європейського бренду потрібен перехід на якісно новий рівень всіх сфер суспільного життя: йдеться про подальшу інтеграцію країн — членів. Без широкомасштабного реформування не вдасться досягти необхідних результатів. Не варто недооцінювати і роль масової комунікації. Люди повинні знати про всі переваги європейського об'єднання — економічні, політичні, культурні. Необхідним є збільшення в інформаційних потоках удільної ваги «європейських» повідомлень в порівнянні з «національними». Люди повинні почати цікавитися загальноєвропейськими проблемами і питаннями, а не лише своїми внутрішньодержавними. Цілеспрямована інформаційна кампанія в поєднанні з усестороннім розвитком ЄС призведе до зміни ставлення до нього як всередині, так і в інших країнах.

Говорячи про конкретні кроки на шляху до ребрендування Європи, автори називають такі.

По-перше, необхідно визначити переваги спільного ринку та почати активно інформувати про них громадськість. Необхідно акцентувати увагу на майбутніх вигодах, а не на можливих поразках. Переваги спільного ринку вже усвідомили бізнесмени; необхідно досягти аналогічного усвідомлення їх широкою громадськістю. Слід поширювати приклади корпорацій, успіхи яких пов'язані в першу чергу із інтеграцією європейського ринку. Іншим напрямом роботи має стати робота з університетами: введення нових спеціальних курсів, проведення семінарів, круглих столів тощо, заохочення наукової роботи студентів в цьому напрямку.

По-друге, слід попрацювати над новим баченням ЄС. Після Другої світової війни його прообраз створювався з метою гарантування миру. Сьогодні це вже не є актуальним. Слід віднайти нову ключову ідею, новий салоган ЄС. Це може бути щось на зразок «прогрес через солідарність», «сила в різноманітності», «можливості для всіх», «процвітання і безпека» тощо. Що б це не було, гасло повинно бути таким, щоб легко запам'ятовувалося, коротким, але змістовним.

По-третє, необхідно долучити всіх і кожного в Європі до спільної роботи, метою якої є процвітання Союзу.

Брендінгова політика НАТО. НАТО була створена в 1948 році як противага соціалістичному таборові, що почав формуватися в Центральній та Східній Європі після закінчення Другої світової війни. В 1956 році було створено Організацію Варшавського договору (ОВД) як східноєвропейський аналог НАТО, і ці два військові блоки майже на півстоліття стали найбільш наочним прикладом і втіленням протистояння між Сходом і Заходом. Інтенсивність цього протистояння могла змінюватися, однак питання про ціль кожного з блоків та його місце в світовому політичному порядку не виникало.

В кінці 80-х – на початку 90-х років система почала руйнуватися. Припинила своє існування ОВД, розпався СРСР, постсоціалістичні країни стали на капіталістичний шлях розвитку. В цих умовах НАТО втратила сенс свого існування в її первинному розумінні. З цього часу почався період пошуку нової ідентичності НАТО. На сьогодні вона зупинилася на боротьбі з міжнародним тероризмом, однак надто агресивна політика НАТО в Югославії та США, з якими, в першу чергу, асоціюється НАТО, в Афганістані та Іраку викликала погіршення іміджу організації.

Про необхідність перегляду місії організації та її цінностей говориться в рекомендаційному документі щодо стратегії ребрендування НАТО, запропонованому агентством SpinMute, підрозділом Mute Media Group Ltd, які є філією BigCorp Worldwide [517]. Компанія провела серію досліджень, результати яких представила у вищезгаданому документі. Так, опитування представників цільової аудиторії НАТО (в якості таких були визначені особи, що мають прибуток вище середнього, мешкають в Західній Європі і є європейцями за походженням) визначили в якості первинних цінностей бренду НАТО «війну», «бомбардування», «імперіалізм» та «страх». Така ситуація є неприпустима, оскільки ці характеристики не можуть розглядатися як позитивні або як перевага. Далі згадується американська марка одягу TheWest, цільова аудиторія якої дуже близька до аудиторії НАТО і яка отримала дуже позитивну оцінку в рамках того самого дослідження. У зв'язку з цим висловлюється припущення про можливі позитивні наслідки спільних маркетингових дій НАТО та цієї марки одягу, зокрема, що стосується використання стилю The West для просування заходів НАТО.

В якості можливої перспективи розвитку бренду НАТО називається розтягування бренду. Напрямками такого розтягування може стати: надання соціальних послуг, робота з людьми, що мають обмежену дієздатність, легкі розважальні послуги або навіть своя лінія одягу. Найбільших змін у сприйнятті бренду слід прагнути досягти в молодіжному сегменті та сегменті працюючих жінок. Так, можливим заходом в цьому напрямку може стати проведення марафону НАТО, прибутки від якого будуть використані для надання допомоги жертвам конфліктів, з одночасним запуском лінії сувенірних курток, кепок та сумок. Позитивно буде сприйнята ініціатива віддання пев-

ного відсотку прибутку від продажу цих речей неполітичним благодійним організаціям.

Однак, таке розтягування бренду лише частково покращить ситуацію. Необхідна масштабна робота з визначення корпоративної ідентичності та презентації. Є навіть пропозиції змінити назву організації та/або логотип, причому рекомендується використати в новому логотипі об'єкти, що базуються на більш жіночних, м'яких лініях.

Рекомендується також звернути увагу на особливості мови та якість графіки при висвітленні діяльності НАТО. Зокрема, можна використовувати більш нейтральні слова для військових термінів. Варто слідувати загальному образу доброго садівника, що сіє насіння добра і взаєморозуміння.

У дослідженні робиться висновок, що за умови приділення достатньої уваги питанню необхідності ребрендування та перегляду самоідентифікації та достатнього фінансування НАТО має реальні шанси зберегти та покращити свої позиції в світі.

Отже, основним фактором, що визначає негативне ставлення до НАТО в світі, є в першу чергу асоціювання цієї організації з наймогутнішим її членом – США і переконання в тому, що через свою діяльність в НАТО Штати займаються відстоюванням своїх власних інтересів в Європі та інших регіонах. Подолання такого упередженого ставлення можливе лише через продуману, добре скоординовану, централізовану інформаційно-просвітницьку кампанію, при чому надзвичайно важливим є урахування регіонального аспекту при плануванні кампанії: сприйняття організації населенням різних країн різниться залежно від багатьох критеріїв: власне належність – неналежність до організації; історичний досвід спілкування/співпраці/конфліктів з НАТО; позиція, яку займала країна під час «*холодної війни*»; пануючі в державі релігійні та культурні традиції тощо.

Для прикладу можна проаналізувати бачення НАТО мусульманським світом (за статтею Мустафи Алані, старшого радника і директора Програми дослідження питань безпеки і тероризму дубайського Дослідницького центру Перської затоки, опублікованої у зимовому випуску «Віснику НАТО» в 2005 році) [518]. Дослідник констатує негативність образу НАТО на Близькому Сході і називає деякі причини такого ставлення. Арабська громадськість не відділяє НАТО від західних та інших держав, які утворили цю організацію і входять до її складу. Таким чином, імідж НАТО було сформовано ставленням арабського світу до подій, в яких брали участь основні члени НАТО. До них відноситься колоніальне правління Франції і, зокрема, алжирська війна; причетність Італії до подій в арабській Північній Африці; окупація Великою Британією країн Перської затоки, її вплив і контроль в цьому регіоні; підтримка Ізраїлю Сполученими Штатами, яка видається необмеженою і непохитною. Більш того, пряма чи опосередкована підтримка НАТО сприймається сьогодні як одна з причин швидкої перемоги Ізраїлю і приниження арабів у війні 1967 року. Що ж стосується холодної війни, то більшість арабських національних

політичних рухів симпатизували радянському блоку і ОВД (і підтримувалися ними). Отже, причиною негативного образу НАТО на Близькому Сході є історичні передумови.

Дещо інша ситуація склалася в Україні, де необізнаність громадян щодо організації і її діяльності спричиняє недовіру і неприйняття [519]. В статті, опублікованій в газеті «Дзеркало тижня», автор пише про замовчування з боку найвищих посадових осіб країни, яким супроводжується євроатлантична інтеграція України. Як наслідок, населення не має повноцінної зваженої інформації про НАТО, оскільки в інформаційному полі країни переважають повідомлення на цю тему анти-натівськи налаштованих російських ЗМІ. А з точки зору майбутнього вступу України до НАТО та, відповідно, референдуму, без якого цей вступ не відбудеться, надзвичайно важливою є своєчасна інформаційна кампанія уряду, метою якої має бути формування в населення прихильного ставлення до організації та перспективи українського членства в ній. Про важливість такої кампанії свідчить, зокрема, досвід Норвегії. У 1994 році більшість населення Норвегії (52%) проголосувала проти членства країни в ЄС. Значною мірою на цей результат вплинула інтенсивна кампанія партій та угруповань, налаштованих проти інтеграції, яка тривала протягом двох років перед референдумом. Натомість норвезький уряд розпочав власну пропагандистську кампанію за кілька місяців перед проведенням референдуму [520]. Отже, українській владі, а, можливо, і НАТО, саме час подумати над інформаційною кампанією – супроводженням євроінтеграційних зусиль України, адже підтримка українським населенням перспективи вступу до НАТО є надзвичайно низькою: за даними Київського міжнародного інституту соціології, в травні 2005 року 21,3% українців були впевнені, що членство України в альянсі відповідає національним інтересам (39% - що суперечить) і 22,1% - згодні зі вступом України до НАТО (55,7% - не згодні; за даними Центра Разумкова) [519].

Основними проблемами сприйняття НАТО в світі є: ідентифікація НАТО з її країнами – членами, і в першу чергу – з США; сприйняття НАТО в першу чергу як військової, а не політичної організації; сприйняття НАТО як агресора. Однак ці проблеми цілком реально подолати шляхом активізації масово-інформаційної роботи. Зокрема, на конференції, присвяченій інтеграції України в НАТО та інформаційному супроводженню цього процесу, висувалися наступні пропозиції [520]. Рекомендується через мас-медіа репрезентувати НАТО як організацію, в рамках якої, попри несхожість ситуацій і національних військових потенціалів держав – членів Альянсу, всі вони однаковою мірою відчувають себе в безпеці, що, в свою чергу, сприяє загальній стабільності в Європі, створює сприятливі умови для зміцнення співпраці всередині Альянсу, а також між його членами та іншими країнами.

Інформаційні матеріали, розповсюджувані інформаційними центрами НАТО в різних країнах, мають містити визначення основних завдань Альянсу в галузі безпеки, зокрема:

- створення необхідного підґрунтя для стабільного середовища безпеки в Європі на основі зміцнення демократичних інституцій та прагнення до вирішення спорів мирним шляхом. Забезпечення умов, при яких жодна країна не змогла б вдаватись до залякувань чи тиску, спрямованих проти будь-якої іншої європейської держави, аби нав'язати своє панування через застосування сили, чи погрози силою;
- забезпечення стримування та захисту від будь-якої форми агресії, спрямованої проти території будь-якого члена НАТО;
- сприяння безпеці і стабільності шляхом здійснення постійної й активної співпраці з усіма партнерами через Партнерство заради миру та Раду євроатлантичного партнерства, а також через консультації, партнерство та співробітництво з Україною та Росією.

Далі зауважується, що з метою об'єктивного інформування населення України через можливості ЗМІ щодо структури, основних завдань і цілей Північноатлантичного альянсу, слушним було б:

- створення регіональної інформаційної мережі, яка б співпрацювала, з одного боку, з Центром інформації та документації НАТО в Києві, й місцевими НУО та ЗМІ, - з іншого;
- організація відповідних семінарів для журналістів, котрі спеціалізуватимуться з натівської тематики;
- організація та проведення лекцій і семінарів "лікнепівського спрямування" для студентської та учнівської молоді із залученням місцевих експертів, представників НАТО в Україні тощо.

Як видно з вище викладеного, НАТО і ЄС, попри відмінності у своїй сутності, цілях, політиці, тобто в «наповненні» бренду, мають аналогічні проблеми у сфері брендінгу, і ці проблеми пов'язані із недостатньою інформаційною роботою організацій і, відповідно, недостатньою поінформованістю громадян про їх діяльність. Обом організаціям слід активізувати свою роботу в сфері комунікації, і певні факти свідчать про те, що вони це усвідомили і працюють в цьому напрямку (для ЄС таким фактом є прийняття Білої книги з європейської комунікаційної політики [512]; для НАТО, зокрема, спільна російсько-натівська програма «Росія-НАТО: об'єднуючи зусилля», яка проходила з 11 по 26 травня минулого року і передбачала проведення конференцій, семінарів, круглих столів, зустрічей з пресою, культурних і спортивних заходів в різних містах країни з метою популяризації організації та її діяльності [521]).

Варто зупинитися на цільовій аудиторії брендінгової комунікації кожної з організацій. У сукупності аудиторія практично співпадає; обидві організації, хоч і є регіональними, однак діють на світовому рівні і фактично є суб'єктами глобальної політики. Тому адресатами їх інформаційної політики може виступати все населення Земної кулі, а особливо інші міжнародні організації, уряди країн, політичні діячі національного та світового рівнів, інтелектуальна еліта країн, журналісти та ін. Відмінності полягають в різній необхідності диверсифікувати цільову аудиторію і, відповідно, інформаційні потоки. Йдеться

про те, що з точки зору сприйняття НАТО світова громадськість набагато більш диверсифікована, аніж щодо сприйняття ЄС і це зумовлено в, першу чергу, історичними обставинами, а також цілями організацій. Це ставить перед НАТО додаткові більш складні завдання щодо планування інформаційно-комунікативної діяльності.

Однак найбільш значні відмінності в брендінгових стратегіях обох організацій пов'язані із особливостями їх цілей, завдань, суті діяльності тощо. НАТО – це в першу чергу військова і політично-безпекова організація, ЄС – політико-економічне інтеграційне утворення. Очевидно, що з цими специфічними рисами пов'язане різне наповнення і різна орієнтація брендів: НАТО – як гарант безпеки для країн членів і для всього регіону, а також постачальник гуманітарної допомоги, допомоги при стихійних та інших катастрофах тощо; ЄС – як гарант економічного процвітання, забезпечення прав людини тощо. Тут варто звернути увагу на те, що ЄС створювався в цілях гарантування безпеки після Другої світової війни, однак на сьогодні така позиція є застарілою, необхідна переорієнтація бренду на більш гуманітарний вимір. Як говорилося вище, експерти оцінюють стан брендів обох організацій як незадовільний. Вони потребують змін, тим не менш вони є пізнаваними, мають певне інформаційне наповнення і можуть виступати зразками для наслідування. Зокрема, провідні співробітники консультаційної агенції Prophet, що спеціалізується на розробці брендінгових і маркетингових стратегій, Рейчел Сіммонс та Лайза Маркізе, аналізуючи бренд ООН, вказують на успішність брендування обох європейських організацій, яким вдалося обом одночасно стати символом «західності», успіху, процвітання і при цьому зберегти свою ідентичність, уникаючи плутанини між ними [522].

Все свідчить про те, що ситуація щодо брендів ЄС та НАТО є не дуже сприятливою і в принципі аналогічною для обох організацій, однак за умови достатньої уваги, достатнього фінансування і правильного планування інформаційних кампаній можливе досягнення високих результатів.

4.5. Сучасні інструменти та технології впливу на політичний дискурс

Сьогодні в світі склалася ситуація, коли певні цінності, норми поступово поширюються на більшість регіонів земної кулі, коли ми говоримо про "світову спільноту" і глобалізацію, коли утворюється абсолютно новий вид суспільства, якого ще не існувало в попередні епохи, і долучення до якого нібито свідчить про високий стан демократії в країні. Це суспільство політичні науковці, бажаючи бути оригінальними і послідовними водночас, визначали по-різному: постіндустріальне (Д.Белл), постбуржуазне (Дж.Літхейм), постмодерне (А.Етціоні, Ф.Ліотар), постідеологічне (Л.Файєр), постнафтове, постліберальне, постколективістське , "третьої хвилі" (О.Тоффлер) і, навіть, "кінець історії" (Ф.Фукуяма). Пошук оригінальності, проте, як бачимо, не

позбавив ці терміни ані префіксу "пост", ані відчуття завершеності, пустоти, яка лишається "після" (post).

Одним із основних компонентів цього етапу "завершеності" можна вважати формування "медіа-направленої свідомості", яка переорієнтовує людину на сприйняття вже готових образів через засоби масової комунікації (ЗМК). Завдяки світовому поширенню електронної мережі і перетворенню телебачення на невід'ємну частину життя цей феномен сприяв появі суспільства позбавленого інших цінностей, окрім нав'язаних ЗМК, - суспільства масового споживання інформації. Якщо ж говорити про політичну площину такого суспільства, то насамперед в ньому зникають ідеології, як сукупності ідей, за які треба боротися, і віра в які передається "з покоління в покоління". Через це завданням політика в сучасному світі стає намагання викликати таке бажання в електорату, причому наголос переноситься: замість вдосконалення політичних гасел, аби вони більше подобалися виборцям, ми споглядаємо поліпшення методів маніпулювання вподобаннями виборців. Замість виведення досконалих економічних чи соціальних програм політик вивчає основи психології, аби підштовхнути виборця до необхідного йому рішення, і зокрема, змусити проголосувати за нього на виборах, важливому елементі будь-якого політичного процесу. Отже, що обличчя політика сьогодні, і відповідно його шанси на перемогу у виборах у демократичних країнах, визначають не ідеології, але більшою мірою політичні технології, і зокрема конкретна сфера їх застосування – політична реклама [523].

Одним із популярних методів політичної реклами, який чи не найкраще характеризує стан суспільства сьогодення, стало Нейролінгвістичне програмування (Neurolinguistic Programming, НЛП) – управління людською свідомістю за допомогою лінгвістичних конструкцій, архетипів, візуальних зображень тощо. Цей розділ практичної психології на рівні теорії виник ще в сімдесятих роках минулого століття, а років через десять західні політики стали активно використовувати його на виборах (Рональд Рейган та Маргарет Тетчер розпочали цю практику на найвищому рівні). В російську політику теоретичне НЛП прийшло вже на початку 90-х, і використання досвіду західних політтехнологів було найкраще продемонстровано вже на президентських виборах 1996 року. Україна натомість тільки сьогодні вступає в фазу застосування цих "високих" технологій – всі попередні вибори здебільшого проходили з використанням стандартних методик політичної реклами (тобто без урахування психологічних факторів впливу на електорат). Учасники українського політичного процесу ще й досі сприймають НЛП як певну релігію, майже магію, яка дозволяє безперешкодно отримати владу [524].

Але закономірно, що ставлення потроху змінюється (цей процес відбувався так само на Заході та в Росії: від "Структури магії" батьків НЛП Бендлера та Гріндера з їх "самовдосконаленням" – до серйозних наукових центрів, які взялися до детального вивчення технік НЛП, від групи провінційних ентузіастів – до серйозних іміджевих компаній на кшталт "Никколо М" чи

"Имидж-Контакт") – і тому можемо прогнозувати, що вже на президентських виборах 2009 року використання НЛП нарешті стане загальною практикою для політиків.

На жаль, в Україні існує невелика кількість наукових досліджень чи просто матеріалів про використання нейролінгвістичного програмування в політиці. Так само мало спеціалістів у галузі політичної реклами, які б могли проводити такі дослідження і відповідно забезпечити професійне проведення виборчих кампаній. Тому єдиним виходом поки що залишається залучення іноземних спеціалістів (зокрема, в Росії НЛП досліджують О.Ситников, С.Горін, А.Куртов, М.Каган та інші, в США та Європі – Е.Роббінс, М.Дейвін, С.Шарплі, ще й досі практикують засновники НЛП Р.Бендлер та Дж.Гріндер), і це на сьогодні складає основну проблему вітчизняної практичної політології. З огляду на вищезазначене можна тільки підкреслити нагальність та доцільність даного дослідження – в період, коли НЛП набуває все більшого значення як техніка психологічного впливу на людей, зростає необхідність в деміфологізації цієї техніки, позбавленні її рис магічності, всесильності [525].

Вже сьогодні в Україні точаться суперечки про "чисті" чи "брудні" технології – суперечки викликані власне відсутністю ґрунтовних праць з цієї проблематики (питання може стояти лише так: правові чи неправові технології). Так само помітною є тенденція до перебільшення ролі психологічних політтехнологій (в той час, як повністю нехтуються такі методи, як робота з фокус-групами, написання логічних і коректних передвиборних програм, організація роботи в регіональних осередках партій і т.д.).

Цю ситуацію можна виправити лише підведенням наукової основи до теорії політичної реклами, і НЛП як одного із її засобів – тим більше, що вже сьогодні постало питання із його практичним застосуванням.

Зазначалося, що сферою застосування нейролінгвістичного програмування в політиці є переважно політична реклама, причому до неї відноситься не тільки продукція рекламних фірм (постери, кліпи, листівки), але й будь-яка діяльність, спрямована на популяризацію:

- образу індивіда чи групи індивідів (організації), які прагнуть посісти певне становище у суспільстві (шляхом демократичних виборів, призначення на посаду, отримання пільг), зберегти таке становище або не допустити до нього своїх опонентів чи позбавити їх вже набутого статусу;
- ідей, норм, цінностей, в яких зацікавлений замовник реклами (наприклад, заклики сплачувати податки, берегти навколишнє середовище, підтримати політику уряду, соціальні чи економічні програми, вираження протесту – як це було із російським каналом НТВ, та ін.).

Отже, елементи політичної реклами наявні також у промовах політиків, слоганах та програмах політичних партій, газетних статтях, іміджевих інтерв'ю та інших засобах поширення інформації про осіб, зацікавлених в такій рекламі, або ж проти конкурентів таких осіб. Надалі політична реклама

буде розглядатися саме в такому її значенні – але насамперед варто звернутися до ширшого погляду на цей феномен комунікативних процесів у суспільстві.

Призначену спочатку для стимулювання торгівлі і згодом могутнє знаряддя конкурентної боротьби в комерції, рекламу в другій половині XX століття стали активно використовувати й у боротьбі суб'єктів політичної системи, власне кажучи, нав'язуючи тих чи інших кандидатів у політичних виборах. Відомий американський фахівець з реклами Джордж Луїс зазначав з цього приводу: "Добре це чи погано, але факт у тім, що реклама - єдиний спосіб, за допомогою якого кандидат може розказати про свої чесноти. Без реклами будь-який кандидат, незважаючи на усі свої шляхетні якості, буде просто знищений, на нього просто ніхто не зверне уваги" [526].

Але реклама – це не тільки цілеспрямована діяльність, що поширює яку-небудь інформацію, іміджеві характеристики чи ідеї політичного характеру з метою їхнього закріплення у свідомості мас. Така діяльність (на відміну від звичайних новин) також фактично корегує ставлення виборців до політика, по суті, впливає на суспільну свідомість. Таким чином, реклама є потоком інформації, який вибирає свою цільову аудиторію, або, що стало типовим для сучасної культури, формує власну цільову аудиторію, і створює у цієї групи людей певне (позитивне чи негативне, схвальне чи таке, що засуджує) уявлення про дану інформацію. В цьому розумінні рекламу ще часто називають пропагандою. Виборча пропаганда – систематизований, цілеспрямований вплив, здійснюваний партією або групою підтримки кандидата на виборчу посаду з метою поширити серед населення певну партійну ідеологію, переконати виборців віддати свої голоси за конкретну партію чи кандидата .

Причому особливістю політичної реклами є необхідність приховування такого впливу, маскування його, і через це загальний алгоритм діяльності, у порівнянні з комерційною рекламою, змінюється.

Хоча основні етапи, і відповідно задачі, залишаються сталими:

- привернути увагу виборців;
- зацікавити їх;
- змінити їхнє ставлення до політичного діяча;
- примусити їх до голосування.

Політична рекламна кампанія, звичайно, має на меті продати свій продукт – імідж політика, та особливість цієї мети – не тільки в досягненні ситуації, коли виборець просто купує товар, але і коли він "любить" кандидата і тому голосує за нього. А також можна зазначити ще одну - протилежну - ситуацію, коли виборець "ненавидить" чи "не любить" одного кандидата, і тому голосує за іншого. Цей другий варіант притаманний тільки політичній рекламі, оскільки традиційні етичні норми комерційної сфери забороняють схожу діяльність.

Також ознакою політичної реклами є те, що вона продає віртуальний продукт, той, якого фактично не існує, – імідж (політика чи ідеї). Імідж – це

спеціально створюваний, навмисно сформований політичний образ для досягнення конкретних цілей. Імідж, який будується за допомогою політичної реклами та інших засобів для досягнення цих цілей в межах певної стратегії, політичні консультанти ще називають стратегічний образ. І сьогодні в світі складається ситуація, коли стратегічний образ фактично заступає собою справжню сутність людини – в результаті політики говорять, діють і живуть так, як їм вказують спеціалісти зі створення іміджу [527].

Звідси й відома сентенція, що політичний діяч в наш час – це скоріше штучний телевізійний образ, аніж жива істота, якщо ж підвести це формулювання під наукову основу, то воно звучатиме так, що в новочасних західних демократіях реклама перестає бути "дискурсом про речі", і набуває все виразніших ознак "*дискурсу-речі*" . В Україні ця ситуація поки що є скоріше винятком, аніж загальною практикою – вітчизняні політичні діячі продовжують частіше керуватися власними емоціями, ніж порадами політтехнологів (можна в цьому плані згадати численні бійки політичних діячів, особливо ті, які повністю суперечать вже створеному).

Говорячи про інші особливості політичної реклами, варто також пам'ятати, що це форма непрямої політичної комунікації, тому вона має відповідну структуру: джерело інформації, засоби її доставки і адресат (реципієнт). І, для того, щоб акт комунікації відбувся, треба, аби комунікатор і адресат спілкувалися однією мовою і однаково сприймали мовлене, щоб вони мали спільний досвід, необхідний для розуміння символів, тобто пережили б ряд однакових подій.

Саме тому політики використовують в політичній рекламі концепції, близькі виборцям, історії, які є знайомими, слова, що зрозумілі цільовій групі. Фактично ж завдяки цьому створюється нерозривний зв'язок між джерелом інформації і адресатом – бо власне тільки за цієї умови мета буде досягнута – "*товар буде придбано*". Такий зв'язок в наш час прийнято називати "*маніпуляцією*", іноді – "*промиванням мізків*", також модним стає до цього згадувати "нейролінгвістичне програмування".

Маніпуляція – це програмування думок і прагнень мас, їхніх настроїв і, навіть, психічного стану з метою забезпечити таку їхню поведінку, яка конче потрібна власникам засобів маніпуляції . Очевидно, що цей термін підходить так само і під поняття "політичної реклами", тому варто підкреслити, що, говорячи "маніпуляція", ми описуємо загалом негативні аспекти рекламування – не просто приховані, але такі що приховано порушують природні права людей, втручаються в їхню психіку.

Проте, маніпуляція – це не насильство, це метод представницької демократії. Ідея маніпуляції якраз і полягає в тому, щоб фактичне нав'язування думки виглядало зовні як власне бажання людей.

Між іншим, на цьому ґрунтується один із закидів демократичним режимам – створення таких методів управління людьми, які набагато важче виявити і викорінити, ніж звичайний деспотизм.

Ускладнює ситуацію ще й той факт, що маніпулятивних технологій є декілька: 1) створення позитивних установок виборців на "політичний товар", 2) трансформація інформаційного потоку (брехня, замовчування, створення інформаційного шуму тощо), 3) в особливу групу виділяють використання підсвідомих і підпорогових інформаційних стимулів різних модальностей: аудиальних, візуальних, тактильних та інших .

Саме до них відноситься НЛП. І якщо політична реклама загалом має декілька важливих функцій (інформаційна, функція переконання, привабленя, спонукання), то політичне НЛП має лише тільки одну — нав'язування цінностей і формування вибору індивіда [528].

Перед тим, як переходити до огляду використання нейролінгвістичного програмування в політиці варто коротко оглянути особливості політичної реклами. По-перше, і найголовніше — це те, що політична реклама (і НЛП зокрема) є ознаками демократичного суспільства, в якому проводяться вибори до представницьких органів влади, існує мережа недержавних громадських організацій і засобів масової комунікації. За інших умов вона стає просто непотрібною, оскільки є засобом конкурентної боротьби, а в тоталітарному суспільстві конкуренція неможлива (звичайно, НЛП можна використовувати для впливу диктатора на натовп — як-то несвідомо робив А.Гітлер, але такий вплив є несуттєвим, якщо диктатор володіє іншими методами примушення — наглядовими та каральними органами тощо).

По-друге, політична реклама є комунікаційним процесом, який не просто надає інформацію, але й створює її, аби спонукати громадян до певних дій. Або, як влучно зазначив Пол Лайнбарджер: "Факт — це не пропаганда. Пропаганда — це інтерпретація факту". Саме тому треба ставитися до політичної реклами як до самостійного й незалежного дискурсу, що використовує різноманітні техніки, аби непомітно нав'язати виборцю цінності, і потім маніпулювати його діяльністю. До таких технік відноситься нейролінгвістичне програмування (НЛП).

У роботах, присвячених питанню використання НЛП-технологій в політиці не існує чіткого і єдиного визначення НЛП — термін розуміють порізному, і часто зводять до декількох коротких, іноді метафоричних дефініцій. Втім, їх можна скомпілювати в одному спільному понятті:

Нейролінгвістичне програмування (Neurolinguistic programming, НЛП) — це методика вивчення суб'єктивного досвіду, і створення відповідних моделей поведінки і наборів навичок та технік.

В той же час легше зрозуміти сутність НЛП через предмет його вивчення. Таким предметом є "*паттерни*" (patterns) — в даному випадку неперекладний термін, який означає приклади поведінки, що створені взаємодією мозку (звідси частка "*нейро*"), мови ("*лінгвістичне*") і тіла. Теорія НЛП з'явилася власне через аналіз таких "паттернів досконалості" в експертів у різноманітних галузях професіональної комунікації.

Засновниками НЛП вважаються американці Джон Гріндер і Ричард Бендлер (John Grinder and Richard Bandler) – до речі, в 90-х роках їх було визнано одними зі ста видатних людей, які вплинули на розвиток США. Д.Гріндер був асистентом професора лінгвістики в університеті Каліфорнії в Санта Круз, Р.Бендлер – програмістом, студентом математики (за деякими джерелами – психології, але версія із математикою видається вірогіднішою, бо вся теорія НЛП просякнута бажанням віднайти певні алгоритми людської діяльності, структурувати її) в тому ж університеті. Вони вирішили віднайти "код ефективної комунікації", і в 1974 році стали вивчати дії трьох видатних психотерапевтів: Ф.Перлза, засновника школи гештальт-терапії, Вірджинії Сатир, сімейного терапевта, і, нарешті, Мільтона Еріксона, всесвітньо відомого гіпнотерапевта (саме він винайшов надзвичайно популярний сьогодні ериксоніанський гіпноз – такий, що не вводить пацієнта в стан трансу, але все одно нав'язує певні твердження, цей гіпноз багато чого надав для подальшого розвитку нейролінгвістичного програмування).

У результаті вчені знайшли взаємозв'язок між жестами, мімікою людини і структурою її мови. Бендлер і Гріндер не збиралися відкривати нову школу терапії, вони просто хотіли визначити "паттерни", які застосовують терапевти, щоби налагоджувати ідеальний контакт зі своїми пацієнтами. Але до 1976 року вони назбирали достатньо матеріалу, щоби створити "нейролінгвістичне програмування" – доволі недолугий термін, який, за їх власним зізнанням, слугував більше привертанню уваги, аніж поясненню цієї теорії.

Втім, ідея була простою – НЛП має справу зі структурою суб'єктивного досвіду людини: як ми організуємо те, що бачимо, чуємо і відчуваємо (відчуття людини – це є частка "neuro"), і як ми редагуємо і фільтруємо за допомогою органів почуттів те, що отримали із зовнішнього світу. НЛП також досліджує те, як ми описуємо це в мові (linguistic), і як ми діємо – навмисно чи ненавмисно – щоб одержати результат (programming) [529].

Вважається, що НЛП (у своєму спрощеному вигляді) виникло досить давно і майже всі видатні історичні постаті вдало застосовували ті чи інші його техніки, зокрема, видатні оратори, генерали, диктатори. Часто в літературі, присвяченій нейролінгвістичному програмуванню, можна зустріти посилання на Наполеона чи Лінкольна, як на першовідкривачів деяких засобів НЛП. Але найчастіше все ж таки згадують діячів двадцятого століття – насамперед через розвиток психологічних наук (вчення про архетипи Юнга, дослідження Еріксона також стали здобутками НЛП) й існування багатьох політичних прецедентів із використанням технік НЛП (наприклад, А.Гітлера та Й.Сталіна вважають професіоналами в цій справі). Багато хто вважає, що дослідження НЛП з'явилися в СРСР, навіть, раніше, ніж в США, і першими центрами цієї сфери психології стали відділи ЦК КПРС з агітації та пропаганди (наводяться й конкретні випадки – так звана "фраза-зомбі" *"Партія – розум, честь і совість нашої епохи"*). Проте, тільки в вісімдесятих роках XX століття ней-

ролінгвістичне програмування стало повноправним елементом політичної боротьби [266].

Кінець двадцятого століття взагалі характеризують як початок періоду, коли політичні технології починають грати вирішальну роль під час політичних виборів, а політична реклама шукає все нових засобів впливу на аудиторію. В цей же час люди починають усвідомлювати негативні сторони впливу на підсвідомість, і намагаються обмежити на законодавчому рівні застосування таких технік. Так, в багатьох країнах було заборонено такі методи НЛП, як 25-ий кадр та використання звуків, що не сприймаються на рівні свідомості. Через це все більше уваги забирають легальні – візуальні, вербальні та інші техніки нейролінгвістичного програмування. Першими на науковому рівні (тобто з консультаціями професіоналів, створенням окремих центрів) їх почали використовувати такі відомі політики, як Рональд Рейган та Маргарет Тетчер.

Зокрема, відомий спеціаліст з НЛП, який консультував Вільяма Клінтона впродовж обох президентських кампаній США, Ентоні Роббінс, в своїй книжці зазначає, що Р.Рейган, балотуючись в президенти, постійно використовував у телевізійних роликах образ ведмедя, який для американців є "сильним негативним символом Росії". Також застосовувалися зловісні музика й освітлення, і в результаті Р.Рейган отримав імідж "сильного президента", який знає, як побороти радянську загрозу. О. Ситников згадує про спеціалістів з нейролінгвістичного програмування Трилевана та Гергена, які працювали з Рейганом, а потім – з Дж. Бушем. Фактично ж, сьогодні жодні вибори на Заході не проходять без застосування НЛП – причому ще й досі застосовують недобросовісні та заборонені техніки. Так, на виборах Президента США в 2000 році сталася ситуація, коли Республіканську партію звинуватили в тому, що вона впливає на підсвідомість телеглядачів: у відеорекламі про реформу медичного страхування Джорджа Буша під час асоціювання демократів Альберта Гора з бюрократами (bureaucrats) двадцять п'ятим кадром проходило слово "пацюки" (rats). Ситуацію, щоправда, "зам'яли", проте спеціалісти вважають її типовим прикладом застосування заборонених технік НЛП [530-531].

У країни СНД НЛП прийшло тільки з відлигою, а в політиці його почали використовувати в 1991 році в Росії (наприклад, під час виборів в Росії імідж Б.Єльцина створювали на контрасті з М.Горбачовим). Але тільки в 1996 році в Росії нейролінгвістичне програмування стало нормальною практикою, коли навіть головний слоган виборчої кампанії "Голосуй або програєш" та його символіка стали найкращим втіленням нейролінгвістичних технік. В Росії сьогодні НЛП є справді розвиненою галуззю, в яку вкладаються великі гроші, і яку досліджують численні центри ("Никколо М" та "Имидж-Контакт" – видають літературу, проводять семінари, формують виборчі стратегії в багатьох країнах пострадянського простору).

Давно створені іміджеві компанії, які використовують західний досвід і консультують відомих політиків (В.Путіна, В.Жириновського). Ней-

ролінгвістичне програмування настільки ввійшло в політичне життя Російської Федерації, що існує, навіть, пов'язана з ним версія появи Володимира Путіна в російській політиці: адміністрація президента Єльцина (символ "ведмедя", найсильніший для російського менталітету) шукала політика із іміджем "вовка", який би заступив менш популярний символ "кабана" Лужкова. Тобто фактично жодне політичне рішення сьогодні не ухвалюється без консультації зі спеціалістами з НЛП.

Україна в цьому плані набагато відстає від Росії – майже не існує компаній, які б серйозно займалися дослідженням НЛП, для проведення виборів здебільшого запрошують російських спеціалістів, які, не знаючи особливостей українського політичного дискурсу, просто не в змозі вибудувати необхідні стратегії. Ще й досі можемо споглядати недолугі плакати, слогани, телерекламу, які не враховують особливості людської психіки, і тому часто мають протилежний від бажаного ефект.

Проте ситуація поступово змінюється: з'являється вітчизняна література з політичних технологій (насамперед книги Г.Почепцова, В.Бебика, Ю. Романенко та ін.), політики серйозно цікавляться нейролінгвістичним програмуванням. Видається, що президентські вибори 2009 року будуть проходити вже із повним застосуванням технік НЛП (нехай і за допомоги російських спеціалістів). Проте ці вибори скоріше за все ще більше закріплять в суспільстві враження про НЛП, як про всемогутню методику, науку, що може вирішувати будь-які задачі. Саме тому найближчою задачею політичної психології (підтримка держави була би бажаною – недарма ж в США НЛП займається Пентагон) є деміфологізація НЛП, критичний підхід до його технік і виведення аксіом щодо його впливу на підсвідомість людини [532-533].

У літературі, присвяченій НЛП, дуже рідко можна зустріти критичні погляди на природу цього феномену – здебільшого автори описують випадки перемоги безперспективних кандидатів у президенти чи нав'язування цілим групам певних суджень.

Насправді ж НЛП не є такою всемогутньою зброєю в руках політичних технологів. Його застосування не часто приносить стовідсоткові результати – зазвичай це незначне підняття рейтингу, корекція іміджу чи поступове нарощення симпатії виборців. НЛП – дієвий метод тоді, коли його поєднують з іншими методами під час виборчої кампанії.

Також хибною є думка про науковість нейролінгвістичного програмування. Насправді теорію НЛП майже ніколи не перевіряли "в лабораторії". Ті ж психологи, які проводили дослідження деяких технік НЛП у контрольованому середовищі, не перебільшують його можливості. Зокрема, на сайті "*What About NLP?*" зібрано критичні матеріали з літератури до 1997 року, які іноді сутність нейролінгвістичного програмування характеризують таким чином [534]:

"Незважаючи на твердження, що невропатологія (neuroscience) є його джерелом, погляди НЛП на зв'язки між функціями мозку та когнітивними

можливостями людини зводяться хіба що до сирих аналогій. НЛП має гарні рекомендації, але Національна Рада з досліджень не може надати жодних свідчень на його користь, чи навіть лаконічного визначення його теорії".

"...НЛП. Теорія не є чітко артикульованою, її термінологія, передумови та висновки – двозначні або ж погано окреслені. ...основною причиною для неадекватності теорії є запозичення нею з інших теорій, які є антагоністичними одна до одної... Висновки після огляду літератури такі, що, як теорія, вона є нерозвиненою і незв'язаною, а її техніки не пропонують нічого нового".

"Результатом стали значні співвідношення (intercorrelation) між діями суб'єкта в різних сенсорних режимах, але й цей єдиний можливий результат не було передбачено НЛП". "Головні положення НЛП було неможливо точно довести в майже 86% випадках контрольованих студій... НЛП досягло статусу на кшталт культу, коли воно стало нічим іншим, як ще однією психологічною примхою" .

Звичайно, такі судження є дещо емоційними, і не варто повністю покладатися на думку консервативних науковців, які чинять спротив новим віянням в науці. Теорію З.Фройда так само критично сприймали в наукових колах, сьогоднішні ж психологічні та філософські погляди багато чого запозичили у видатного психоаналітика. Тому, досліджуючи нейролінгвістичне програмування, необхідно пам'ятати, що воно – теорія практичного застосування засобів психологічного впливу на підсвідомість людини, а також методика проведення ефективних комунікаційних процесів.

Будь-яка абсолютизація цих визначень – чи в бік психологічної релігії, чи повного неприйняття теорії – призводить до ще більшого віддалення від науковості предмету і нав'язування стереотипів чи ярликів.

НЛП – не наукова теорія, бо й справді не доводить своєї дієвості в контрольованих умовах, але інша його сторона – вчення про правильне спілкування, про уникнення конфліктів гарантує його популярність попри будь-яку критику. До того ж, НЛП все ж має власну специфічну сферу, набір методик і технік, які й відрізняють його від інших шкіл практичної психології. Метою залишається не безперестанна критика НЛП чи його абсолютизація, але впорядкування вже набутого знання, структурування його у вигляді чітких тверджень, правил та аксіом.

Тільки в цьому випадку можна буде передбачувати наслідки застосування НЛП в політичній рекламі, використовувати його техніки відповідно до чітких регуляцій, а не власного бачення проблеми. Звичайно, нейролінгвістичне програмування ніколи не стане строгою наукою, але набуття чіткої структури є важливою вимогою для цієї теорії. Сьогодні така структура існує тільки у визначенні технік НЛП та можливостей їх застосування – власне з цього і почалося нейролінгвістичне програмування – зі знаходження методів, "паттернів" діяльності.

Як вже зазначалося, науковим є поділ не на "чорну" чи "білу" політичну рекламу, а на правову та неправову. Нейролінгвістичне програмування во-

лодіє прикладами технік обох напрямів. Зокрема, найвідомішим неправовим методом, який заборонено в усіх розвинених демократичних країнах, є так званий ефект 25-го кадру. Точніше, sublimina чи "феномен 25-го кадру", чи *"ефект 36-го кадру"*, чи *"ефект Берда"* – у відеоматеріалах, а також відповідник в аудіо форматі – messude [535].

Сьогодні питання 25-го кадру є доволі суперечливим. З одного боку, цей досить корисний ефект використовують у навчанні, коли підсвідомість легше сприймає інформацію (свідомість "розуміє" лише 24 кадри в секунду, якщо їх буде більше – то інформація сприймається тільки підсвідомістю, що є набагато ефективніше). Водночас, застосовуючи цей феномен, наприклад, в політиці, можна програмувати людські дії, проте сьогоднішні технології (звичайний відеомагнітофон розпізнає покадрову інформацію) дозволяють з легкістю виявляти зловживання цією можливістю (вже згаданий конфлікт на виборах 2000 року в США). Через такий стан речей sublimina має неоднозначний характер серед технік НЛП – забороненими лишаються маніпуляції зі свідомістю, але процеси навчання, лікування, релаксації, що використовують 25-й кадр, сприймаються доволі позитивно. Зовсім інший стан речей споглядаємо в царині аудіо-пропаганди.

Тут існує свій 25-й кадр – messude, який є набагато ефективнішим засобом маніпуляції, і майже непридатним для розпізнавання. Його специфіка полягає в тому, що поряд зі звичайним текстом, наприклад, прочитанням політичного гасла, в ефір пускають звук нижчий або вищий, ніж його може сприймати свідомість. Тут можливі два варіанти. По-перше, цим можна створювати настрій слухачів – так, доведено, що ультразвук не надто низьких частот викликає в людині відчуття паніки, остраху, агресії.

Цю властивість можна використовувати в політичній антирекламі, коли бажано створити образ ворога ("вони"), "червоної загрози" (що практикували на виборах в Росії 1996 року і в Україні 1999 року), бажання не голосувати за певного кандидата. По-друге, можна паралельно з одним текстом, нейтральним по суті, транслювати інший, який буде сприйматися підсвідомістю як аксіома, але людина не зможе свідомо його почути.

Цим текстом нав'язуються конкретні цінності, поняття, а не просто відчуття страху чи обережності. Саме так, наприклад, можна створити у виборців впевненість, ніби кандидат в депутати має якийсь стосунок до торгівлі зброєю, наркотиками тощо. Якщо закріпити цю впевненість статтею в регіональній пресі, то зазначений політик вже матиме конкретний, хоча й фактами не доведений, імідж. Схожі технології, за деякими свідченнями, було вдало використано на парламентських виборах 2006 року. Але оскільки тільки спеціальною апаратурою можна виявити маніпуляції на рівні звуку, то часто можна лише здогадуватися про методи пропаганди, які використовують сучасні політичні діячі.

Звук і освітлення взагалі є універсальними засобами створення настрою, але засобами правовими, тому тут ми лише підкреслимо їх значення у

створенні теле- чи аудіореклами. Натомість варто згадати, що неправові техніки – це також ті, які суперечать існуючому виборчому законодавству. Тому, наприклад, неприпустимими є застосування дозволених методів НЛП держслужбовцями, також агітація в день виборів. Для кращого розуміння можна навести приклад згаданої вже парламентської кампанії 2006 року в Україні. Основним слоганом однієї з політичних партій був вираз "Вибирай серцем". Ця фраза була створена з урахуванням технік НЛП – слова "душа" та "серце" сприймаються підсвідомістю, як близькі, такі, що не потребують пояснення, роздумування. Втім, цю техніку застосовують повсюди. Таким чином, відбулася "активізація установки", і хоча можна сперечатися про фактичний вплив цієї фрази на вибір українців.

Наприкінці аналізу неправових методів НЛП у політичній рекламі згадаємо про моральні аспекти цього питання. Насамперед, це стосується країн пострадянського простору, де законодавством ще не визначено, які техніки можна застосовувати, а які – ні. Через це вибір методів має робити кожен політик і політичний технолог відповідно до власних етичних переконань. І хоча "чорний PR" так само домінує в політичній рекламі США чи інших західних країн, все ж варто іноді дотримуватися правил моралі у політичній боротьбі. Інакше, вершинами реклами залишатимуться плакати на кшталт "Ткаченко зможе, якщо віагра допоможе". Політична реклама – мистецтво, в якому важливо не просто перемогти супротивника, але й зробити це красиво. Як приклад творчого підходу, можна навести плакат в центрі Москви, який демонстрував малюнок із "Маленького принца" Сент-Екзюпері, і фразу "БаоБАБи треба висапувати, інакше вони розірвуть планету на частини", де абревіатура БАБ стосувалася відомого політика Бориса Абрамовича Березовського (книжки типу "*Маленького принцу*" сприймаються підсвідомістю як щось беззаперечне, істинне). Політична реклама є дієвою не тільки, коли вона застосовує психотехніки, але й коли приваблює виборця оригінальністю, гумором, сюжетом. І також бажано, щоби вона відповідала нормам чинного законодавства.

Говорячи про НЛП, важливо завжди пам'ятати, що це технологія правильного спілкування. Через це головний принцип НЛП – тільки ефективна комунікація може привести до політичної влади, а така комунікація можлива лише зі створенням гнучкого ставлення до інформації та комунікаційних актів. Як приклад ідеального вирішення цього питання часто наводять політику Французького Національного Фронту Жана-Марі Лє Пена (Jean-Marie Le Pen), яка ґрунтується на твердженні, що "політична боротьба має вестися на рівні ідей та за умови політичної гнучкості". Саме це дозволило партії об'єднувати в собі досить різні сили, реагувати на зміни в середовищі, "погоджуватися, а не конфліктувати" [536].

І якщо комунікація – це тло НЛП, то його основою, тим, з чого воно виникло, є встановлення раппорту (rapport) чи емпатії, особливого зв'язку між джерелом інформації та реципієнтом. Раппорт – це налагодження таких сто-

сунків, коли комунікація проходить на ідеальному рівні, коли джерело інформації, політичний агент, не потребує докладати великих зусиль, щоби переконати реципієнта, маніпулювати ним — реципієнт не противиться впливові. Раппорт — це аналог наведення трансу, хоча адресат і залишається в повній свідомості, він просто не відчуває, що ним маніпулюють. У будь-якій сфері людської діяльності раппорт є важливим для встановлення атмосфери довіри, конфіденційності й порозуміння.

Елементами встановлення раппорту є приєднання і ведення. Приєднання (pacing) — це зміна власної поведінки для того, щоб налагодити підсвідомий контакт із реципієнтом. Фактично для приєднання важливо повторювати основні елементи поведінки іншої людини — займати таку саму позу (або віддзеркалювати її — повторювати не повністю, але деякими елементами — схрещувати, наприклад не руки, але долоні), дихати в такт, рухатися, рухати зіницями. Цим налагоджується зв'язок між джерелом і адресатом інформації. Через деякий час після приєднання адресата можна буде вести, тобто створювати в нього стан наближений до трансу. Ведення (leading) — це зміна власної поведінки, стану, що призводить до такої ж зміни в реципієнта. Фактично, процес є аналогічним приєднанню, тільки обернений, і тепер адресат є доволі керованим і підданим впливові. Ось чому важливо спочатку приєднатися — довести його до стану, коли інформація буде сприйматися ним беззаперечно, і вже потім нав'язувати йому конкретні судження про політика, його конкурентів, соціальну програму тощо.

Ведення можливе і без приєднання (багато сьогоднішніх політиків просто не в змозі його провести). Для цього достатньо впливати на людей, які вже знаходяться в стані межового стану свідомості. Саме тому сучасна політична реклама широко послуговується масовими зібраннями людей — концертами, футбольними матчами, мітингами (ритм, нестача кисню, голосні звуки, як доведено медициною, створюють ефект ейфорії, трансу, коли людина є надзвичайно піддана впливам). Між іншим, попри досить часте звернення до концертів як методу пропаганди, вітчизняна політика досить непрофесійно використовує ці засоби, оскільки неправильними є шляхи донесення інформації. Зазвичай, політичні лідери виходять із промовами до початку дійства, тоді як робити це необхідно під час, або опісля концерту чи матчу — причому необхідно дотримуватися в промові загальної ритміки видовища. Серед вітчизняних політиків досить вміло у свій час використав цю техніку В.Кононов, лідер партії Зелених України (тому в молодіжному середовищі склалося уявлення про нього як про "свого" — і ПЗУ прекрасно підтримує цей імідж, складається враження, що двозначність слогану *"Прикольнись — присядь на траву"* — не недолугість політтехнологів, а вдало продуманий хід) [537].

Загалом же *приєднання та ведення є найефективнішими техніками* НЛП. Тільки професіонали можуть вводити виборців у стан, наближений до трансу, але позитивний результат доводить зручність методики встановлення

раппорту. У політичній діяльності найкращими засобами для раппорту є промови, телевізійні шоу, теле- та радіотрансляції (за допомогою звуку, освітлення, ритму встановлюється певний настрій електорату, потім політичний агент приєднується до цього стану, і на останньому етапі нав'язує виборцям необхідні установки). Щоправда, вважається, що існує певне часове обмеження — раппорт не може забезпечити тривалу установку, тому серйозні маніпуляції з підсвідомістю бажано проводити за короткий час до виборів (тиждень — два дні), або ж робити сеанси періодично.

Прикладом вдалого практикування теорії приєднання і ведення наводять знову ж таки Французький Національний Фронт. У його політиці це звучить як ідея, що поступове та обережне наведення зв'язків у потенційно ворожому суспільстві призводить до знищення бар'єрів між антагоністичними групами. Всі інші техніки НЛП значною мірою залежать від встановлення раппорту — таким чином, він є не тільки основою нейролінгвістичного програмування, але й передумовою застосування інших методів. Втім, приєднання та ведення можливі також за дотримання політтехнологом конкретних умов — зокрема виявлення стану реципієнта, до якого й треба приєднуватися.

У зв'язку з цим в НЛП існує друга основна ідея: будь-яка діяльність формується під впливом, переважно, трьох груп факторів, трьох репрезентативних систем — візуальної (сприйняття образів), аудиальної (сприйняття звуків) та кінестетичної (сприйняття доторків, відчуття шкірою). В психологічній теорії НЛП це дозволило розділити людство на окремі типи, в характері яких домінує той чи інший фактор сприйняття, тому й відповідно впливати на них можливо тільки у їх власній системі почуттів. Але нас, насамперед, цікавить можливість застосування цієї теорії в політичній пропаганді.

Згадаємо техніку *"очі як ключі доступу" (eye accessing cues)*. Відповідно до неї рухи зіниць у певних напрямах можуть вказати на візуальне, аудиальне чи кінестетичне мислення (це справджується у 90% людей з домінантною правою рукою). Так, доведено, що рух очей вліво вгору свідчить про згадування візуальних образів, вправо вгору — уявлення образів (можливо утопічних), вліво — згадування звуків, вправо — конструювання ніколи не чутих аудиальних образів, вниз направо — відчуття емоцій, тактильних (доторки) рухів тощо.

Чим корисна в політичній діяльності ця техніка? Насамперед, досить ефективною вона виявляється на індивідуальному рівні спілкування, коли необхідно визначити домінантний тип адресата інформації. Після такого визначення по рухові очей можна спілкуватися в системі образів близьких реципієнту, коли він легше довірятиме джерелу інформації. Зокрема, дослідники НЛП давно вивели конкретні поради із застосування тих чи інших мовних конструкцій в залежності до типу співрозмовника — їх можна знайти в роботах Р.Бендлера і Дж. Гріндера, С.Горіна, О.Ситникова. Проте, у зв'язку з тим, що політична реклама дуже рідко послуговується індивідуальним спілкуван-

ням і орієнтується здебільшого на масову аудиторію, у даному випадку цікавить інший аспект застосування ключів доступу до уявлень людей. Це – підкреслення в тексті тих мовних конструкцій, які важливі для маніпулювання свідомістю виборців. Зокрема, відповідно до особливостей руху очей, робити це можна рукою, нахилами голови тощо. Так, говорячи про образ "червоної загрози", описуючи довгі черги, талони на продукти перед аудиторією, можна піднімати вправо (для аудиторії – вліво) руку, надаючи промові образного характеру, нав'язуючи уявлення про промовця, як про цілісну, чесну людину.

Але не тільки очі свідчать про поточний стан людини, сприйняття нею інформації. Це можна дізнатися і з тих мовних конструкцій, які вона вживає. І водночас навпаки – в процесі ведення важливо використовувати такі мовні, емоційні та мімічні засоби, щоб ефективно впливати на підсвідомість реципієнта. Так, Сергій Горін, російський психотерапевт, визначає такі способи виділення повідомлень [538]:

- аудиальні: зміна темпу, тембру, інтонації, голосності мови, супутні звуки (постукування по столу, поплескування в долоні);
- візуальні: зміна положення тіла, жестикуляція руками, пальцями, пантоміміка;
- кінестетичні: простий дотик, поплескування по плечу, потиск руки (занадто довгий, наприклад);
- змішані: зміна дистанції до співрозмовника, рухи водночас зі звуками ("шумна жестикуляція"), аналогове маркування (analogue marking) – т.зв. "мова тіла".

Пам'ятаючи про ці техніки можна завжди діяти в одній системі почуттів з адресатом, тим самим полегшуючи контакт. Ці ж елементи є необхідними в політичній телевізійній та радіорекламі, де ніщо не передасть нервове напруження краще, ніж перестукування пальцями по столу, а атмосферу довіри створить тихий голос й уповільнення його темпу.

Проте, особливості людського сприйняття можна використовувати не тільки в спілкуванні. Так, текстове наповнення будь-якого документа (листівки, плаката) теж визначається відмінностями між репрезентативними системами різних людей. Головним правилом при створенні такого політичного документа є вимога позитивних емоцій по кожному з каналів сприйняття інформації. Так, позитивні емоції створюють візуальні образи: ока, долара, архетипів; аудиальні: шелест купюр, гімн, романтична мелодія гітари; кінестетичні: тканина, оксамит, шкіра.

Нарешті, форма подачі матеріалу може носити нестандартний характер, виходити за рамки нормального сприйняття і цим викликати транс. Так, коли людина раптово натрапляє на інвективне слово (цим часто користується російський політик В.Жириновський), вона почувається дезорієнтованою і менш критично сприймає наступні за ним імперативи.

Отже вдале використання технік НЛП потребує від виконавця ґрунтовного знання людської психології, швидкого реагування і вміння налагоджува-

ти контакт. Звичайно, не варто абсолютизувати поділ людства на три репрезентативні системи відповідно до світосприйняття, але з огляду на комунікаційні основи нейролінгвістичного програмування, ця методологія видається почасти дієвою – принаймні як передумова налагодження раппорту.

Ще однією технікою, важливою для НЛП як теорії, є міжгалузевий і комплексний метод "якорів" (anchors). Якорі – поняття доволі складне, яке увібрало в себе вчення про архетипи, ярликування, стереотипи та сигнальні системи Павлова. Стисло, якір – це стимул, що зв'язаний з конкретним фізіологічним станом людини і запускає його. Принцип схожий на створення умовного рефлексу – внутрішня реакція зв'язується з якимсь зовнішнім стимулом, щоб потім можна було цю реакцію швидко (іноді скрито) відтворювати [539].

У НЛП якорі ділять на візуальні (жести рукою, улюблені фотографії, червоне світло), аудиальні (певні звуки, слова, дзвінок), кінестетичні (доторки). Критеріями створення правильного якоря є інтенсивність переживання (сильна емоція формує стабільний якір), синхронність (повторювання асоціації між інформацією та, наприклад, кольором створює якір) та точність подальшого відтворення стимулу. Ці три умови забезпечують маніпулювання поведінкою адресата.

Якорі – це все, що викликає емоційний стан, і вони є настільки очевидними і широко розповсюдженими, що люди часто не помічають їх – і цим користується реклама, зокрема політична. Так, при створенні будь-якого пропагандистського документу необхідно враховувати результати досліджень з якорями кольорів, шрифтів, символів, ієрархією елементів реклами.

Особливе смислове навантаження несе в собі кольорова гамма політичного плакату – оскільки контраст за рахунок сильнішої стимуляції зорового нерву привертає більшу увагу, закріплює установку на позитивне чи негативне сприйняття кандидата чи ідеї. Кольори – це не просто засіб полегшення прочитання тексту (так, найкраще читається чорний текст на жовтому фоні), створення візуальних ілюзій (червоний – близькості, синій – навпаки, віддаленості), вони несуть також психологічні стереотипи.

Ці стереотипи необхідно враховувати в одязі політика, при створенні інтер'єру телевізійної реклами: жовтий – тепло, світло; чорний – офіційний, серйозний або скорбота, нещастя; зелений – свіжість, чистота, життя; синій – спокій, меланхолія; коричневий – деградація, тривога, депресія і т.д. Власне самими тільки кольорами можна створювати настрій політичної реклами – і разом із нейтральним текстовим наповненням вона може нести позитивний чи негативний сенс (фраза "вони одягаються в коричневі костюми" нейтральна, проте викликає недовіру до "них").

Близькими до ролі кольорів є й інші засоби графічного зображення тексту, зокрема, шрифти. Наведемо лише один, але класичний, приклад польського антиплакату, на якому у верхній частині білого листа було написано "Лех Валенса" в стилі графіті (так страйкарі писали у 80-і роки), а в нижньому –

те ж саме, але в стилі логотипа Кока-Коли. Саме так поляки стверджували, що лідер "Солідарності" продався американцям.

Проблемою кольорів, шрифтів та дизайну загалом є їх візуальна прив'язаність, отже, неможливість застосування в радіорекламі. Проте величезний блок символів-якорів як техніки НЛП в політичній рекламі цілком компенсує цю нестачу. Символи (*стереотипи, архетипи*) завжди використовувалися в людському мовленні для короткого визначення тих чи інших істин. Вони давно закріпилися у підсвідомості як самостійні смислові форми, що сильно впливають на свідомі дії людини (сюди відносимо національні стереотипи). У практиці НЛП давно було помічено, що створення якоря на такі символи є досить сильним і дозволяє маніпулювати діями людей [540].

У політичній пропаганді ця техніка отримала чи не найширше застосування: навіть в країнах СНД все більше уваги надають ролі непрямої пропаганди: поле (свобода), дорога (асфальтована — символ змін), дім (тепло, єдність, злагода), дерево (українські архетипи калини, дуба) — ті символи, які часто виражають конкретну політичну ідею. Саме так виник відомий слоган "Наш дім — Росія" і плакат, де Чорномирдін склав долоні будинком (це придумав О.Ситников, керівник компанії "Имидж-контакт").

Так само врахували, що образ вогнища, міцного даху над головою лежить глибоко в підсвідомості кожної людини, і технологи Всеукраїнського об'єднання демократичних сил "*Злагода*", на логотипах якого часто по-дитячому намальовано будиночок і сонце. Постійно говорять про ідеальний символ яблука — в комерційній сфері у фірми "Apple", а в Росії — у партії "Яблуко" (щоправда, графічне зображення в останньої є вкрай непрофесійним — коло із ввіткнутим у нього трикутником). Отже, очевидно, що вдале застосування символів — як візуально, так і в мовних конструкціях дозволяє нав'язувати виборцям певні ідеї, підводити їх до конкретних дій.

Ще двома прикладами якірної технології є установка-твердження і ефект зв'язки, які застосовують як в промовах політиків, так і телевізійній рекламі майже повсюди. Установка-твердження — це подання якого-небудь твердження, з яким виборець погоджується навіть без аргументації. Через це радять кожну промову починати якою-небудь простою істиною — це налаштує реципієнта на позитивне сприйняття інформації, і надалі допомагає впливати на формування його думки.

В Україні типовим прикладом була телевізійна реклама партії "Демократичний союз", де стверджується, що держава має надавати громадянам засоби для захисту самих себе. Після цього просто називається партія, яку ніби й не рекламують, але опосередковано пов'язують з цією істиною — підсвідомо виборець погоджується з фактом "держави-захисника", і це погодження також прив'язується до Демсоюзу. Схожу істину декларувала Селянська партія України: "*Село — колиска України. О.Ткаченко*".

Ефект зв'язки використовує конкретні факти, події, щоб на їх фоні зробити реальним і можливим певне твердження. Так, в Росії першим викорис-

тав цю техніку в 1995 році С. Шахрай: його рекламний ролик складався з елементів чужих перемог: стартує Гагарін, хокеїсти перемагають. В Україні схожі методи використовувала Партія Зелених на виборах 1998 року. Часто ефект зв'язки використовують для антиреклами. Так, помістивши фотографію небажаного кандидата на одній сторінці з фотографією смітника, воєнних дій, а фотографію бажаного — поруч з фотографією красивого пейзажу, дитини, що усміхається, ми отримаємо досить стійкі підсвідомі образи цих людей [541].

Як бачимо, якорі є однією з найкращих і найпростіших технік НЛП — вони забезпечують чітке й оригінальне вираження складних політичних ідей, наближають їх до виборця, створюють ефект реальності (за рахунок нескладного візуального уявлення символу). Так само вони створюють цілісний імідж джерела інформації, дозволяють йому впливати на виборця, формулювати в нього позитивні чи негативні враження від реклами. Якорі — одна з найчастіше застосовуваних технік НЛП, чого часто навіть не уявляють автори вдалих логотипів, слоганів, плакатів.

Ще однією групою технік нейролінгвістичного програмування можна вважати так зване "використання особливостей людської підсвідомості". Сюди відноситься ціла низка методів, часто різних за спрямуванням, але таких, що їх завжди згадують, говорячи про НЛП (на відміну від символів, використання кольорів тощо). Саме завдяки їм НЛП отримало статус теорії маніпулювання людською свідомістю, хоча ці техніки досить рідко приносять очікуваний результат.

Лінія часу — доволі простий приклад застосування особливого сприйняття світу людською підсвідомістю, який можна пояснити з огляду на вже згадувані нами "ключі доступу через очі". Цю техніку згадують майже завжди, коли заходить мова про НЛП в політиці, очевидно, через її простоту і науковість. Справа в тім, що люди сприймають час лінійно, причому зліва знаходиться минуле, справа — майбутнє, посередині — сучасність. Через це логічно вважати, що фотографія рекламованого кандидата має проектуватися в майбутнє — знаходитися в правому верхньому куті плаката, обличчям дивитись в той бік. Якщо ж це зображення зробити кольоровим, то підсвідомість буде сприймати його як бажане майбутнє.

Цю техніку варто враховувати і в текстовій рекламі, яка так само повинна обіцяти майбутнє. Саме тому абсолютно неприйнятними є слогани на кшталт реклами російського "Яблука": "Наші батьки дивляться на нас з минулого". Має бути: "Наші діти дивляться на нас з майбутнього" [542].

Ще однією технікою є "лапки" (quotes) — паттерн, в якому повідомлення включається в цитату, яку нібито сказав хтось інший. Цим самим маскується маніпулювання, нав'язування думки. При цьому вигідно згадувати авторитетну думку, таку, що не потребує перевірки (ефект зв'язки). Також можна використовувати символічні лапки, що узагальнено згадують певний факт, як не надто важливий, але тим самим привертають до нього увагу.

Також технікою НЛП є "ілюзія вибору", яка так само маскує вплив на підсвідомість. Це досить проста методика, про вплив якої можна сперечатися. Її суть легко продемонструвати на прикладі: "Ви можете проголосувати за пана Х вранці чи ввечері". Вибір часу голосування є ілюзорним, оскільки має передумовою факт голосування.

Цікавою особливістю підсвідомості є те, що вона не сприймає частки "не". Цим часто користуються в статтях на замовлення, матеріалах, які нібито не несуть негативного аспекту (щоправда, частіше, не знаючи цієї техніки, самі ж кандидати шкодять собі). Зокрема, фраза "Неправда, що наш кандидат знаходився під карним розслідуванням" буде сприйматися як така, що обвинувачує.

Ця досить непоширена техніка є доволі невивченою і потребує додаткової уваги в плані виявлення можливої кількості негативної інформації, яка б не шкодила іміджеві політика.

І нарешті техніки, що послуговуються особливою здатністю підсвідомості до запам'ятовування, знаходження фактів.

Це можна продемонструвати і на прикладі 25-го кадру, який власне й орієнтується на підсвідомість. Але феномен sublimina – неправовий, в той час, як його відповідники у тексті чи промові – цілком дозволені та дієві. Так, можна вводити і виділяти в тексті окремі слова, які, окремо взяті і прочитані підсвідомістю, будуть формулювати установку. І навпаки, можна відволікати увагу від сенсу тексту, наприклад, просити порахувати, скільки в ньому літер "р". У цьому випадку значення речення лишається в підсвідомості, а людина ж звертає увагу головним чином на цікаву загадку.

Так само спрацьовують введені в текст чи зображення символи, яких свідомо людина не помічає. Найкраще в цьому плані спрацьовують архетипи, пов'язані зі статями, життям і смертю – так, часто в логотипах, слоганах застосовують слово "секс", зображення статевого акту, і якщо свідомо реципієнт просто сприймає текст, то його підсвідомість реагує на скриті символи, і встановлює стійкий якір на загальну інформацію.

Подальше використання цієї інформації (стимулу), наприклад, на виборчій дільниці може викликати транс, в якому реципієнтом можна буде маніпулювати. Щоправда, знову ж таки – перевірити цей факт науково складно, тому стверджувати однозначно, що саме конкретна техніка НЛП привела політика до влади, не можна.

Отже, розглянуто основні методи, які застосовуються в політичному дискурсі, і які прийнято групувати під назвою нейролінгвістичного програмування. В країнах Європи ці техніки вже давно стали елементами демократичних виборів будь-якого рівня, їх використовують поряд з іншими методами пропаганди та агітації.

Натомість країни пострадянського простору звертаються до них, як до засобів нав'язування тоталітарної політичної культури – вважається, що "безумовна ефективність" цих технік може підтримати існуючі режими, сприяє

найгіршій формі макіавеллізму, коли неправові методи маніпулювання є, навіть, бажанішими, ніж правові. Проте, створений міф про НЛП навряд чи сприяє його дієвості – тому необхідно підкреслити, що тільки в поєднанні з іншими засобами нейролінгвістичне програмування може істотно впливати на хід політичного процесу.

4.6. Мас-медійний ресурс іміджу України як фактор національної інформаційної безпеки

Вихід суперечливої за змістом інформації – загроза інформаційній безпеці України. Під час соціологічного опитування Українським центром економічних і політичних досліджень експертам було запропоновано оцінити рівень загроз інформаційній безпеці України. 62% експертів оцінили як високий рівень і 24% як середній рівень загрози "створення негативного іміджу України на міжнародній арені внаслідок неефективної інформаційної політики" [543]. Думається, така одноголосність експертів невипадкова, оскільки імідж держави сьогодні – важливий фактор формування її відносин з різними міжнародними акторами як у сфері політики, так і економіки. Мати сприятливі стартові умови для розвитку міжнародного співробітництва вже недостатньо. Необхідно володіти інструментарієм , який дозволяє подавати існуючий образ країни в позитивному ракурсі. Саме те, як вона сприймається, є основою для формування зовнішньополітичних і економічних відносин зі світовим співтовариством, механізмом регулювання внутрішніх процесів [544]. А тому ігнорування факту існування, скажемо так, не завжди позитивного іміджу України – це недооцінка загрози безпеці держави.

Як показує практика, сьогодні *українською державою* вже багато зроблено в напрямку оптимізації її інформаційної політики та діяльності. Проте серед інших невирішених проблем, що стосуються формування позитивного сприйняття України у внутрішньому та зовнішньому інформаційних просторах, залишається, на наш погляд, проблема подолання інформаційних загроз, пов'язаних з виходом суперечливої за своїм змістом інформації із зовнішньополітичних відомств і з вуст посадових осіб, що представляють Україну на міжнародних форумах.

Розуміння цього існує не лише в політичних та наукових колах, але і серед пересічних громадян, яким іноді стає соромно за українських політиків і державних діячів, котрі "*виносять сміття з хати*", продовжуючи дискутувати зі своїми "внутрішніми" опонентами на високих міжнародних форумах і трибунах, під час інтерв'ю зарубіжним засобам міжнародної інформації.

Аналізуючи подібну ситуацію в Росії, К. Хачатуров підкреслює, що турбота про репутацію держави починається з порога власного будинку. Він наводить досить слушне в зазначеному контексті висловлювання одного з зарубіжних послів: "плюралізм аж до рукоприкладства, – тільки у власному бу-

динку, в іноземній аудиторії – солідарна підтримка позицій Вітчизни" [545]. Зрозуміло, доки державні та політичні діячі не навчаться зважувати кожне своє слово, опинившись на міжнародній трибуні, важко буде сформувати позитивний імідж держави, а тому буде залишатися загроза інформаційній безпеці Україні. Але і цього, на нашу думку, не достатньо. Покладатися лише на вихованість та свідомість політичних та державних діячів, їх відповідальне ставлення до своїх представницьких функцій не можна хоча би тому, що залишаються ще численні засоби масової інформації та журналісти, від котрих стриманості та дипломатичності очікувати не доводиться.

У державі повинний існувати спеціальний механізм попередження та регулювання витоку несприятливої для іміджу країни інформації. У першу чергу, сама держава повинна турбуватися про запобігання витоку суперечливих повідомлень як від представників держави, так і від журналістів. Може здаватися, що вирішити дану проблему неможливо: як кажуть, на кожний роток не накинеш хусточку, до кожного журналіста не приставиш контролера чи спостерігача. Проте, думається, це не зовсім так: світова практика показує, що ця сфера, хоча і не без зусиль, але регулюванню піддається.

Держава повинна не лише встановлювати порядок визначення та упорядкування діяльності з таємною інформацією (у цьому напрямку вже досить багато зроблено), але і здійснювати демократичний контроль над поширенням нетаємної інформації. І це не заклик повернутися до цензури чи якихось законодавчих обмежень. На наш погляд, свободу доступу та поширення інформації повинний супроводжувати контроль за засобами масової інформації і комунікації, які в наш час комерціалізовані, монополізовані та дуже часто виражають інтереси їхніх власників, а не інтереси суспільства. Абсолютної свободи інформації ніколи не було і не буде. Лише гармонійна рівновага між свободою та контролем дозволять забезпечити консенсус у суспільстві та захистити національно-державні інтереси, яким загрожує безсистемне та неконтрольоване поширення інформації щодо країни, її державних органів, їх політики та діяльності у національному та міжнародному інформаційному просторі.

Спіндокторство та його роль у здійсненні контролю за змістом та поширенням інформації. Досвід інших країн свідчить, що збалансування свободи інформації та контролю за нею, державне регулювання витоку інформації із державних установ та від посадових осіб, що уособлюють владні рішення та позиції, здійснюється за допомогою менеджменту новин, який дозволяє керувати процесом комунікацій через посередництво новин, які відображають зацікавленість громадської думки тими чи іншими проблемами.

Як зазначають американські дослідники, те, що в урядових колах називають управлінням новинами, – справа більш, ніж складна, оскільки органічно пов'язана з формуванням та змінами громадської думки, яка дуже чутлива до замовчування, неправди чи брехні. Можна певний час обманювати всіх людей, – у свій час говорив А. Лінкольн, – можна весь час обманювати

певну частину людей, проте не можна всіх людей обманювати весь час [546]. Це висловлювання видатного політика стосувалося зв'язків з громадськістю (хоча термін, добре відомий нам зараз, тоді ще не мав сучасного змісту), але повною мірою воно може бути віднесено і до менеджменту новин, які є невід'ємною важливою складовою частиною комунікацій з громадськістю .

На думку деяких дослідників, управління новинами в державному секторі часто стає єдино доступним інструментарієм, який не асоціюється з маніпулятивними технологіями. Особливе значення менеджмент новин має в кризових ситуаціях, оскільки спрямований на прийняття правильної лінії роботи зі ЗМІ та дає можливість максимально вплинути на те, яка інформація про державну структуру та її діяльність з'явиться в засобах масової інформації. У зв'язку з тим, що новини є відображенням інтересу громадської думки до того чи іншого питання, управління новинами і стає тим інструментарієм, який дає можливість ввести елементи управління в сферу, яка здавалось би не піддається управлінню [547].

Менеджер новин має справи не з подіями безпосередньо, а з їх відображенням в громадській думці та висвітленням у засобах масової інформації новин, що інформують про ці події. Необхідність втручання в комунікаційний процес зумовлена тим, що подія та її висвітлення (певна новина) – це два різні об'єкти, які можуть і не збігатися. Для ефективного впливу на громадську думку варто організовувати як перше, так і друге, ретельно відбираючи події та акцентуючи увагу на найбільш значущих новинах. Тому управління новинами має два основні аспекти: підготовка очікувань громадськості щодо певної події (а тому і новини) та виправлення незадовільного висвітлення події засобами масової інформації.

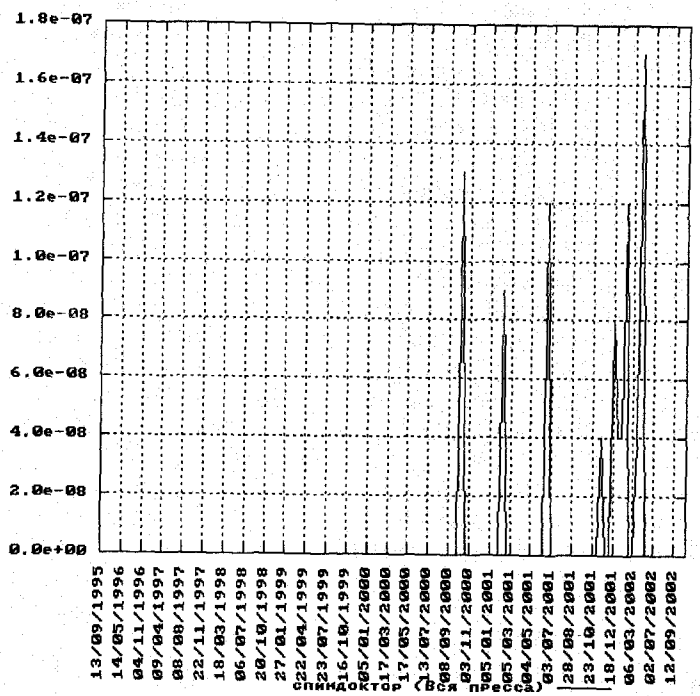
Основні завдання, що вирішуються менеджментом новин, пов'язані:

- по-перше, з передбаченням реакцій та оцінок щодо події, яка планується або очікується;
- по-друге, зі змінами очікувань щодо події, яка міститься в основі тієї чи іншої новини;
- по-третє, зі змінами сприйняття новин, які інтерпретуються в небажаному для того чи іншого суб'єкта комунікації напрямі.

Поряд з поняттями "управління новинами" або "менеджмент новин" застосовують термін "спіндокторство"[1] (spin doctoring). Слово "*spin*" перекладається українською мовою як "*вертіння, крутіння*", означаючи в теорії комунікації та паблік рилейшнз подання подій у більш сприятливому вигляді, своєрідне "лікування події".

Ця діяльність доволі поширилась в останні роки і відноситься до людей, які спеціалізуються на висвітленні у позитивному світлі компаній або політичних структур в засобах масової інформації [548]. У той же час спіндокторство як явище не є відкриттям двадцятого століття. Воно виникло набагато раніше, задовго до того, як з'явилися засоби масової інформації. Фахівці вважають, що діяльність, подібна до функцій спіндоктора, мала місце в різних країнах

світу, а як професійна діяльність уперше оформилася в паризькій опері в 1820 році, коли був створений феномен "*клаки*", де товаром стали оплески [549].



Термін "спіндоктор" у західній науці та практиці також існує досить давно, на теренах же колишнього СРСР він з'явився лише на рубежі тисячоліття, про що наочно свідчить показник вживання та поширеності даної словоформи в засобах масової інформації Росії – прес-індекс[III], показаний на малюнку 1. На жаль, у нас поки що відсутні подібні бази даних, щоб виявити такий кількісний показник застосування даної словоформи в українських виданнях. Проте, на наш погляд, ситуація у нас подібна до російської, тим більше, що цей термін частіше за все застосовується в російськомовних чи російських публікаціях Г. Почепцова або посиланнях на них. Поняття "спіндоктор" також з'являється в рекламних оголошеннях PR-фірм і агентств, що пропонують відповідні послуги, називається серед інших спеціалізацій діяльності в галузі паблік рилейшнз.

Досвід інших країн у застосуванні менеджменту новин як засобу контролю інформації. Значний досвід у галузі спінопераций, спрямованих на ко-

ректування чи покращення іміджу різних соціальних суб'єктів, на думку вчених, мають Сполучені Штати, де управління новинами, хоча і неоднозначно оцінюється, але практикується і в комерційній, і в політичній сфері.

Дослідники говорять, наприклад, про зростання важливості застосування технологій спіндокторства в управлінні іміджем сучасних фінансових компаній, що зумовлене міцними зв'язками PR з керівництвом, яке витрачає тепер на комунікації 30-40% свого часу, зростанням тиску на керівників різних рівнів з боку груп інтересів і акціонерів, збільшенням онлайнових засобів масової інформації та уваги журналістів до фінансових новин. Все це потребує, на їх думку, послідовної і ретельної підготовки текстів виступів керівників, прес-релізів та інформаційних повідомлень, які не повинні містити суперечливої інформації і неточностей [550].

Особливо великий досвід у застосуванні менеджменту новин мають державні установи США: Білий дім, Конгрес, Пентагон. Їх служби паблік рилейшнз професійно готують громадську думку, інтерпретують події та факти таким чином, щоб вони мінімально шкодили іміджу країни та іміджу державних посадових осіб. Спіндоктори Білого Дому працюють так, щоб імідж президента мав привабливий вигляд дієздатного політика. Вони застосовують різні методи та прийоми для того, щоб у ЗМІ діяльність президента та його команди висвітлювалася так, як це потрібно урядовцям. А в разі виникнення небажаних інтерпретацій та розуміння тих чи інших подій вносяться необхідні корективи, і новини щодо Білого дому підправляються, коректуються в бажаному напрямі [551].

Спіндокторства потребує не тільки управління іміджем президента, а і іміджем Конгресу та парламентарів, що робити дещо складніше, оскільки президент один, а парламент – структура децентралізована, має десятки комітетів і підкомітетів. У той же час відносини між парламентарями та журналістами більш "теплі", тоді як між виконавської владою та ЗМІ вони були ускладнені традиційною ворожнечею виконавчою та законодавчою гілок влади. На думку Р. Д. Курза, існує "*фундаментальний контраст*", між "*презумпцією відкритості*" децентралізованого Конгресу й "презумпцією таємниці", що переважає в ієрархічній системі виконавчої влади. Ця розбіжність має тенденцію створювати тенденцію до природного союзу між законодавцями й журналістами: вони разом використовують спільну конкуренцію проти виконавчої гілки влади.

Робота з іміджем передбачає не лише організацію та реагування на внутрішні, а і на зовнішні новини, оскільки, як зазначають американські дослідники, "новини за кордоном звичайно стають новинами в Сполучених Штатах, особливо коли це стосується американських інтересів". Саме тому, навіть, повідомлення в невеликій зарубіжній газеті може впливати на тих, хто робить політику США. Феномен "*медіалізму*" ("medialism") продукує великі потоки все менш і менш фільтрованої інформації, що перетинають національні кордони. Зарубіжні лідери можуть апелювати безпосередньо до

виборчих округів інших країн: слова використовуються, щоб забезпечити "спін", який зламає існуючий політичний режим.

Безумовно, Білий дім присвячує багато часу й енергії керуванню відносинам із засобами масової інформації. Сприятливий президентський імідж у громадській думці ґрунтується на позитивному іміджі, що створюється ЗМІ. Ще за правління Рейгана Білий дім розвив відносини з пресою до рівня мистецтва. Одержання сприятливого щоденного "спіна" і здійснення "менеджменту новин" стало турботою, якщо не нав'язливою ідеєю, а репортери часто конкурують за добре ставлення Білого дому, щоб одержати доступ до могутніх посадових осіб і здаватися успішними своїм редакторам [552].

Не менш успішно забезпечується вирішення зазначеної проблеми інформаційної безпеки за допомогою менеджменту новин урядовими структурами Великої Британії. Як зазначає К. Хемпсон, урядова система паблік рилейшнз цієї країни виконує два основні завдання: перше пов'язане з реалізацією права суспільства на отримання достовірної інформації щодо діяльності влади, друге — із побудовою іміджу влади та формуванням позитивної думки щодо її діяльності. Для цього створена система підрозділів (вона представлена на малюнку 2), деякі з яких виконують функції управління новинами.

Основою урядових паблік рилейшнз Великої Британії є Комітет стратегічних комунікацій — КСК (Strategic Communication Unit), до складу якого входять директори 12 регіональних відділів інформації, особисті секретарі *кожного міністра та шість представників різних партій*. КСК *вирішує*, яку саме інформацію уряд повинний надати населенню. Щоранку, під керівництвом прес-секретаря Прем'єр-міністра, члени КСК отримують інформацію з Комітету моніторингу ЗМІ, аналізують, що говорять про уряд і вирішують, яким чином на це реагувати. Щотижня проводяться соціологічні опитування за допомогою фокус-груп, результати яких щопонеділка обговорюються в КСК. Із врахуванням цих результатів здійснюється пошук "фактів-убивць"("killer facts"), оприлюднення яких покращило б уявлення про роботу уряду. Було навіть створено спеціалізований дослідницький підрозділ, метою якого і стала така пошукова діяльність. Знайдені факти спрямовуються в "мережу знань" для поширення серед членів уряду чи парламенту (вони мають пейджер, на який направляється необхідна інформація).

КСК виконує ще одну дуже важливу в контексті зазначеної проблеми функцію: жодна інформація, що стосується урядової політики, навіть та, що виходить від директора з інформації будь-якого міністерства, не може бути опублікована буз узгодження стилю та часу публікації з КСК. Це здійснюється за допомогою спеціального відділу та спеціального комп'ютера, котрий називається *"Порядок денний"* ("Agenda") та встановлює графік публікації урядових повідомлень. Усі департаменти повинні домовлятися з відділом про час оприлюднення своєї інформації, щоб більш важливі повідомлення не перекривалися менш важливими.

Ще одним важливим елементом системи управління новинами є "комп'ютер швидкого реагування", на якому створена база даних, яка поповнюється щодня. У ній є всілякі висловлювання на різні теми, що стосуються політики, державних та політичних діячів, журналістів газет і телебачення. У лічені хвилини при необхідності можна знайти "компромат" на опонента влади (його висловлювання на дану тему) та аргументи на захист певної позиції владних структур чи державних діячів. Цей комп'ютер зв'язаний з урядовими департаментами в регіонах та Центральним бюро інформації та його регіональними відділами.

Особливе місце в структурі КСК займає відділ спічрайтерів, які готують промови для міністрів або пишуть статті, що друкуються за підписом Прем'єр-міністра або міністра, а також відділ спіндокторів (4-6 чоловік), які надають урядову інформацію в засоби масової інформації під найбільш вигідним кутом зору.

Оскільки виникають ситуації, коли в засоби масової інформації все ж таки попадає інформація, що може бути небезпечною для національних інтересів, уряд наділений повноваженнями (так звана Директива "Д") заборонити газетам її друкувати. І хоча зараз, як зазначає К.Хемпсон, вона фактично не використовується, оскільки уряд бажає виглядати демократичним і не тиснути на пресу, раніше вона застосовувалася у випадках витоку інформації, коли про це повідомляли спецслужби [553].

Технологія спіндокторства. На думку російського PR-фахівця А.Н. Чумікова, управління інформацією має два аспекти. Перший передбачає пряме чи опосередковане управління безпосередньо засобами масової інформації – наприклад, за допомогою лібералізації або делібералізації механізмів реєстрації ЗМІ, контролю за змістом ЗМІ з боку органів влади, повне фінансування або певні фінансові дотації, розширення чи звуження можливостей для отримання необхідної інформації. Другий пов'язаний з управлінням інформацією як такою [554]. Г.Л. Тульчицький зазначає, що управління новинами – "вищий пілотаж" роботи зі ЗМІ, коли акцент фактично переноситься з інтерпретації новин і подій на створення самих подій. Він вважає, що менеджер новин не стільки впливає на журналістів, скільки на факти, їм доступні [555].

Менеджмент новин – це галузь PR-діяльності, пов'язана з управлінням "новинно-подієвим" простором – процесами формування новин та їх висвітлення у засобах масової інформації.

Технологія управління новинами містить декілька основних операцій. По-перше, це планування події (її передбачення, прогнозування), відбір події. Спіндоктор, аналізуючи можливі події в найближчий період або в перспективі, визначає ті, які можуть бути вигідними для іміджу країни, державного інституту чи політичного або державного діяча, які – можуть нашкодити їм. Він вирішує, чи можна задовольнитися спонтанними подіями, чи варто підготувати спеціальну подію, на фоні якої певний суб'єкт буде виглядати приваб-

ливіше. Така підготовча робота може забезпечувати необхідні новини щодо будь-якої організації чи установи, а значить і щодо країни та держаних інституцій. Фактично всі подієві комунікації або, як їх ще називають, "поставлені події" стають основою майбутніх новин, причому таких, які потрібні у конкретний час. Зрозуміло, що складніше передбачити і спланувати спонтанні події. Але це цілком реальне завдання. Наприклад, святкові дати, планові заходи в громадському житті (*День міста, історичні дати міста*), усім відомий графік підготовки до виборів або акцій міжнародних організацій тощо можуть стати основою для створення планових новин, якщо служба паблік рилейшнз, наприклад, обласної чи міської державної адміністрації запропонує організації спосіб, як "вписатися" в них. Це може бути і спонсорство, пов'язане з цими подіями, і виставка чи конкурс, приурочені їм, і зустрічі з громадськістю (збори, виступи керівників), і дні відкритих дверей, і рекорди, встановлені напередодні "обраних" подій, і нагороди, і, навіть, особисті події (річниця діяльності працівника і т.п.).

По-друге, це підготовка події. Визначивши необхідність створення події або передбачивши її перспективність із погляду програми пабліситі державної установи чи політичної організації, спіндоктор готує її появу як новину для громадськості. Перш за все, тут йдеться про безпосередню підготовку, яка здійснюється за принципами і правилами підготовки подієвих комунікацій. Спіндоктор займається постановкою події відповідно до обраної ним стратегії. Прикладом такої постановки можуть бути репетиції керівників або політичних лідерів перед виступами на радіо, телебаченні, зборах, прес-конференціях, розробка сценарію події, гасел і так званих "звукових цитат" щодо події, яка готується, обрання фону, який зможе впливати на інтерпретацію події, і навіть попередня підготовка запитань та передача їх журналістам, яким довіряють і які будуть брати участь у прес-конференції.

З іншого боку, підготовка події як основи майбутніх новин, пов'язана з управлінням очікуванням подій, що спрямоване на надання новинам певної значущості. Вирішення цього завдання пов'язане з "*інформаційною обробкою*" громадськості та розставленням необхідних інформаційних акцентів. Наприклад, фактично в усіх країнах здійснюється управління очікуванням таких подій, як візити іноземних державних делегацій. Інформація, що поширюється напередодні візитів, як правило, містить відомості про країну, її зовнішню та внутрішню політику, особу державного лідера, взаємовідносини з країною відвідування та іншими державами, перспективи розвитку співробітництва тощо. При цьому керуються відомою максимою: "Візит, якого не помітила преса, не відбувся". Аналогічно потребують позиціонування й інші події державного значення, без чого вони можуть або залишитися "непомітними", або будуть висвітлюватися новинами, що не сприяють зміцненню позитивного іміджу. Управління очікуваннями не слід розглядати як маніпулятивні технології. Вони, на наш погляд, як раз дозволяють реалізувати той самий демократичний контроль за інформацією, про який йшлося

раніше. Як зазначають фахівці, американці, наприклад, залучають до виконання таких завдань осіб, які користуються повагою та авторитетом у рамках конкретного інформаційного простору і здатні підтримати плани адміністрації. Відмінності демократичної схеми управління громадської свідомістю, на думку Е. Тарашвілі, полягають, перш за все, в контролі окремих ситуацій та позитивній орієнтації на "витискування" одної, небажаної, події іншою, більш сприятливою для формування іміджу того чи іншого соціального або політичного суб'єкта [547].

Важливою складовою менеджменту новин є висвітлення події. На відміну від журналіста, для якого метою комунікації є власне новина, для спіндоктора, на перше місце виходить управління її розвитком, яке передбачає гальмування новин, прискорення їх поширення, продовження життя новин. Гальмування новин може здійснюватися різними шляхами, зокрема: недопущенням події в мас-медіа, змінами модусу події, зміщенням акцентів тощо. Прискорення поширення новин можливе за допомогою такого інструментарію, як розповідь про подію в багатьох ЗМІ, акцент на її важливість у приєднанні до іншої важливої події, використання коментарів. Продовження життя події (і відповідно новини, що пов'язана з нею) здійснюється за допомогою неодноразового повторення новини, спеціально сконструйованого циклу проходження новин тощо.

На думку фахівців, важливе значення у вирішенні проблеми висвітлення новин під певним кутом зору грає такий принцип організації PR-діяльності, як координація роботи. Зазначають, що особливо наочно дію цього принципу можна прослідкувати на практиці англійської та американської школи державного паблік рилейшнз. Тут інформаційні служби ретельно піклуються про те, щоб у повідомленнях державних структур не було суперечностей та розбіжностей з того чи іншого приводу, узгоджується робота всіх підрозділів та регіональних інформаційних агентств, що працюють на позитивний імідж держави, застосовують досить різні форми роботи, зокрема наради з керівниками прес-бюро, PR-агентами, щотижневі брифінги для акредитованих журналістів (*"запис без камер"*), телефонні прес-конференції керівників прес-служб провідних держдепартаментів, на яких чітко розподіляється, хто буде давати відповіді на запитання журналістів з актуальної проблематики тощо. Дещо інша ситуація в Росії, де, за висновками російських спеціалістів, в організації висвітлення роботи органів, особливо регіонального управління присутня спонтанність, поверхневість, "компанійщина" [556], думається, що і в нас у цій галузі ще досить багато проблем, які потрібно вирішувати.

Як наслідок неспрацьованості державних інформаційних служб або непрофесіоналізму окремих державних та політичних діячів нерідко з'являється інформація, що негативно впливає на їх імідж. А це потребує виправлення помилок та несприятливого сприйняття новин громадськістю. Вирішення цього завдання пов'язане з іншою інтерпретацією новини, ніж та, яка мала місце під час події (наприклад, у промові керівника), роз'ясненням позиції, під час якої

уточнюються, коректуються аспекти, які не задовольнили громадськість. Зрозуміло, більш ефективним є не виправлення помилок та несприятливого ставлення, а їх профілактика, запобігання. Цілу низку прийомів такої профілактики виробили західні спіндоктори, які працюють у політичній сфері. Серед них такі: "пробні шари"; "диригування комунікацією"; монополізація інформації; "пакетування" негативних новин; пряма комунікація; створення кола "довірених" журналістів; підготовка такої комунікації, яка б не допускала журналістської диктатури; прес-тури тощо.

Таким чином, враховуючи те, що концепція інформаційної безпеки держави передбачає необхідність попередження поширення несприятливої інформації про державу та її діяльність всередині країни та за рубежем, державні структури повинні не лише всіляко сприяти формуванню навколо себе відкритого та прозорого інформаційного простору, а і забезпечувати власний інформаційний потік, який повинен бути контрольованим та керованим, щоб запобігати інформаційним загрозам, пов'язаним з появою у засобах масової інформації суперечливої за змістом та несприятливої для іміджу країни інформації

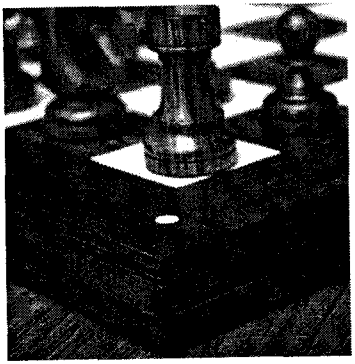
Примітки

I Одним із перших в Україні ввів у науковий обіг поняття "спіндоктор" та "спіндокторство" професор Г.Почепцов.

II Клака (франц. claque), група підставних глядачів — клакерів, найманих для створення штучного успіху або провалу артиста або цілого спектаклю.

III Прес-індекс – один з інструментів аналізу, система побудови графіків вживання словоформ. Система розбиває весь масив, що зберігається в даний момент у архіві Національної Електронної Бібліотеці (НЕБ), де представлені російськомовні ЗМІК практично з усіх регіонів Росії, країн СНД, Балтії і далекого зарубіжжя, на вибірки заданого обсягу, по кожній з яких будується частотний словник відповідного тимчасового періоду. Зміни частот використання визначених словоформ відображаються на графіку. Щодня кілька тисяч журналістів демонструють у своїх статтях популярність тих чи інших слів. Аналізуючи масив НЕБ (сьогодні це більш 4.000.000 документів, приблизно 1,2 млрд. слів), можна одержати представлення про зміну числа статей, що відповідають зазначеним критеріям, словниковому оточенні заданих слів, частоті використання словоформ.

АНТОЛОГІЯ



Андреев А., Давыдович С.

ОБ ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ В ХОДЕ ВООРУЖЕННОГО КОНФЛИКТА В КОСОВО

Одним из наиболее характерных и показательных примеров использования СМИ в интересах оказания воздействия на войска и население противника является агрессия НАТО против Югославии в 1999 году. Практика проведения информационного воздействия в ходе этого конфликта настолько разнообразна, что на протяжении последующих десятилетий будет основным источником анализа и изучения специалистов в области информационной войны (ИВ).

Освещение конфликта в Косово СМИ стран НАТО. Принципиальные направления содержания информационно-психологическою обеспечения военной акции против Югославии, а также общие планы ведения ИВ и психологические операции были согласованы и утверждены высшим руководством США и других ведущих стран НАТО еще на этапе принятия решения о начале агрессии против этого независимого государства.

Информационно-психологическая подготовка к вооруженному вмешательству НАТО в Косово началась в 1998 году. В западных СМИ было инициировано поэтапное нагнетание антисербской истерии и муссирование темы «этических чисток» в Косово. Результатом регулярной демонстрации на телеэкранах, страницах газет и журналов «сербских зверств» и «страдании албанского народа» стало то, что уже к концу 1998-го — началу 1999 года общественное мнение Запада было в основном подготовлено к силовому варианту урегулирования косовской проблемы. Опросы общественного мнения, проведенные накануне войны и странах НАТО показали, что воздушные удары по СРЮ готовы поддержать 55-70 проц. населения этих государств.

Основные цели информационного обеспечения натовской агрессии на стратегическом уровне с самого начала заключались в формировании позитивного для США и НАТО на Балканах внутреннею (в странах самого альянса) и международного общественного мнения н нейтрализации влияния России, Китая и других стран, занявших негативную позицию в отношении действий Североатлантического союза. На оперативно-тактическом уровне цели *информационной кампании* сводились к дестабилизации внутриполитической обстановки в СРЮ, дискредитации правительства С. Милошевича в глазах собственного народа и дезорганизации системы государственного управления, деморализации населения и личного состава югославских вооруженных сил, склонению к дезертирству и неповиновению, поощрению оппозиционных властям СРЮ организаций, политических деятелей и СМИ.

В содержании информационною обеспечения агрессии НАТО против Югославии на протяжении всей операции доминировали следующие основные направления: разъяснение «гуманных» целей военной акции, предпри-

нятой якобы только но имя «благородных целей» спасения косовских албанцев от «геноцида» и их «безопасного возвращения к родным очагам»: убеждение мировой общественности в том, что только НАТО (а не ООН или ОБСП) может быть адептом мира и стабильности на Балканах и во всем мире, в необходимости и размещения и Косово международного военного контингента под эгидой НАТО; демонстрация «монолитного единства» стран блока и военной мощи альянса.

Между тем отдавший приказ бомбить Югославию президент США Б. Клинтон признался, что большинство американцев даже не могли отыскать Косово на карте, им не было особенно интересно, что можно и нужно делать в этом регионе. К моменту начала авиационных ударов у значительной части американскою населения был сформирован образ сербов и Югославии. В американской печати публиковалось большое количество исторических статей об этой стране, в которых сербы были представлены как агрессоры и поработители соседних народов.

Таким образом, анализ материалов западных СМИ за период подготовки операции НАТО против Югославии позволяет сделать вывод, что теле- и радиокомпании, газеты и даже сеть Интернет широко использовались для проведения беспрецедентной по своим масштабам информационной кампании. Необходимо отметить. что они отличалась также большим количеством недостоверных фактов, а порой и откровенной ложью. Главной целью являлось побудить мировое общественное мнение если не к поддержке, то, но крайней мере, к тому, чтобы оно не препятствовало вооруженному вторжению НАТО на Балканы. Основными каналами распространения подобной информации являлись такие издания. как влиятельная американская газета «Вашингтон пост», теле- и радиокомпания Си-эн-эн, английские журналы «Тайме» и «Экономист», компания Би-би-си и немецкая газета «Ди Вельт». При этом упор был сделан на проблему этнических албанцев в Косово, где обстановка действительно была далека от благополучной.

Однако, оценивая информационные сообщения по данной проблеме, можно говорить даже не о субъективности подхода, а о преднамеренной дезинформации, направленной на решение следующих задач:

- Дискредитация в глазах мировой общественности военно-политического руководства СРЮ, и в частности президента С. Милошевича. С этой целью в СМИ часто распространялись сообщения с критикой в его адрес самого разного характера от обвинений в «политике шовинизма» и организации этнических чисток до неспособности управлять экономикой страны.
- Создание отрицательною имиджа сербских властей и населения. Одно за другим появлялись сообщения о неоправданной жестокости правительственных войск по отношению как к военнопленным, так и к мирным албанцам. Широкую известность получил случай в селе Рачак, где, но заявлению главы миссии ОВСЕ американца С. Уокера, правительст-

венные войска учинили кровавую расправу над албанцами. Сюда же следует отнести и так называемые «концлагеря», устроенные сербами для албанцев.

- Формирование положительного образа косовских албанцев, что было довольно сложной задачей. Так, общепризнанными стали факты торговли албанской диаспорой наркотиками. Кроме того, необходимо было оставить «пространство для маневра», ведь в случае ввода миротворческою контингента НАТО нужно было контролировать обе стороны, а от албанцев можно было ожидать любых непредвиденных шагов. Таким образом, появлялись статьи и передачи, подчеркивавшие, в первую очередь, гордый и независимый характер албанцев, которые отстаивают свою независимость и, самое главное, в отличие от сербов, готовы решать вопросы путем переговоров.
- Создание иллюзии легитимности требований сепаратистов. Такой эффект достигалсяся как чисто лексическими средствами, например путем многократного употребления словосочетаний типа «демократические требования албанцев» и «право на самоопределение», так и с помощью замалчивания множества фактов, имеющих определяющее значение с точки зрения международного права. В частности, ничего не говорилось о том, что все члены «Освободительной армии Косово» (ОАК), с которой вели переговоры международные организации, согласно закону любого государства являлись преступниками и подлежали суду как минимум за участие в незаконных вооруженных формированиях.
- Преувеличение «гуманитарной катастрофы» в Косово и обоснование вмешательства мировой общественности. Огромное количество материалов было посвящено рассказам о том, в каком бедственном положении находились этнические албанцы. При этом мало кто догадывался, что зачастую под видом «угнетаемых албанцев» в кадрах репортажей были засняты сербы.

С началом воздушных ударов интенсивность информационно-пропагандистских мероприятий, направленных против СРЮ, заметно усилилась. Выступления руководителей ведущих стран НАТО с разъяснениями и оправданиями военной акции против Югославии транслировались на всех основных языках мира и сербском через всемирные теле- и радиослужбы. Госсекретарь США М. Олбрайт по спутниковым телеканалам за период воздушной кампании дважды обращалась к населению Югославии па сербском языке.

Важнейшим инструментом информационной войны против СРЮ стала пресс-служба НАТО. В задачи этой структуры входит анализ сообщений западных, югославских и международных СМИ о ситуации на Балканах и выработке рекомендаций для руководства альянса по определению обшей стратегии в отношении освещения в этих средствах хода военных операций, подготовка информационных материалов для пресс-конференций, брифингов и пресс-релизов штаб квартиры НАТО. Четко управляя журналистским корпу-

сом, официальные структуры альянса в то же время исключительно жестко реагировали на попытки некоторых репортеров довести до западною общественного мнения точку зрения югославской стороны.

По общему убеждению, отношение американского общества к проблеме Косово в первые дни войны в Югославии формировалось исключительно СМИ США, и прежде всего телевидением, возможности которого в наши дни позволяют создавать иллюзию непосредственного участия в происходящем на другом конце планеты. Характерна динамика поддержки американцами участия сухопутных войск в операции па Балканах: с 47 проц. она выросла сначала до 57, затем до 65 проц., а последний опрос установил, что 71 проц. респондентов выступал за применение наземных войск для отстранения от власти С. Милошевича и предания ею суду как военного преступника, поскольку «на Соединенных Штатах лежит ответственность за установление мира в Косово».

При проведении бомбардировок Югославии президенту Клинтону было необходимо, в первую очередь, убедить американскую нацию в том, что операция на Балканах необходима. В этих целях был проведен ряд информационно-психологических мероприятий по дискредитации военно-политического руководства Югославии, а также возможных тенденций в мире по поддержке позиции Югославии. Во время своих выступлений госсекретарь США М. Олбрайт постоянно использовала метод навешивания ярлыков. Она даже сравнила события в Косово с истреблением фашистами евреев в годы Второй мировой войны. В интервью газете «Вашингтон пост» она заявила, что глубоко убеждена: «Гитлера и других тиранов можно было остановить, если бы им было оказано сопротивление с самого начала». Именно с этой точки зрения она всегда смотрела на Югославию.

С началом бомбардировок рассказы о зверствах в Косово приняли еще более масштабный характер, несмотря на то что в СРЮ уже не осталось американских (за исключением Си-эн-эн) корреспондентов. Все жуткие истории о расстрелянных и сожженных заживо в собственных домах передавались со слов беженцев, охваченных паникой, заслуживающих безграничного сочувствия, но не обязательно доверия (что является нарушением американских журналистских стандартов, требующих информации из первых рук). Так, в сознании американцев С. Милошевич стал ассоциироваться с Гитлером. Один из известных американских журналистов уверенно заявил: «Для сербов ненависть это профессия, жалость к себе, ощущение себя жертвой — национальные свойства сербов».

Несмотря на общую антисербскую риторику в СМИ США, в целях создания «объективности» некоторых сербских представителей охотно притащили на американское телевидение. Кроме того, на одном из каналов каждый день транслировали с английским переводом выпуски последних известий из Белграда, в которых НАТО клеймили как «фашистскую организацию», а его бомбы и самолеты именовались «злодейскими». Однако югославская пропаганда нейтрализовалась ежевечерними репортажами. в которых показывали

тысячи беженцев из Косово. В каждом таком репортаже можно было услышать ужасающие рассказы о перенесенных албанцами мучениях.

Одним из наиболее ярких примеров дезинформации в американских СМИ явился репортаж о «расстреле мирных албанцев в окрестностях села Рачак», снятый на любительскую камеру якобы одним из фермеров. Но никто: ни албанцы, ни эксперты — не мог объяснить, почему в овраге, где якобы сербская полиция расстреляла 45 гражданских лиц, не было обнаружено следов крови, а на одежде убитых — следов от пуль. Это явно свидетельствовало о том. что все тела привезли в овраг из других мест, а об их принадлежности к боевикам ОАК свидетельствовали следы пороха на руках. Уже после боя убитых переодели в гражданскую одежду. Несмотря на экспертизу международной комиссии, признавшей фальсификацию, многие средства массовой информации по-прежнему утверждали, будто сербы «учинили бойню в селе Рачак». В течение нескольких недель тиражировались сообщения о том, что сербская полиция расстреляла всех учителей одной из школ на глазах их учеников. Затем сообщалось о том, что в районе Приштины сербы устроили концлагеря, в которых «творятся злодеяния» против албанцев. В итоге западным СМИ пришлось признать, что все это «не подтвердилось», но опровержение было подано таким образом, что его практически никто не заметил.

В то же время информация западных СМИ не была однородной по своей направленности. В некоторые западные издания нередко поступали сведения, не совпадающие с общим вектором освещения конфликта, просачивалась информация и о боевых потерях НАТО. Так, греческая газета «Атинаики» па первой странице сообщила, что тела «первых 19 убитых американцев» доставлены из Македонии в Салоники, откуда они будут переправлены в США. Сообщалось. что тела «в строжайшей тайне и под усиленной охраной доставлены через Сконье в 424-й военный госпиталь» в г. Салоники для подготовки к дальнейшей транспортировке, причем «греческие власти утверждали, что им ничего об этом не известно». «Атинаики» утверждала, что США придерживались «закона молчания», как это бывало и ранее (во Вьетнаме и Ираке), чтобы сообщить о своих потерях позднее, в более подходящий момент.

Каждый раз, когда появлялась «неудобная» информация, американские официальные лица вели себя примерно одинаково: на первом этапе происходило официальное опровержение компрометирующего факта, в дальнейшем проводилась линия но обвинению югославской стороны в подготовке провокации. Такое имело место в случаях с гражданскими объектами в Югославии: с пассажирским поездом, с конвоем беженцев, уничтоженными самолетами НАТО. Признания правомерности подобных сообщений имело место лишь в том случае, если другая сторона приводила совершенно неопровержимые доказательства. Так произошло, например, со сбитыми самолетами НАТО. Признаны были лишь те случаи, когда югославам удалось предъявить обломки с опознавательными знаками, бортовыми номерами и маркировкой агрегатов сбитых машин.

Также неоднозначно освещалась проблема беженцев. Информация подавалась в таком виде, будто албанцам нравилось, когда НАТО бомбит города и деревни косовских албанцев. По сообщениям американских телекорреспондентов, из нескольких сотен тысяч беженцев ни один (именно так сообщалось в выпусках Си-эн-эн) не высказал недовольства бомбардировками. А пресс-секретарь НАТО Дж. Шеа на одной из пресс-конференций даже заявил, что «звук бомбардировщиков косовские албанцы сравнивали с «полетом ангелов».

После начала агрессии западные радиостанции резко увеличили объемы вещания на сербском, албанском, болгарском и македонском языках. Так «Голос Америки» н «Свободная Европа» организовали круглосуточное вещание на Югославию в УКВ-диапазоне с помощью трех передатчиков, расположенных в Боснии, Македонии и Венгрии. Позднее, в мае, США также добились от Румынии согласия на размещение на ее территории передатчиков «Голоса Америки», работающих в СВ- и УКВ-диапазонах. Радиостанция «Немецкая волна» развернула вещание на СРЮ на сербском языке в УКВ-(FM-) диапазоне. В свою очередь Би-би-си, помимо вещания на Югославию с использованием сети своих передатчиков на территории Албании, предоставила свои спутниковые каналы для ретрансляции на СРЮ материалов запрещенной оппозиционной радиостанции «В-92», переправлявшихся на Запад по каналам Интернет.

Не осталась без внимания и печатная пропаганда. В Македонии при финансово-технической помощи Франции и Великобритании был налажен выпуск ежедневной газеты «Коха диторэ» для косовских албанцев тиражом 10 тыс. экземпляров. В апреле руководство государственных радиовещательных служб США («Голос Америки»), Великобритании (Би-би-си), ФРГ («Немецкая волна») и Франции («Международное радио Франции») договорились о координации своего вещания на Балканах на сербском и албанском языках и создании по периметру СРЮ единой сети СВ- и УКВ-передатчиков и ретрансляторов, работающих на частотах югославского государственною радио.

Важнейшим инструментом информационной войны против СРЮ стала пресс-служба НАТО в Брюсселе во главе с представителем Великобритании Дж. Шеа. После начала боевых действий штат пресс-службы блока, ранее состоявший всего из шести сотруднике», был резко увеличен. Под руководством специально направленного в Брюссель пресс-секретаря британского правительства А. Кемпбелла при ней был срочно сформирован так называемый «военный кабинет» — специальный координационный орган в составе 40 специалистов по связям с общественностью и СМИ (12 представителей Великобритании, восемь — США, остальные — от ФРГ, Франции и других стран блока). Задачами этой структуры были: анализ сообщений западных, югославских и международных СМИ о ситуации на Балканах; выработка рекомендаций для руководства альянса по определению общей стратегии в отношении освещения в этих средствах хода военных операций: подготовка информационных материалов для пресс-конференций, брифингов н пресс-ре-

лизов штаб-квартиры НАТО. По оценкам независимых экспертов (в частности. шведских), для деятельности пресс-службы блока были характерны такие черты, как односторонняя подача и «дозирование» информации, преднамеренное искажение фактов и шаблонное перекладывание вины за «ошибки» натовских военных на сербскую сторону или «неполные разведданные», жесткие ограничения доступа к информации для журналистов и постоянные попытки манипулирования СМИ в своих интересах.

На брифингах в брюссельской штаб-квартире НАТО война на Балканах в соответствии с практикой, отработанной еще во время войны с Ираком, представлялась в «чистой виртуальной форме»: в виде бесконечных видеозаписей поражения целей высокоточным оружием. Острые вопросы о потерях сил блока, жертвах среди мирного населения, бомбардировках иностранных посольств, «ошибках» натовских летчиков оставались, как правило, без комментариев, либо ответами на них были дежурные фразы о «неизбежности трагических случайностей в ходе военных действии». Зато трибуна пресс-службы альянса охотно предоставлялась представителям «Освободительной армии Косово», выступавшим с очередными разоблачениями «военных преступлений сербов». Практиковалась также организация специальных телемостов между пресс-центром НАТО в Брюсселе и лагерями косовских беженцев в Македонии и Албании, в ходе которых специально подготовленные и оплаченные «живые свидетели» рассказывали о с градациях албанцев и «бесчинствах» сербских сил безопасности в Косово.

В ходе Косовского конфликта администрация президента США Клинтона и НАТО постоянно приводили в средствах массовой информации заранее согласованные данные о потерях с обеих сторон. Однако при дальнейшем расследовании стало очевидно, что эти данные значительно преувеличивались. Министерство обороны США заявляло уже не о 100 тыс. албанцев, убитых сербами в ходе этнических чисток, а о 10 тыс. В косовских горах скрывалось вовсе не 600 тыс. «бездомных, голодающих албанцев, которые боялись вернуться в свои селения» или вовсе зарытых сербами в братских могилах, а гораздо меньшее количество.

Компьютерная сеть Интернет также превратилась в «поле боя», где ИВ велась в двух формах – с одной стороны, противники пытались нарушить информационную инфраструктуру друг друга, в том числе путем взлома компьютерных сетей, а с другой – обе стороны активно использовали возможности сети в пропагандистских целях для доведения до широкой аудитории своих взглядов на происходящие события.

Свидетельством напряженности, а также косвенным подтверждением эффективности сербской антинатовской пропаганды могут служить ракетно-бомбовые удары НАТО по радио- и телецентрам Югославии. Представители альянса объясняли бомбардировки телевизионных станций не стремлением лишить Югославию «права голоса» и своим страхом перед сербской пропагандой, а «случайными» попаданиями при нанесении ударов по воинским ра-

диорелейным линиям связи. Видимо, для югославских СМИ могла остаться только одна возможность – производить вещание своих программ через Интернет. В свою очередь, собственное теле- и радиовещание на Югославию страны НАТО вели всеми доступными им средствами, в том числе с территории приграничных государств, со специальных самолетов «Коммандо Соло», через космические спутники всемирной компьютерной сети.

Страницы, посвященные событиям на Балканах, появились на многих официальных сайгах, в том числе и американских вооруженных сил. Помешенная на них информация. предназначенная как для национальных. так и зарубежных пользователей, призвана была пропагандировать официальную точку зрения и формировать благоприятное общественное мнение. Одновременно с этим предпринимались усилия но поддержке пользователями сети Интернет оппозиционных властей Югославии. В частности. американская компания «Апопугтег» организовала для косовских албанцев, сербов и всех тех, **кто** регулярно пишет о текущих событиях в Косово, бесплатное техническое (в том числе криптографическое) обеспечение анонимности личностей при использовании ими таких возможностей Интернета, как электронная почта, доступ к информации и участие в компьютерных (сетевых) дискуссиях. По мнению западных аналитиков, возможность передавать через эту сеть нужную информацию в условиях, когда все другие каналы были заблокированы, превратило ее и потенциально наиболее сильное оружие, способное влиять на ход войны и Косово.

Деятельность СМИ Югославии в ходе конфликта. Задолго до бомбардировок, в октябре 1998 года, в Югославии был введен новый закон о СМИ, предусматривавший уголовное наказание за оскорбление государственного строя. После этого в г. Белград были закрыты несколько негосударственных местных радиостанций.

Югославские телеканалы были подготовлены к пропаганде заранее. В первую ночь бомбардировок по телевидению показали фильм о битве на Косовом поле, а затем в течение нескольких дней круглосуточно демонстрировали фильмы о Второй мировой войне и героических титовских партизанах. Тогда же и родился один из главных штампов югославского телевидения — «преступная агрессия НАТО против независимой Югославии». Все сообщения о бомбардировках использовали этот оборот, так что в течение одного выпуска новостей фраза произносилась не меньше 20 раз, как ведущими, так и корреспондентами. В сознании югославского народа слово «преступный»» четко ассоциируется со Второй мировой войной и зверствами, которые совершили усташи (хорватские националисты, сражавшиеся на стороне фашистов) по отношению к сербским партизанам. На каналах национального телевидения шел процесс по «радикализации официального языка», начало которому положил С. Милошевич.

Следующим этапом информационной кампании в югославских СМИ стала дискредитация противника. На телевидении был показан клип, в котором Б. Клинтон, Т. Блэр и Ж. Ширак стоят в одном видеоряду с А. Гитлером.

Фюрер похлопывает мальчика из «гитлерюгенд» по плечу, произнося вложенную ему в уста фразу: «Молодец, Солана, так держать!» Одновременно стал меняться телевизионный киноассортимент. Сербам стали демонстрировать американские фильмы: о войне во Вьетнаме – «Апокалипсис сегодня» (трижды за неделю) и «Охотник на оленей», о коррумпированном американском обществе – «Крестный отец», «Сеть», «Хвост виляет собакой» (трижды за пять дней).

Одной из главных особенностей деятельности зарубежных СМИ в Югославии являлась строжайшая военная цензура. Все это политическое руководство страны объясняло требованиями военного времени. Журналисту, приехавшему в Югославию, для работы нужна была аккредитация поенного пресс-центра. Любая съемка требовала специального разрешения. Официально съемки были разрешены только в трех местах Белграда, причем в течение не более 4 ч в день. Невыполнение данных инструкций каралось строго, вплоть до высылки из страны. Кроме того. журналистам рекомендовалось не снимать общие планы улиц, чтобы не показывать какие-либо здания в привязке к местности. Все материалы просматривались и если что-то не устраивало местные власти, то такие материалы не могли быть переданы в эфир.

Однако у американской телекомпании Си-эн-эн было явное преимущество перед своими коллегами. Ее репортеры знали точное время ночных налетов заранее. Камеры были включены и размещены на выгодных ракурсах непосредственно перед тем, как крылатые ракеты должны были поразить здание МВД Сербии. Именно Си-эн-эн первой сообщала со ссылкой на анонимные источники и Пентагоне, что ракет было восемь. Таким образом, благодаря ее журналистам американцы смогли убедиться, что деньги налогоплательщиков тратятся не зря и ракеты «Томагавк» стоимостью 1 млн. долларов попадали в намеченные цели. В интервью Си-эн-эн президент США Клинтон заявил, что о новых ударах просили албанские беженцы, он также подчеркнул, что здания МВД Югославии и Сербии являлись теми центрами, где планировались все операции против косовских албанцев.

Многие югославские СМИ активно стали использовать возможности Интернета: для трансляции своих материалов в условиях, когда большинство ретрансляторов были разрушены авиацией альянса. Так, криптографическим обеспечением н сети Интернет пользовалась к негосударственная радиостанция Белграда «В-92», которая и течение двух лет передавала информацию через сеть с использованием «тоннельного» шифрования (оно обеспечивает невидимость канала связи со стороны) из Белграда через Амстердам электронной почтой во все концы света, а также в Лондон на Би-би-си, откуда через спутник велась передача на 35 независимых радиостанций Югославии. С началом натовских бомбардировок передатчики этой радиостанции были закрыты югославским правительством, но «В-92» продолжала транслировать свои программы через Интернет вплоть до 2 апреля 2000 года, пока официальные власти не закрыли как саму радиостанцию, так и «Открытую сеть».

Противостояние сербов и косовских албанцев во всемирной компьютерной сети началось весной 1999 года, причем инициативу сразу захватили албанцы. Вероятнее всего, это не было случайностью: распространение информации по Интернету обходится недорого, и лучшего способа информировать зарубежную аудиторию о своей точке зрения на происходящее в мятежном сербском крае албанцы и придумать не могли.

Первым во всемирной сети появился сайт http://www.kosova.com. близкий к Демократическому союзу Косово — партии национального лидера Ибрагима Руговы. Его авторы — студенты так называемого параллельного албанского университета в Принципе, которые, впрочем, открыли и свою собственную домашнюю страницу — http:// www.alb-net.corn. Чуть позже наладила выпуск электронной версии самая популярная косовская газета, выходившая на албанском языке «Коха диторэ» (http://www.kohaditore.com), собственные страницы или сайты имеют некоторые зарубежные организации косовских албанцев. ОАК — главная албанская повстанческая сила — к услугам Интернета не обращалась, но информацию о ней в изобилии можно было отыскать по любому албанскому компьютерному адресу. В начале октября появился завершивший оформление структуры косовского Интернета сайт, первая страница которого была озаглавлена так: «Сайт Республики Косово, находящейся под временной виртуальной оккупацией Сербии» (htlp://www.kosova-state.org), а по своему содержанию ничем не отличается от сайтов органов государственной власти любой существующей в реальности страны — герб, гимн, флаг, данные о составе населения, история, адреса политических партий и т. д. Собственного провайдера в албанском Косово не было — энтузиасты Интернета арендовали сайты за границей, а потому отличительной особенностью всех этих страниц являлась их тесная взаимосвязь: достаточно открыть одну, чтобы более не затруднять себя поисками новых адресов, — в специальном разделе имеются исчерпывающий список координат коллег по пропаганде национальной идеи.

Сербская компьютерная пропаганда хотя и появилась раньше албанской, однако уступала ей в оперативности. Например, сайт Сербскою движения сопротивления содержал в основном религиозно-патриотические проповеди и очерки, утверждающие «сербскую правду о Косово». Естественно, что ключевым словом для всех интернетовских поисковых систем служило слово «kosovo». Распространением правительственной информации и сообщений югославского агентства ТАНЮГ по компьютерной сети занималось министерство информации Сербии (htlp:www.serbia-info.com), но его продукция отличалась сухостью и официальностью и была малоинтересна. Поживее работали авторы сайта медиацентра (http://www.mediacentar.org в г. Приштине созданного белградскими властями для оперативного информирования журналистов и общественности. Вообще Югославия была еще весьма далека от поголовной компьютеризации — в стране с населением почти в 10 млн человек Интернетом постоянно или эпизодически пользовались не более 100 тыс.

Впрочем, посвященные военным событиям в Косово сайты сербские специалисты рассматривали прежде всею как средство внешнеполитической агитации и пропаганды, предназначенное в первую очередь для американских пользователей.

В ответ на ракетно-бомбовые удары НАТО сербские хакеры «контратаковали» сервер альянса, перегрузив его большим количеством обращений, чем он мог обработать, в результате чего доступ к нему был заблокирован в течение трех дней. Средства массовой информации оценили это событие как первую победу сербских хакеров в «электронной войне» против альянса. По сообщению официального представителя НАТО Дж. Шеа, в течение трех дней, начиная с 28 марта 1999 года, натовская страница во всемирной компьютерной сети была выведена из строя. Неизвестный адресат регулярно присылал на адрес Североатлантического союза около 2000 телеграмм в день, которые переполнили его электронный «почтовый ящик». Компьютерные специалисты были вынуждены основательно потрудиться, чтобы восстановить для журналистов возможность пользоваться открытой информацией НАТО через Интернет.

После начала агрессии против Югославии компьютерным хакерам неоднократно удавалось проникать на американские сайты и оставлять свои пропагандистские сообщения, в том числе на страничке ВМС. Неизвестные взломщики сумели испортить даже личный сайт американского президента Б. Клинтона. Сербские хакеры привели длинный список преступлений албанских террористов против полиции и мирных граждан, сообщили номера банковских счетов для помощи жертвам ОАК. Они информировали общественность о захвате албанскими сепаратистами двух журналистов агентства ТАНЮГ, расстреле сербских заложников.

Ведение информационного противоборства и нейтрализация пропаганды НАТО в СМИ Югославии требует дальнейшего детального изучения. Давая оценку информационной кампании НАТО против Югославии, необходимо отметить, что освещение боевых действий впервые вышло за рамки традиционных СМИ и осуществлялось по большей части с помощью Интернета. Во всем мире осознали возможности сети как источника альтернативной информации, не подвергающейся цензуре со стороны противоборствующих сторон. Американские специалисты в области информационной войны столкнулись с непростой проблемой, когда подаваемая ими информация ежедневно опровергалась югославскими СМИ, транслирующими на весь мир реальные результаты «гуманитарной операции» НАТО.

Однозначно определить «победителя» в информационной войне в ходе косовского конфликта невозможно. Специалисты НАТО добились определенных успехов благодаря согласованности действий, использованию современных технологий и СМИ в интересах оказания воздействия на общественное мнение как в Югославии, так и во всем мире. Между тем потенциал по ведению информационной войны в самой Югославии оказался достаточным для нейтрализации большинства усилий западных пропагандистов.

Воронков Д.А., Богуш Д.А.

МАНИПУЛЯТИВНЫЕ СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ (ОБЗОР ЗАРУБЕЖНЫХ ИСТОЧНИКОВ)*

"Мысли, внедренные в сознание людей, это пули разящие насмерть... Гораздо больше можно выиграть обольщением и обманом, чем принуждением". Из статьи "Конгрешнл рекорд"(официальный орган конгресса США) времен холодной войны [1].

Термины "информационная операция" (ИО), "информационная война" (ИВ) начали активно употребляться после окончания войны в Персидском заливе, а первым официальным документом по этой проблеме стала директива министра обороны США №TS 3600.1 от 21 декабря 1992 года под названием "Информационная война" [2, 3]. В директиве ставились задачи объединенному штабу Комитета Начальников Штабов (КНШ) по разработке новой концепции. Эта работа была завершена к концу 1993 года и нашла свое отражение в директиве председателя КНШ МОР №30-93, в ней информационное противоборство определялось, как :"...комплексное проведение по единому замыслу и плану психологических операций, мероприятий по оперативной маскировке, радиоэлектронной борьбе и физическому уничтожению пунктов связи с целью лишения противника информации, вывода из строя или уничтожения его систем управления при одновременной защите своих сил от аналогичных действий" [3]. Данный документ стал отправной точкой для всех документов и исследований, как военного, так и государственного характера изданных позже не только в США, но и в других странах.

В своем выступлении "Национальная безопасность в следуещем поколении" в марте 2001 года года председатель Национального Совета по Разведке (National Intelligence Council) Дж. Гэннон (Gannon) сформулировал основные задачи стоящие перед США для решения задачи обеспечения безопасности страны, и подчеркнул, что в мире с высокой степенью интеграции всех процессов для предотвращения возникновения возможных рисков потребуется высокая степень взаимодействия гражданских правительственных и неправительственных организаций, военных структур и масс-медиа, а также вовлечение в этот процесс правительств иностранных государств [7].

Масс-медиа или средства массовой информации (СМИ) не случайно выделены в этом перечислении. "Брошенное слово означает больше, чем сброшенная бомба", - эти слова американский разведчик Л. Фараго, произнес еще 40 лет назад [1]. А за прошедшее время средства распространения информации сделали огромный шаг вперед, и теперь слова, которые СМИ "бросают" в эфир могут сравниться уже с применением оружия массового поражения (ОМП), силы и средства которого находятся в состоянии постоян-

ной боевой готовности, распространение которого никак не ограничивается международными соглашениями, более того его распространение всячески поощряется и декларируется. В настоящее время использование информации, как средства борьбы стало решающей составляющей при проведении мероприятий, направленных на поддержание жизнедеятельности любого общественно-политического образования.

Мартин Либики (Libicki) в своей монографии "Что такое информационная война" выделяет 7 форм ИВ [4]:

- борьба с пунктами управления и связи противника;
- борьба за получение информации о собственных силах и силах противника в режиме реального времени, для получения решающего превосходства над противником;
- радио-электронная борьба (РЭБ);
- психологическая война;
- "хакер" война (борьба против компьютерных систем противника);
- блокирование или направление экономической информации в необходимое русло для получения экономического доминирования;
- кибервойна.

В свою очередь по степени интенсивности, формам и характеру воздействия на информационное пространство (ИП) в современных конфликтах можно выделить 3 следующих этапа:

1. Этап применения "мягких" методов воздействия (характеризуется отсутствием ярко выраженного физического противоборства);
2. Этап непосредственно политического/военного конфликта;
3. Период мирных переговоров и урегулирования конфликта.

Данные этапы в свою очередь могут подразделяться на подэтапы.

Американский аналитик Р. Боудиш (Bowdish) выделяет также 3 этапа, но подразделяет их следующим образом [6]:

1. Состояние мира;
2. Состояние конфликта;
3. Состояние войны.

В любом случае единственными формами ИВ, которые будет присутствовать на протяжении всех этапов будут: психологическая война и блокирование или направление экономической информации в необходимое русло для получения экономического доминирования.

Актуальность рассмотрения взглядов на применение именно этих форм будет заключаться не только в том, что они являются основными манипулятивными составляющими ИО, но также в том, что признание их, как формы военных действий стирает границы между понятиями "комбатант" и "некомбатант". Примерами могут служить: Китай, где термин "народная война" приобрел совершенно новое значение в свете современной китайской военной реформы (руководством страны было заявлено о развертывании телекоммуникационной системы двойного назначения (предусматривается ее ис-

пользование, как в гражданских, так и военных целях), основной персонал которой будет состоять из резервистов, и которая как считают станет ключевым элементом в объединении гражданских и военных усилий, и также в их кординации [9]); США, где в официальном документе "Единая перспектива - 2020" появляется термин "национальная война" [8].

Психологическая война. Документ КНШ JP 3-53 "Доктрина проведения психологических операций" прямо указывает, что психологические операции (ПсО)являются жизненно важной составляющей в политической, военной, экономической и информационной деятельности США [10]. В нем ПсО определяются, как мероприятия по распространению специально подготовленной информации с целью оказания воздействия на эмоциональное состояние, мотивацию и аргументацию действий, принимаемые решения и поведение отдельных руководителей, организаций, социальных или национальных групп и отдельных личностей в благоприятном для США и их союзников направлении. Они могут быть стратегическими, оперативными и тактическими по своим масштабам.

На стратегическом уровне психологические операции могут проводиться в форме пропаганды определенных политических или дипломатических позиций, официальных заявлений либо сообщений руководителей государства.

На оперативном и тактическом предполагается использование печатных и электронных СМИ и пропаганды для создания необходимого психологического климата (нагнетание страха, разжигание разногласий, побуждение к саботажу и капитуляции и т.п.).

По мнению российских аналитиков одной из важнейших задач на подготовительном этапе информационного противоборства становится использование возможностей СМИ для введения потенциального противника в заблуждение, дискредитации его военно-политического руководства и конкретных лидеров, а также мероприятий по ограничению информационно-пропагандистской деятельности противника вплоть до организации частичной или полной информационной блокады [2]. Китайские военные аналитики к этим задачам добавляют "создание постоянного психологического давления на противостоящую сторону", что по их мнению должно снижать эффективность управления и парализовывать ответные действия [9].

Как видно приведенные определения представителей различных военно-научных школ имеют много общего.

Уже упоминавшийся М. Либики предлагает деление психологической войны на такие сегменты, как [4]:

- операции против национального самосознания;
- операции против руководства противостоящей стороны;
- операции против войск противника;
- культурные конфликты.

Давая оценку данным сегментам он замечает, что сторона желающая манипулировать другой стороной через масс-медиа должна пержде всего выделить целевые аудитории в населении противостоящей стороны: - часть населения предрасположенную верить во все сказаннное; часть - предрасполо-

женную не доверять ничему; часть - предрасположенную верить в противоположное сказанному; часть не придающую никакого значения сказанному ("плывущими на своей волне"). Другой американский аналитик Л.-В. Кокс (Cox) предлагает такое деление целевых аудиторий: - национальные лидеры; - региональные лидеры; - остальное население; (указанные категории могут делиться на подкатегории) [12].

Данные разделения указывают на краеугольный камень применения любого оружия вообще и психологического в частности - его эффективность применения. С. Мец (Metz) в своем исследовании, посвященном эволюции современных конфликтов, пишет: "Последствия применения психологического оружия сейчас нельзя предсказать с такой же точностью, как применение высокоточного оружия". И предлагает прежде всего "развивать более высокую психологическую точность, включая полное использование нелетальных возможностей противоборства" [11]. Данные рекомендации уже успешно претворяются в жизнь; например, в США особое внимание уделяется созданию коллективных и индивидуальных моделей поведения представителей высшего и среднего звена государственного и военного руководства, в частности составление психологических портретов на руководителей; воздействие на политических и военных лидеров, а также на руководителей (наиболее заметных представителей) СМИ, культуры и искусства противостоящей стороны считается важным аспектом информационного противоборства и ПсО [3].

Kulturkampf (нем. борьба между культурами), как ее называет М. Либики не являясь формой вооруженного противоборства, в прямом понимании этого слова, ставит своей задачей культурную экспансию, которая также облегчает применение психологического оружия и, что самое главное, позволяет более точно прогнозировать результаты этого применения (еще один прием повышающий эффективность применения).

Внимание аналитиков сейчас сосредоточено не только на способах планирования и проведения ПсО, но и на трудностях и ограничениях при их проведении, так У. Боудиш указывает на такие трудности при проведении психологической войны, как [6]:

- необходимость планирования и развертывания на длительный срок времени;
- неполная информация, поступающая от разведывательного сообщества;
- трудности координации между военными и гражданскими информационными агенствами, что дает время противнику на развертывание контрпропаганды;
- недостаток квалифицированного персонала - лингвистов, разбирающихся в культурном, политическом, экономическом, социальном и идеологическом состоянии противника;
- законы войны;
- доступность потенциальной целевой аудитории.

Блокирование или направление экономической информации в необходимое русло для получения экономического доминирования. Главной отличительной чертой конфликтов нового поколения стало стремление к интеллектуальному доминированию, в отличие от конфликтов прошлого, когда преобладало физическое доминирование. Стремление "победить противника не сражаясь" или лишить его возможности и желания сопротивляться, привело к усилению роли такой формы ИВ, как блокирование или направление экономической информации в необходимое русло для получения экономического доминирования. Применение подобной формы борьбы можно сравнить с применением стратегической дезинформации в открытом военном конфликте. К сожалению, вопросы применения манипулирования с экономической информацией не нашли достаточного отражения в исследовательской литературе. Поэтому здесь будет приведена точка зрения только М. Либики на эту проблему [4]. Он считает, что объединение методов информационной и экономической войны приводит к появлению таких двух форм борьбы, как: блокирование экономической информации и информационный империализм. Если первая из этих форм присутствовала во все времена и сейчас получила дополнительные возможности для применения, связанные с получением информации в реальном режиме времени, то - вторая присуща только современной эпохе. Также, как на заре XX века объединение финансового и промышленного капиталов привело к появлению экономического империализма (см. работу В.И. Ленина "Империализм, как высшая стадия развития капитализма"), так сейчас на заре XXI века присоединение к ним информационного капитала привело к появлению информационного империализма. Не являясь в полной мере формой борьбы, также как и kulturkampf, информационный империализм облегчает транснациональным корпорациям, которые все больше теряют национальную окраску, бороться за экономическое доминирование. В свете вышесказанного хотелось бы отметить, что в США отнюдь не информационные риски ставятся на первое место среди угроз, с которыми может столкнуться государство в ближайшем будущем, а недофинансирование науки и образования (2е место среди угроз после применения ОМП). "К 2015 году образование станет определяющим фактором для достижения успеха" [13]. Думаю, что было бы правильнее применить термин "интеллектуальный империализм", а не "информационный империализм".

Важным аспектом ИВ, на который также необходимо обратить внимание, является стремление, если не "монополизировать информационное пространство", то получить в борьбе за него решающее превосходство. Реализация данной задачи является основополагающей при информационном противоборстве с противостоящей стороной. Зарубежные аналитики для характеристики этого процесса используют термины: "информационное превосходство" [8, 14] или "информационное доминирование" [15]; и считают, что его можно определить, как способность собирать, обрабатывать и распространять (термин "манипулировать" также встречается Авт.) информацию достаточную для получения политического, военного или экономического домини-

рования. Примером может служить создание в Китае концепции "информационного контроля", которая полностью отвечает данным требованиям [14].

В России развитию нормативной правовой основы обеспечения информационно-психологической безопасности уделяется достаточно большое внимание. Например, подготовлены и активно обсуждаются в комитетах Государственной Думы Российской Федерации, проекты федеральных законов "Об информационно-психологической безопасности" и "Безопасности психосферы" существует "Доктрина информационной безопасности России".

Под информационно-психологической безопасностью понимается состояние защищенности граждан, отдельных групп и социальных слоев, массовых объединений людей и населения в целом от негативных информационно-психологических воздействий.

Данными вопросами занимаются Академия национальной безопасности (СПб), Институт системного анализа РАН, Институт медико-психологических проблем, Институт психологии РАН, МГУ и др. Проведены конференции "Проблемы информационно-психологической безопасности" в 1995, 1996 и 1997 г.г., "Информационно-психологическая безопасность избирательных кампаний" 1999 г.

Можно с уверенностью можно сказать, что применение манипулятивных форм воздействия в информационном пространстве с течением времени будет становится все более интенсивным. Это будет происходить, потому что ожидается не только сохранения числа кризисных ситуаций на прежнем уровне, но даже их увеличение [7], при этом применение прямого физического воздействия, в мире с высокой степенью экономической зависимости друг от друга, становится действительно крайней мерой, урегулирование кризисных ситуаций перестало предполагать обязательное применение силы [5].

В заключении хотелось бы привести отрывок из введения к секретному документу британской разведки СИС (SIS) № 2279/HB от 17.02.1959 г., в котором впервые были сформулированы стратегические основы ведения психологической войны: "На заре века престарелый маршал Лиотэ - предводитель французских колониальных войск в Марокко и Алжире - направлялся со свитой во дворец. Был полдень, нещадно палило африканское солнце. Изнывавший от жары маршал распорядился обсадить дорогу деревьями, которые давали бы тень. "Деревья вырастут ведь только через пятьдесят лет", - заметил один из приближенных. "Именно поэтому, - прервал старик, - работу начните сегодня же" [1].

ИСТОЧНИКИ:

1. "Секреты секретных служб США", - М., 1973 г., Издательство политической литературы
2. Россия (СССР) в локальных войнах и военных конфликтах второй половины XX века. М., "Кучково Поле", 2000 г., 575 стр. (Институт Военной Истории МО РФ)

3. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение.-2001.-№1.
4. Martin Libicki. What is information warfare?//National Defence Univercity, ACIS Paper 3, August 1995, Washington, D.C.
5. Энтони Крэгг. Стратегическая концепция НАТО//Военный парад.-1999.- № 5(35)
6. Bowdish R. G. Information-Age Psychological Operations//Military Review, vol. LXXVIII, December 1998 - February 1999, № 6
7. "National Security in the Next Generation" Address by John C. Gannon, Chairman of National Intelligence Council to The Academy of Senior Professionals At Eckerd College St. Petersburg, Florida, 27 March 2001
8. Joint Vision 2020, US Government Printing Office, Washington DC, June 2000
9. Timothy L. Thomas.China's Electronic Strategies// Military Review, vol. LXXXI, May - June 2001, № 3, p.47
10. Joint Pub 3-53 "Doctrine for Joint Psychological Operations", US Government Printing Office, Washington DC, July 1996
11. Steven Metz. Armed conflict in the 21st century: The information revolution and post-modern warfare// Strategic Studies Institute, U.S. Army War College, April 2000
12. Lee-Volker Cox. Planning for Psychological operations. A proposal//A Research Paper Presented To The Research Department of Air Command and Staff College, March 1997
13. Global Trends 2015: A Dialogue About the Future With Nongovernment Experts NIC 2000- 02, December 2000
14. Qingmin Dai, "Innovating and Developing Views on Information Operations," Beijing Zhongguo Junshi Kexue, 20 August 2000, 72-77. Translated and downloaded from Foreign Broadcast Information Service (FBIS), 9 November 2000.
15. Martin C. Libicki. Information Dominance//Strategic Forum № 132, November 1997
16. Лопатин В.Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации (проект). - М.: Издание Государственной Думы, 1998. - 159 с.
17. Проблемы информационно-психологической безопасности / Под ред. А.В.Брушлинского и В.Е.Лепского. М.: Институт психологии РАН, 1996. - 100 с.
18. Смолян Г.Л., Зараковский Г.М., Розин В.М., Войскунский А.Е. Информационно- психологическая безопасность (определение и анализ предметной области). - М.: Институт системного анализа РАН, 1997. - 52 с.
19. Лепский В.Е. Технократический подход к информатизации общества - источник угроз национальной безопасности России / II Всероссийская научная конференция "Россия XXI век". М. 1999. С.143-147

Гриняев С.Н.

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ ВОЙНЫ ВО ВРЕМЯ АГРЕССИИ НАТО ПРОТИВ ЮГОСЛАВИИ (ПО МАТЕРИАЛАМ ОТКРЫТОЙ ПЕЧАТИ)*

Особенности информационной войны накануне агрессии. При подготовке агрессии против Союзной Республики Югославии НАТО придавало большое значение организации и ведению информационной войны. Военно-политическое руководство блока исходило из того, что умелое и эффективное осуществление информационно-психологического воздействия в значительной степени определит уровень международной поддержки проводимых НАТО силовых акций и существенно скажется на морально-психологической устойчивости вооруженных сил и руководства СРЮ.

При планировании агрессии основные усилия информационных структур блока направлялись на решение следующих задач:

- формирование негативного представления о военно-политическом руководстве СРЮ как об источнике кризиса и основной причине гуманитарной катастрофы в Косово и Метохии, деструкцию морально-этических ценностей сербского народа и нагнетание неблагоприятного психологического климата в отношениях различных политических сил СРЮ;
- создание и поддержание у военно-политического руководства СРЮ сдерживающего страха перед силовыми акциями НАТО, в том числе и за счет подчеркивания реализуемости декларируемых угроз, афиширования высокой эффективности имеющихся вооружений и потенциальных возможностей объединенных вооруженных сил блока;
- формирование репутации внешнеполитического руководства США и НАТО как весьма жесткого в своих решениях и последовательного в действиях;
- прицельную информационную обработку ключевых фигур в руководстве СРЮ на основе учета их психологических особенностей, политической и иной ориентации, пропаганду и внедрение форм общественного поведения, снижающих моральный потенциал нации.

Одновременно с решением перечисленных задач планировался целый ряд мероприятий по воздействию на информационную инфраструктуру СРЮ.

События в Югославии в этой области развивались стремительно и зачастую трагично. Югославские СМИ старались всячески подчеркнуть единство союза. Однако мировое общественное мнение формировалось под воздействием западных СМИ, склонных к поддержке сепаратистских тенденций и настроений в югославских республиках. В силу этого предыстория гражданских, а затем и межгосударственных военно-политических конфликтов на

http://www.agentura.ru/equipment/psih/info/yugoslav/

территории бывшей Югославии не получала должного освещения, тем более, что негативный образ СРЮ был создан и поддерживался в мировом общественном мнении еще со времени военного конфликта в Боснии и Герцеговине.

На основании решения президента США были определены объекты воздействия: на политическом уровне – это широкие слои населения стран НАТО и мировая общественность, на стратегическом – правительство, народ и вооруженные силы Югославии. Все мероприятия планировалось провести в два этапа.

На первом этапе (до начала агрессии) было предусмотрено информационное воздействие на политическом уровне. Его основными объектами являлись: широкая общественность стран НАТО, других государств Европы, включая Россию, население Ближнего и Среднего Востока, Азии. Главные цели, поставленные на этом этапе, состояли в обеспечении международной поддержки курса США и их союзников по НАТО в отношении СРЮ, убеждении мирового сообщества, что в Югославии нарушаются права албанцев, и оправдании необходимости применения военной силы.

На втором этапе (с началом агрессии) акцент был сделан на ведение информационного противоборства на стратегическом уровне. В качестве основных объектов воздействия на территории Союзной Республики Югославии были определены ее правительство, личный состав вооруженных сил и население. Конечная цель всех мероприятий по информационному воздействию на этом этапе – безоговорочная капитуляция СРЮ на условиях США и НАТО.

План информационной войны был согласован со всеми странами-участницами НАТО, от которых были выделены воинские контингенты. В ее осуществлении участвовали высшее политическое руководство стран НАТО, министерства иностранных дел, спецслужбы, национальные СМИ, армейские структуры ведения психологических операций. Участие этих сил в информационной агрессии против Югославии было подтверждено многочисленными теле- и радио заявлениями президента США, премьер-министра Великобритании, генерального секретаря НАТО, руководителей министерств иностранных дел и обороны стран-членов Североатлантического альянса.

В США основные задачи в информационной войне на стратегическом уровне выполняли государственный департамент, Информационное агентство США (ЮСИА) со своими подразделениями (международные спутниковые телесети, радиостанции "Голос Америки", "Свобода", "Свободная Европа"), Центральное разведывательное управление и специалисты-психологи из Пентагона.

Структурные подразделения ЮСИА бесплатно рассылали в адрес тысяч радиостанций многих стран мира свои передачи в записи, издавали различные информационные бюллетени. Большое значение в деятельности ЮСИА придавалось реализации американских материалов в зарубежной прессе. Необходимо особо отметить, что распространение продукции самого ЮСИА внутри США было строго запрещено.

Таким образом, против СРЮ была осуществлена целая серия информационно-психологических операций. Она включала мощное воздействие на информационные системы Югославии с целью разрушения информационных источников, подрыва или ослабления системы боевого управления, изоляции не только войск (сил), но и населения.

Составной частью информационной агрессии явилось и развертывание направленного и интенсивного вещания на территорию Югославии радиостанции "Голос Америки", уничтожение теле- и радиоцентров с целью обеспечения контроля над общественным мнением населения. Так, после разрушения телецентров в Приштине и Белграде местные жители вынужденно оказались в информационном поле СМИ только стран НАТО. Для непосредственной "оккупации информационного пространства Югославии" НАТО применяло апробированные ранее США в Ираке, Гренаде и Панаме способы, в том числе летающую теле- и радиостанцию "CommandoSolo", которая транслировала свои передачи на частотах, используемых сербским телевидением.

В рамках информационно-психологических операций было спланировано ведение радиовещания на Югославию с территорий сопредельных стран, а также разбрасывание пропагандистских листовок. Предполагалось активное использование штатных формирований психологических операций и соответствующих СМИ, находящихся в распоряжении командования сухопутных войск США. Для нарушения работы югославских компьютерных сетей Нью-Йорским университетом по заказу Пентагона были разработаны программные пакеты вирусов для внедрения в компьютерные базы данных.

Информационное обеспечение военных действий США и НАТО было направлено, прежде всего, против системы управления ВС СРЮ. В этих целях помимо применения управляемых ракет планировалось использование электромагнитных бомб, разрушительное действие которых сравнимо с поражающим фактором электромагнитного импульса, возникающего при ядерном взрыве. Этот импульс способен вывести из строя всю радиоэлектронную технику в радиусе десятков километров.

Успешное выполнение задач информационного обеспечения, по мнению военных экспертов, предполагало достижение трех важнейших целей:

- способности к дешифровке и пониманию работы информационных систем противника;
- наличия разнообразных и эффективных средств их поражения;
- готовности к оценке качества уничтожения информационных целей.

В ходе военной операции против СРЮ руководство США и НАТО добивалось не только всестороннего обеспечения выполнения конкретной акции. Значительное внимание уделялось отработке перспективных способов ведения информационной войны.

По взглядам руководства НАТО, вооруженные силы, владеющие информационными технологиями, представляют собой новую категорию войск с особой тактикой ведения боевых действий, организационно-штатной струк-

турой, уровнем подготовки личного состава и вооружением, полностью отвечающим требованиям современной войны. Войска и силы, привлекаемые для ведения информационной войны, активно применяют технологии цифровой связи, целостные системы боевого управления и разведки, высокоточное оружие и связь со всеми операционными системами. Важнейшим условием эффективных действий этих сил является их оснащение самыми современными видами вооружений: радарами второго поколения, системами опознавания типа "свой–чужой", глобальными космическими навигационными системами и боевой техникой со встроенной цифровой аппаратурой.

Особенности информационной войны в ходе операции. Информационное воздействие в операции НАТО "Союзническая сила" велось с использованием отлаженного механизма, который был успешно апробирован в ходе подготовки и ведения военных операций ВС США в 90-х годах ("Буря в пустыне" в Ираке, "Поддержка демократии" на Гаити, миротворческая операция ИФОР – СФОР в Боснии и Герцеговине и др.) Главные усилия в борьбе за информацию между ОВС НАТО и ВС Югославии были сосредоточены в информационно-психологической и информационно-технической сферах.

Основной составляющей информационной войны ВС НАТО во время агрессии против СРЮ являлось массированное идеологическое и психологическое воздействие крупнейших СМИ стран Запада и сил психологической войны ВС США на население и личный состав вооруженных сил Югославии, государств Североатлантического блока, а также мировую общественность. Для обеспечения позитивного мирового общественного мнения о действиях ОВС НАТО в операции "Союзническая сила" страны блока вели мощную и активную пропагандистскую кампанию, направленную на формирование образа врага, против которого не только можно, но и необходимо применить оружие. При этом активно использовались традиционные методы воздействия на общественное сознание:

- репортажи о событиях;
- описание актов геноцида албанского населения Косово и Метохии;
- демонстрация силы и показ возможностей современных видов вооружения ВС США и других стран альянса, результатов ракетно-бомбовых ударов по Югославии;
- комментарии социологических опросов, связанных с событиями на Балканах.

Роль главного агитатора и пропагандиста, призванного защищать позицию США и НАТО в ходе агрессии, была отведена министру обороны У. Коэну. По сообщениям наблюдателей, только за первый день бомбардировок он выступил сразу в восьми телепрограммах, в пяти утренних выпусках новостей основных телеканалов и трех наиболее популярных вечерних информационно-аналитических передачах. У. Коэну помогали также помощник президента США по национальной безопасности С. Бергер и госсекретарь М. Олбрайт.

К гражданам США с антисербским воззванием обратился Б. Клинтон. Своим соотечественникам, находящимся за тысячи километров от Югославии, он популярно, в доступной для американцев форме разъяснил причины применения военной силы в отношении суверенного государства.

В этот же период прошла серия передач заказного характера на телевизионном канале Си-эн-эн, в ходе которых военные эксперты и аналитики буквально заполнили основную часть времени новостных и аналитических выпусков активной пропагандой в пользу действий НАТО. Ведущим корреспондентом Си-эн-эн, умело спекулировавшим на чувствах американцев, являлась К. Аманпор – жена официального представителя госдепартамента США Дж. Рубина. Следует отметить, что использование корреспондента-женщины для освещения сюжетов о зверствах сербов в Косово и Метохии, страданиях косоварских женщин и детей имело сильное психологическое воздействие на американскую аудиторию.

Только в течение первых двух недель операции в Косово и Метохии Си-эн-эн подготовила более 30 статей, которые были размещены в Интернете. В среднем каждая статья содержала около десяти упоминаний о Т. Блэре со ссылками на официальных представителей НАТО. Примерно столько же раз в каждой статье использовались слова "беженцы", "этнические чистки", "массовые убийства". В то же время упоминание о жертвах среди мирного населения Югославии встречалось в среднем 0,3 раза. Анализ содержания текста сообщений позволяет сделать вывод о том, что проводимые психологические операции были хорошо подготовлены и отработаны.

Одним из безотказных приемов воздействия на аудиторию стало использование так называемых объективных цифр и документальных данных. Так, один из аналитиков Си-эн-эн заявил о будто бы имевшем место факте использования 700 албанских детей для создания банка крови, предназначенного для сербских солдат. Такая дезинформация, естественно, произвела сильное впечатление на общественное мнение Запада.

Деятельность Си-эн-эн во взаимодействии с другими СМИ, а также с группами психологических операций ВС США была рассчитана на максимальный охват аудитории, возможность активного ведения дезинформации и включала в себя разнообразные формы подачи материалов с учетом восприимчивости аудитории.

В качестве вспомогательных методов по оказанию психологического давления на "несговорчивых" югославов американские специалисты избрали: введение против Югославии полной экономической блокады; инсценировку (провоцирование) гражданского неповиновения, массовых митингов и демонстраций протеста; нелегальные подрывные и террористические акции.

В ходе информационного противоборства на этапе подготовки агрессии НАТО удалось создать необходимые международные условия для своих силовых акций и их поддержки в международных организациях. Выполнение других задач, связанных с разрушением единства народов СРЮ в отстаивании своих национальных интересов, было не столь успешным.

Несмотря на сильнейшее информационно-психологическое воздействие со стороны США и НАТО и неблагоприятный информационный фон, руководство СРЮ в целом достаточно умело действовало в сфере управления информацией, успешно противостояло информационно-психологическому давлению. В ходе конфликта не было зафиксировано случаев частичной или полной потери контроля над ситуацией со стороны югославских институтов власти из-за нарушения информационной инфраструктуры.

Информационное обеспечение действий войск (сил) НАТО в ходе военного конфликта планировалось руководством блока по следующим направлениям:

- применение разведки для обеспечения войск (сил) необходимой информацией;
- принятие мер по введению противника в заблуждение;
- обеспечение оперативной скрытности;
- проведение психологических операций;
- применение боевых электронных средств с целью последовательного поражения всей информационной системы и личного состава;
- разрыв информационных потоков;
- ослабление и разрушение системы боевого управления и связи противника, принятие необходимых мер по обеспечению защиты своей аналогичной системы.

Наибольшее внимание в планах уделялось реализации следующих основных способов ведения информационной войны:

- применению тяжелого вооружения для полного разрушения штабквартир, командных пунктов и центров боевого управления войск (сил) югославской армии;
- использованию соответствующих электронных средств и электромагнитного оружия для подавления и нейтрализации работы центров сбора информации ВС Югославии, для выведения из строя его средств связи и радиолокационных станций;
- введению в заблуждение югославских органов, ответственных за сбор, обработку и анализ разведывательной информации о противнике посредством имитации подготовки и проведения наступательных действий;
- обеспечению оперативной скрытности посредством строгого соблюдения режима секретности и воспрепятствования доступа противника к своей информации;
- проведению психологических операций, особенно с использованием телевидения, радио, печати для подрыва морального духа войск и населения СРЮ.

При реализации перечисленных способов ведения информационной войны важнейшими формами информационного воздействия были информационно-пропагандистские акции, радиоэлектронная борьба, дезинформация.

Использовались также специально разработанные методики и новые технологии разрушения баз данных, нарушения работы югославских компьютерных сетей.

В то же время повсеместно занижались боевые потери блока, замалчивалась информация о просчетах руководства НАТО, гибели мирного населения, выступлениях мировой общественности против продолжения и эскалации военных действий.

Таким образом, главной целью информационно-психологического воздействия США и руководства НАТО на население и вооруженные силы стран – участниц вооруженного конфликта явилось формирование такого общественного мнения, которое в значительной степени оправдывало бы агрессию ОВС альянса против суверенного государства.

Однако тенденциозный, агрессивный характер информационного воздействия, осуществляемого НАТО в рамках начавшейся операции, впервые вызвал активное противодействие со стороны Белграда. Анализ событий показывает, что руководство США и НАТО на первом этапе операции оказались не в полной мере готовы к таким ответным действиям СРЮ. Подтверждением тому являются не только негативные для НАТО результаты социологических опросов, но и конкретные действия альянса, предпринятые уже по ходу второго этапа операции для того, чтобы вернуть утраченную инициативу в информационном противоборстве.

Используя все возможности СМИ, военно-политическому руководству Югославии удалось временно перехватить инициативу в информационно-психологическом противоборстве. Югославские СМИ, задействованные в пропагандистской кампании, удачно использовали факты жертв среди гражданского сербского и албанского населения Косово и Метохии, нарушений ОВС НАТО основных положений Женевских конвенций и дополнительных протоколов к ним, а также поддержку политических, религиозных и общественных деятелей России, Украины, Белоруссии и других государств.

Проведенные контрмеры вызвали всплеск патриотических чувств среди населения Югославии и подъем морально-психологического состояния военнослужащих ВС СРЮ. За счет ограничения передвижения иностранных журналистов, введения запретов на распространение определенной информации руководство СРЮ добилось сокращения количества сообщений СМИ негативного характера о проводимой им политике.

Таким образом, своевременно принятые меры политическим и военным руководством СРЮ на первом этапе операции "Союзническая сила" помешали США и блоку НАТО убедить мировую общественность в адекватности методов и способов проведения военной операции в Югославии, справедливости ее целей и задач. В результате в мировом общественном мнении произошел определенный раскол в отношении политики США и НАТО на Балканах.

Временные неудачи США и его союзников по западному альянсу в информационно-психологическом противоборстве с Югославией были также обусловлены и многочисленными ошибками, которые были допущены руководством НАТО в сфере связей с общественностью. Так, настоящий провал произошел при интерпретации руководителями НАТО факта авиационного удара по колонне беженцев в Косово и Метохии 14 апреля 1999 года. Пресс-службе альянса потребовалось пять дней, чтобы в конце концов предоставить собственную более или менее ясную версию случившегося.

Несогласованность действий руководителей блока и его пресс-службы наблюдалась также и при оправдании авиационных ударов ОВВС по зданию посольства Китая в Белграде 8 мая, транспортным средствам (12 апреля, 1, 3, 5, 30 мая) и жилым кварталам в городах Алексинац (5 апреля), Приштина (9 апреля), Сурдулица (27 апреля, 31 мая), Софии (28 апреля), Ниш (7 мая), Крушевац (30 мая), Нови-Пазар (31 мая) и другим объектам.

Участившиеся провалы и упущения в работе пресс-службы НАТО привели к тому, что в ходе второго этапа операции в штаб-квартире блока в Брюсселе произошла серьезная реорганизация информационно-пропагандистского аппарата НАТО. Аппарат пресс-службы был усилен опытными специалистами в области "паблик рилейшнз", в том числе организаторами предвыборных кампаний в США и Великобритании.

Для восстановления утраченного в информационном противоборстве превосходства НАТО предприняло целый ряд решительных мер.

Во-первых, ряд ведущих мировых радиостанций ("Голос Америки", "Немецкая волна", Би-Би-Си и др.) значительно увеличили интенсивность радиовещания в УКВ-диапазоне на страны Балканского региона на албанском, сербохорватском и македонском языках. При этом радиостанции использовали американские передатчики, которые в срочном порядке были установлены на границах с Сербией. Передачи информационно-психологической направленности из-за пределов воздушного пространства СРЮ осуществлялись силами авиационной группы 193-го авиакрыла сил специальных операций национальной гвардии ВВС США с бортов самолетов EC-130E/RR.

Во-вторых, с целью подрыва информационно-пропагандистского потенциала Югославии ОВВС НАТО нанесли ракетно-бомбовые удары по теле- и радиостанциям, студиям и ретрансляторам, редакциям СМИ, большинство которых было уничтожено, что фактически означало ликвидацию системы телерадиовещания СРЮ.

В-третьих, на исходе второго месяца вооруженного конфликта под давлением НАТО совет директоров европейской телевизионной компании "ЕУТЕЛСАТ" принял решение о запрете для компании "Радио и телевидение Сербии" вести вещание через спутник. В результате Сербское государственное телевидение лишилось последней возможности транслировать передачи на страны Европы, а также на значительную часть территории своей республики.

В-четвертых, силами психологических операций ВС США над территорией Югославии было разбросано более 22 млн. листовок с призывами к сербам выступить против президента С. Милошевича и способствовать "скорейшему завершению операции объединенных сил НАТО.

В-пятых, впервые мощная информационная поддержка крупной военной операции НАТО была развернута в сети Интернет. В ней было размещено более 300 тыс. сайтов, посвященных или в разной степени затрагивающих косовскую проблему и военную операцию альянса а Югославии. Подавляющее большинство указанных сайтов было создано непосредственно или при содействии американских специалистов по компьютерным технологиям, что, безусловно, повысило эффективность пропагандистской кампании НАТО.

В итоге, несмотря на отдельные сбои, руководство НАТО сумело переломить ситуацию в информационно-психологическом противоборстве с Югославией и завоевать информационное превосходство. Информационно-пропагандистский аппарат альянса в целом выполнил поставленные перед ним задачи, своевременно внес коррективы в свою деятельность, разработал и применил новые формы и методы информационно-психологического воздействия на противника.

С другой стороны, ход боевых действий показал, что умелое управление информацией со стороны руководства СРЮ в определенной степени позволило противостоять информационно-психологическому воздействию со стороны НАТО на население и вооруженные силы страны.

Еще одной составляющей информационного противоборства в операции "Союзническая сила" явилось информационно-техническое противостояние ОВС НАТО и ВС СРЮ.

Борьба за информационное доминирование развернулась прежде всего в сфере электронных средств разведки, обработки и распространения информации ОВС НАТО при активном использовании современных средств и систем разведки, связи, радионавигации и целеуказания. В связи с этим соответствующие подразделения ОВС НАТО провели широкомасштабные акции по поражению важнейших пунктов управления ВС СРЮ, других элементов государственной и военной информационной инфраструктуры Югославии, а также подавлению находящихся на вооружении югославской армии систем и средств радиосвязи и радиолокационной разведки.

В ходе нанесения авиационных ударов по объектам информационной инфраструктуры ОВВС альянса использовали следующие виды нового оружия:

- управляемые авиабомбы JDAM с наведением по сигналам космической радионавигационной системы GPS (США);
- управляемые авиабомбы JSOW и WCMD;
- авиабомбы для вывода из строя средств радиолокации ("И"-бомбы, обладающие способностью генерировать мощные электромагнитные импульсы в радиодиапазоне частот).

Полной дезорганизации системы управления ВС Югославии удалось избежать лишь благодаря комплексному применению защитных мер, включающих оперативную маскировку, радиоэлектронную защиту и противодействие разведке противника. Творчески используя опыт иракских ВС в борьбе с МНС во время войны в Персидском заливе, ВС СРЮ удалось отразить большинство ударов интеллектуальным оружием, сохранить большую часть своего вооружения и военной техники, в том числе средств радиосвязи, радиотехнической и радиолокационной разведки.

Большое значение для сохранения боеспособности армии имели:

- своевременный перевод системы управления группировками войск (сил) ВС Югославии на полевые пункты управления;
- периодическая передислокация частей и подразделений;
- маскировка вооружения и военной техники;
- устройство ложных позиций, в том числе с использованием надувных макетов тяжелого вооружения;
- введение режимных ограничений на работу радиоэлектронных средств.

Другой важнейшей составляющей информационно-технического противоборства явилась борьба за информацию в вычислительных системах. Югославские хакеры неоднократно пытались проникнуть через сеть Интернет в локальные вычислительные сети, используемые в штабах ОВС НАТО. Массовые запросы серверов этих сетей в отдельные периоды времени затруднили функционирование электронной почты. И хотя действия хакеров имели эпизодический характер, применение информационного оружия следует считать перспективным направлением информационного противоборства.

Таким образом, можно заключить, что войска НАТО, оснащенные информационными технологиями, имеют боевой потенциал, троекратно превышающий эффективность боевого применения обычных частей. Анализ боевых действий армии США показал, что информационные технологии обеспечивают сокращение среднего времени подлета и подготовки к атаке ударных вертолетов с 26 до 18 минут и увеличение процента поражения целей ПТУРами с 55 до 93 проц. Обработка и передача донесений в вышестоящие штабы в звене "рота—батальон" сокращается с 9 до 5 минут, вероятность дублирования телеграмм снижается с 30 до 4 проц., передачи подтверждающей информации по телефонным линиям — с 98 до 22 проц.

Однако, как показывает анализ событий, то, что привело к ожидаемым результатам в Панаме и частично в Ираке, в Югославии оказалось малоэффективно. Так, в ответ на бомбардировки и массированное информационно-психологическое воздействие народ Югославии продемонстрировал единство и согласие, в том числе и среди недавних политических противников, а многократный перевес войск стран — участниц агрессии против Югославии в личном составе и технической оснащенности не дал ожидаемых результатов при ведении широкомасштабных боевых действий. Опираясь на это, можно заключить, что даже самые современные информационные технологии вряд ли

когда-либо могут заменить осознание каждым военнослужащим целей и характера войны в защиту территориальной целостности и независимости своей страны.

Безусловно, США и НАТО, обладающие более совершенными методами и средствами информационного противоборства, добились в ходе военного конфликта подавляющего превосходства в информационной сфере. Вместе с тем активные действия военно-политического руководства Югославии по нейтрализации информационно-психологических воздействий со стороны НАТО позволили ослабить информационный натиск на личный состав ВС СРЮ и население страны, а на одном из этапов даже перехватить инициативу в этом противоборстве.

Стратегия оборонительных военных действий ВС Югославии, ограниченность средств ведения радиоэлектронной борьбы, отсутствие методологии применения информационного оружия не позволили им провести комплекс мероприятий по активному информационно-техническому воздействию на системы управления, разведки, навигации и целеуказания противника. Это обусловило поражение ВС СРЮ в информационном противоборстве с ОВС НАТО.

Можно констатировать, что информационное противоборство в операции "Союзническая сила" занимало значительное место в действиях противостоящих сторон. Полученный опыт, а также перспективы технического развития дают основание выделить этот вид противоборства в рамках вооруженной борьбы в отдельную область противостояния между государствами или союзами государств. Особенность такого противостояния заключается в скрытности мероприятий, находящихся в контексте общей политики государств, преследующих свои национальные интересы. Администрация США и руководства других стран-участниц НАТО *развернули мощнейшую пропагандистскую* кампанию и провели ряд операций в ходе информационной войны против Югославии, которая, однако, не сломила волю югославского народа, особенно ее вооруженных сил, их решимости в борьбе с агрессорами. В то же время благодаря активному использованию новейших информационных технологий общественное мнение в США и в большинстве стран Западной Европы оказалось на стороне инициаторов и виновников военного конфликта на Балканах.

Учитывая большие возможности и достаточно высокую эффективность структур НАТО по информационному воздействию в военных конфликтах, следует ожидать, что руководство блока будет активно применять его в ходе подготовки и ведения возможных военных действий. Вследствие этого можно заключть, что роль и значение информационного противоборства в военных конфликтах XXI века будет увеличиваться.

Гриняев С.Н.

ИНФОРМАЦИОННАЯ ВОЙНА: ИСТОРИЯ, ДЕНЬ СЕГОДНЯШНИЙ И ПЕРСПЕКТИВА

Сегодня много говорится об «информационной войне». Однако вряд ли кто сможет точно ответить, что это такое. Более того, даже специалисты не смогут ответить на вопрос о том, когда же все-таки родилось само словосочетание «информационная война», когда впервые был поставлен вопрос о том, чтобы рассматривать информацию в качестве оружия? Далее, если выяснить эту информацию и дать ответы на поставленные вопросы, то, несомненно, сразу встанет целый ряд подобных вопросов, например, что есть информационная война? Какими средствами она ведется и, что ставится целью этой войны? Считать ли нападения хакеров военными действиями, если да, то какие средства ответа будут адекватными? Ниже мы попробуем дать ответы на эти и, возможно, другие вопросы по затронутой теме. Итак.

Первоначально некто Томас Рона использовал термин «информационная война» в отчете, подготовленным им в 1976 году для компании Boeing, и названный «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года. К тому времени было достигнуто единое понимание того, что информация может быть как целью, так и оружием.

В связи с появлением новых задач после окончания «холодной войны» термин «информационная война» был введен в документы Министерства обороны США. Он стало активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления». Эта публикация излагала принципы борьбы с системами контроля и управления как применение информационной войны в военных действиях. Публикация определяет борьбу с системами контроля и управления как: «объединенное использование приемов и методов безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разру-

шения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое». В этом документе была определена организационная структура, порядок планирования, обучения и управления ходом операции. Наиболее важным является то, что эта публикация определила понятие и доктрину войны с системами контроля и управления. Это было впервые, когда Министерство обороны США, определил возможности и доктрину информационной войны.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции «Force XXI»). В ее основу было положено разделение всего театра военных действий на две составляющих - традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину «*кибераневра*», которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин «human network»).

Определение информационной войны. В октябре 1998 года, Министерство обороны США вводит в действие «Объединенную доктрину информационных операций». Первоначально эта публикация называлась «Объединенная доктрина информационной войны». Позже она была переименована в «Объединенную доктрину информационных операций». Причина изменения состояла в том, чтобы разъяснить отношения понятий информационных операций и информационной войны. Они были определены, следующим образом:

информационная операция: действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем;

информационная война: комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Как указывают американские военные эксперты, информационная война состоит из действий, предпринимаемых с целью достижения *информационного превосходства* в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Информационное превосходство определяется как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое. Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Информационное превосходство позволяет иметь реальное представление о боевой обстановке и дает интерактивную и высокоточную картину действий противника и своих войск в реальном масштабе времени. Информационное превосходство является инструментом, позволяющим командованию в решающих операциях применять широко рассредоточенные построения разнородных сил, обеспечивать защиту войск и ввод в сражение группировок, состав которых в максимальной степени соответствует задачам, а также осуществлять гибкое и целенаправленное материально-техническое обеспечение.

Информационное противоборство осуществляется путем проведения мероприятий направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA).

Деструктивное воздействие на системы управления и принятия решений достигается путем проведения психологических операций (Psychological Operations, PSYOP), направленных против персонала и лиц, принимающих решения и оказывающих влияние на их моральную устойчивость, эмоции и мотивы принятия решений; выполнения мероприятий по оперативной и стратегической маскировке (OPSEC), дезинформации и физическому разрушению объектов инфраструктуры.

Какова ситуация сегодня? Пару лет назад Центральное разведывательное управление (ЦРУ) упоминало только Россию и Китай в качестве основных источников угрозы из киберпространства. Сегодня американские эксперты отмечают, что уже более 20 стран планируют и осуществляют различные виды информационных операций, направленных против Соединенных Штатов. ЦРУ отмечает, что ряд противостоящих США государств, включают информационную войну как часть их новых военных доктрин.

Рассекреченная оценка угрозы, проведенная Военно-морским флотом США, выделяет Россию, Китай, Индию и Кубу в качестве стран, которые открыто подтвердили политику подготовки к информационной войне, и которые

быстро развивают их способности в этом направлении. Северная Корея, Ливия, Иран, Ирак и Сирия по сообщениям имеют некоторую способность к движению в этом направлении, а Франция, Япония и Германия уже весьма активны в этой области.

Как же видят в разных государствах основные подходы к ведению информационной войны?

Россия. До последнего времени у нас практически не существовало ясной государственной позиции по этой проблеме, что, собственно, и привело к поражению в Холодной войне. Только в сентябре 2000 года Президентом РФ была подписана Доктрина информационной безопасности России. В отличие от подхода, обозначенного США, в российской Доктрине на первое место ставится обеспечение информационной безопасности индивидуального, группового и общественного сознания.

Для реализации основных положений Доктрины и обеспечения информационной безопасности России было создано Управление информационной безопасности в Совете Безопасности РФ.

Сегодня в работах по разработке отечественного представления информационной войны занимаются Министерство обороны, ФАПСИ, ФСБ и знаменитое Управление «Р» МВД, которое проводит расследования преступлений в высокотехнологической сфере информационных технологий.

США. Деятельность американской администрации в области защиты критической инфраструктуры берет свое начало с формирования Президентской комиссии по защите критической инфраструктуры (President's Commission for Critical Infrastructure Protection) в 1996 году. Отчетный доклад этой комиссии выявил уязвимости национальной безопасности США в информационной сфере. Итоги работы комиссии были положены в основу правительственной политики в области обеспечения информационной безопасности критической инфраструктуры, сформулированной в Директиве президента № 63, подписанной в июне 1998 года (PDD-63).

Во исполнение указаний президента, обозначенных в этой директиве, был разработан Национальный план защиты информационных систем США, подписанный президентом 7 января, 2000 года. На реализацию этого плана было затребовано 2.03 миллиарда долларов из федерального бюджета.

В феврале 2001 года Конгрессу США был представлен отчет о ходе реализации PDD-63. Одной из наиболее важных выполненных Министерством обороны США работ в этом направлении, является существенное продвижение по пути совершенствования приемов и методов работы с доказательствами компьютерных преступлений, что имеет большое значение при проведении расследований любых инцидентов, связанных с применением вычислительной техники. Так 24 сентября 1999 года была открыта Компьютерная судебная лаборатория Министерства обороны (Defense Computer Forensics Laboratory, DCFL). Это – одна из наиболее современных структур, предназначенная для обработки компьютерных доказательств в преступлениях и мо-

шенничествах, а также при проведении контрразведывательных мероприятий для всех организаций, проводящих криминальные и контрразведывательные исследования. Управление специальных исследований Военно-воздушных сил США определено в качестве Исполнительного агентства для DCFL. В настоящее время DCFL имеет 42 позиции для исследователей и судебных приставов, позволяющие обрабатывать компьютерные доказательства наряду со звуковой и видео информацией в судебных делах в самом широком диапазоне: от детской порнографии до вторжений в компьютеры и шпионажа. Эта лаборатория министерства обеспечивает поддержку ФБР по вопросам расследования компьютерных преступлений. Специалисты DCFL уже накопили определенный потенциал и навык работы с инструментальными средствами анализа информации в ходе ряда успешных мероприятий по идентификации групп хакеров, а также при нейтрализации уязвимости в нескольких контрразведывательных операциях, связанных с деятельностью по защите национальных сети ЭВМ. Среди последних - такие нашумевшие мероприятия как "Солнечный восход", "Цифровой демон" и "Лабиринт лунного света" ("Solar Sunrise", "Digital Demon", "Moonlight Maze").

С целью улучшения способности активно защищать информационные системы и компьютеры была создана Объединенная оперативная группа по защите компьютерной сети Министерства обороны (Joint Task Force for Computer Network Defense, JTF-CND), а главнокомандующий космического командования принял полную ответственность за защиту сетей ЭВМ министерства с 1 октября 1999 года. Как отмечают авторы отчета, в ходе инцидента с вирусом "Мелисса" в марте 2000 года, JTF-CND, совместно с Группой реагирования на чрезвычайные ситуации с вычислительной техникой Министерства обороны (Computer Emergency Response Team, CERT), оказалась способной быстро оценить угрозу, сформировать оборонительную стратегию и направить ход соответствующих оборонительных действий. Далее, в мае 2000 года, в ходе эпидемии компьютерного вируса "LOVELETTER" был продемонстрирован еще один пример четких действий JTF-CND. Персонал JTF быстро идентифицировал потенциальное повреждение и обеспечил своевременное уведомление подразделений, служб и агентств министерства, которые позволили им эффективно ответить на вторжение.

С 2000 года Министерством обороны начата работа с союзниками по вопросу обеспечения информационной безопасности: Канада имеет официального представителя, работающего в JTF-CND, развивается система разделения информации между Министерствами обороны в соответствии с основными положениями Меморандума о понимании и Концепции действий подписанными с канадской стороной.

Проведены работы по созданию системы сигнализации при обнаружении уязвимости информационной безопасности (Information Assurance Vulnerability Alert, IAVA) для распределения информации об уязвимости всем подразделениям и службам Минобороны. В 1999 году этой службой было

подготовлено и выпущено 11 предупреждений (IAVT), 3 бюллетеня (IAVBs) и 20 технических консультаций. В 2000 году были выпущены 3 предупреждения, 3 бюллетеня и 9 технических консультаций. Агентство информационных систем Минобороны (Defense Information System Agency, DISA) сформировало банк данных, для немедленного распределения информации об уязвимости каждому администратору системы вместе с краткой информацией о возможных ответных действиях по локализации последствий.

Безусловно, за прошедший год американскими коллегами проделана большая работа. Однако следует задуматься, а насколько она оказалась эффективной?

Информация, доступная по каналам Интерент, позволяет сделать вывод о том, что уровень информационной безопасности систем Минобороны США, не смотря на реализованные мероприятия, увеличился незначительно. Атаки китайских хакеров на системы Минобороны в период кризиса, вызванного инцидентом с разведывательным самолетом Е-3, оказались достаточно эффективными.

Согласно ряду заявлений сотрудников администрации США, созданная национальная система информационной безопасности, оказалась слишком тяжеловесной и неповоротливой. В ряде случаев процесс доведения информации тормозился в силу бюрократических проволочек, что приводило к неприятным последствиям.

Во многих случаях при появлении нового вида компьютерных вирусов противоядие не было своевременно найдено ни сотрудниками CERT, ни JTF-CND.

Существенным препятствием в достижении поставленных целей остается нехватка квалифицированного персонала для работы в сфере обеспечения информационной безопасности, о чем свидетельствуют попытки привлечения студентов-компьютерщиков на работу в федеральные ведомства по контрактам в обмен на оплату их обучения в институтах.

Китайская Народная Республика. Китай уже давно включил термин «информационная война» в лексикон своих военных специалистов. Сегодня он неуклонно движется к формированию единой доктрины информационной войны. Фактически, если революция в военном деле определяется как существенное изменение в технологии, дающее преимущество в военном обучении, организации, стратегии и тактике военных действий, то, возможно Китай из всех стран сегодня испытывает истинную революцию в киберпространстве.

Китайская концепция информационной войны включает уникальные китайские представления о войне вообще, основанные на современной концепции «народной войны», 36 стратегем великого Сун Цзы, а также местных представлениях о том, как воевать на стратегическом, оперативном и тактическом уровне. Многое из его подхода имеет отношение к акценту на обмане, войне знаний и поиске асимметричных преимуществ над противником. Информационная война определена как «переход от механизированной войны

индустриального возраста к... войне решений и стиля управления, войне за знания и войне интеллекта».

Китай развивает концепцию Сетевых сил (воинские подразделения численностью до батальона), которые состояли бы из высококлассных компьютерных экспертов, обученных в множестве государственных университетов, академий и учебных центров. Основной акцент делается на привлечение активной молодежи.

На сегодняшний момент было проведено уже несколько крупномасштабных учений этих сил по отработке концепции информационной войны.

Великобритания. Британское представление об информационной войне подобно таковому в Соединенных Штатах. Это определение информационной войны как действий, воздействующих на информационные системы противника, при одновременной защите собственных систем. Кроме того, Великобритания использует юридическую структуру, основанную на существующих законах, которая в значительной степени может применяться к действиям в киберпространстве – Regulation of Investigatory Powers Act (RIP), принятый в 2000 году. Он предлагает, что нападения на информационные системы может рассматриваться как обычное уголовное преступление со всеми вытекающими последствиями. Данный акт позволяет британскому правительству перехватывать и читать электронную почту, а также требовать расшифровки личных файлов по требованию государственных чиновников.

Германия. Главным образом немецкое представление информационной войны совпадает с таковым в США и Великобритании. Оно включает ведение наступательной и оборонительной информационной войны для достижения национальных целей. Вместе с тем Германия имеет тенденцию быть несколько более систематичной, чем Соединенные Штаты, что свойственно немецкой педантичности. При определении угроз и возможных ответов, иностранные государства рассматриваются отдельно от негосударственных объединений (типа политических партий, международных организаций и средств массовой информации), преступные сообщества (организованное преступные группы, хакеры и т.д.), и индивидуумы (включая религиозных фанатиков и др.).

В двух случаях, однако, немецкое представление об информационной войне может отличиться от американского. Германия включает управление средствами массовой информации как элемент информационной войны. Кроме того, Германия отдельно вводит определение для экономической информационной войны, подобной французам (см. ниже). Это является следствием двух причин: Германия оценила потенциал возможного экономического ущерба, который может быть нанесен немецкому бизнесу и экономике; Германия, возможно, испытала существенные экономические потери от Франции в операциях индустриального шпионаж в киберпространстве; также Германия может искать пути смягчения последствий потенциальных вторжений.

НАТО. По сообщениям существует секретное натовское определение информационной войны, но оно не доступно в открытой печати. На

проведенной объединенным штабом НАТО в начале 200 года конференции по проблемам информационной войны все участники пользовались определениями, разработанными в их странах. Вместе с тем известно, что натовское определение во многом схоже с аналогичным американским определением.

Франция. Французы рассматривают концепцию информационной войны, состоящей из двух главных элементов: военной и экономической (или гражданской). Военная концепция предполагает несколько ограниченную роль информационных операций. Их военная концепция видит место информационным действиям, имеющим место в значительной степени в контексте конфликтов малой интенсивности или в миротворческих операциях. В этом контексте, союзники не рассматриваются противниками.

Напротив, экономическая или гражданская концепция включает более широкий диапазон потенциального применения информационных операций. Французское представление принимает намного более широкое и более глубокое представление для конфликта в экономической сфере. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США. Их подход к экономическому конфликту учитывает тот, чтобы быть и союзником и противником одновременно. Французы даже имеют экономическую школу для информационной войны.

Франция активно формирует структуры по контролю ее граждан в киберпространстве. Есть информация о том, что французы создали собственную версию системы «Эшелон» (по сообщениям американской прессы система направлена на перехват фактически всех частных глобальных коммуникаций). Frenchelon, так некоторые назвали эту систему, по сообщениям используется для контроля и анализа французских коммуникаций особенно в районе Парижа.

Что делать? Анализ показал, что многие страны мира сейчас создают у себя системы защиты от информационной агрессии и американской культурной экспансии. В той же Франции, к примеру, по телевидению разрешается показывать не более 50% иностранных фильмов, абсолютное большинство которых, как известно, американские. Наше государство пока не приняло никаких существенных мер по защите своих граждан.

Учитывая сложность и специфичность информационного воздействия, для обеспечения безопасности Российской Федерации стране жизненно необходим специальный координационный управляющий орган по контролю за созданием и применением информационного оружия. Необходимо также создание межведомственного Аналитического центра по разработке новейших информационно-психологических технологий на базе Академии ФСБ, МИ МВД при возможном патронаже Совета Безопасности РФ.

Следует задуматься о формировании мощного государственного холдинга масс-медиа, работающего в тесном контакте со специалистами из Аналитического центра.

Для решения встающих проблем требуется объединение усилий в научных исследованиях проблем информационной войны, обеспечения информационной безопасности, а также подготовке кадров как исследователей, так и журналистов "нового типа".

К сожалению, и это надо признать, Россия пока остается, практически единственной страной, которая последовательно добивается на международном уровне подобной постановки вопроса. Уже проделана определенная работа, подготовлены и доложены материалы по вопросам информационной безопасности на 53 и 55 сессиях Генеральной ассамблеи ООН. Однако этого явно недостаточно. Необходимо приложить все усилия для того, чтобы в XXI веке достижения в области информационных технологий служили исключительно на благо человечества. Упустив момент сегодня, завтра мы рискуем встать на порог очередного витка гонки вооружений. В этом случае опасность развязывания глобальной информационной войны, объектом воздействия в которой станет самое тонкое достижение эволюции — сознание человека, станет реальностью.

Источники:

1. Thomas P. Rona, "Weapon Systems and Information War", Boeing Aerospace Co., Seattle, WA, 1976.
2. Joint Pub 3-13.1 "Command and Control Warfare", DOD US, February 1996.
3. Joint Pub 3-13 "Information Operations", DOD US, December 1998.

Желтов А.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ *

Увеличение зависимости современного общества от цифровых технологий, а также продолжающееся их проникновение в область принятия решений, поставило перед государствами ряд проблем, связанных с обменом, манипулированием и проблемой секретности информации. Информационная безопасность стала одним из ключевых аспектов межгосударственных отношений и внутренней политики стран. Развитие информационного общества, возведенное в ранг государственной политики США, стран ЕС, и, с недавних пор, России, еще больше добавляет актуальности изучению данной проблемы.

Информационное общество еще далеко от окончательного формирования, и в процессе трансформации и развития оно затрагивает самые различные области, включая систему международных отношений. Международные

отношения на современном этапе также трансформируются из биполярной системы в нечто новое, отличающееся от всего предшествующего на уровне парадигмы. В современном мире существует масса признаков и взаимопротиворечащих тенденций, свидетельствующих об изменениях как в системе международных отношений, так и в общественном сознании:

- Появление на международное арене большого количества новых акторов (международных организаций различного характера, транснациональных кампаний и т.д.).
- Увеличение количества и сложности факторов, влияющих на принятие решений, усложнение и изменение процесса принятия решений в сторону принятия коллективных решений.
- Глобализация ряда проблем, и в связи с этим - делегирование полномочий национальных государств наднациональным структурам для более эффективного их разрешения.
- Развитие международных средств массовой информации позволяет говорить о таких явлениях, как «международное общественное мнение» и манипулирование им, «феномен CNN», и т.д.
- Лавинообразное развитие сети Интернет и зависимости общества от нее, развитие электронной коммерции, рынка информационных услуг, позволяет ввести термин «мировое информационное общество».

Несмотря на то, что контуры новой системы лишь начинают формироваться, можно утверждать, что концепции международных отношений и связанные с ними подходы к проблемам безопасности, основанные на теориях и постулатах времен Холодной войны, не способны адекватно отражать происходящие процессы. Особенно это утверждение касается такой динамично развивающейся отрасли, как отношения в информационной сфере и связанные с ними проблемы безопасности. Исходя из этого, существующие политики в области информационной безопасности, которые во многом являются наследниками страхов периода Холодной войны, можно назвать неадекватными реалиям и потенциалу информационного общества. Данная работа представляет собой попытку анализа существующих подходов к информационной безопасности на основании существующих предпосылок формирования новой системы международных отношений.

Под информационной безопасностью будет пониматься защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.[1]

Это определение во многом не отражает аспекты информационной безопасности, представленные в «Доктрине информационной безопасности РФ», но, в целом, соответствует концепциям, принятым в Европе и США. Такой узкий взгляд на данную проблему здесь будет более предпочтительным,

[1] http://risa.ru/images/stories/Convention/zheltov.rtf

т.к. речь будет идти об информационной безопасности в глобальном масштабе. Усложнение проблемы включением в нее национальных ценностей, культурной идентичности и т.д. чрезмерно усложнит поставленную перед исследователем задачу. В дальнейшем, под терминами «информационная сфера», «информационное общество» и т.п. следует понимать те категории лиц и объектов, которые непосредственно связаны с созданием и использованием электронных и компьютерных технологий, Интернет, электронными СМИ, защитой информации.

Информационная безопасность, в той форме, в которой она будет рассматриваться в данной работе, и учитывая вышеизложенные особенности современного мира и системы международных отношений, имеет ряд характерных черт. Эти черты отличают ее от других видов безопасности, т.е. военной, экономической и т.д., и служат критериями для анализа адекватности подходов к ней:

- Информационная безопасность затрагивает права человека на информацию, свободу слова, тайну переписки и т.д. Вследствие этого, грань между ее обеспечением и «информационной диктатурой»[2] очень тонкая и размытая. В этой области происходит столкновение взглядов и интересов различных групп лиц, по-разному относящихся к данной проблеме.
- В информационной сфере невозможно заранее локализовать «вероятного противника» и идентифицировать источник угрозы. Таким образом, любые превентивные меры носят лишь относительно объектно-ориентированный характер. Также нет необходимости в четкой концепции «врага», поскольку он неидентифицируем, и возможно, даже не существует, т.е. является плодом воображения аналитиков.
- Стремительное развитие информационных технологий делает их регулирование чрезвычайно сложным на всех уровнях. Для информационной безопасности это означает невозможность долгосрочного планирования, быстрое изменение характера угроз, сложность оценки последствий конфликтов в информационной сфере.
- Огромное количество акторов в информационной сфере (спецслужбы, корпорации всех уровней, бизнесмены, хакеры, простые пользователи сетей) и принципиально новая расстановка сил. Небольшая группа хакеров, в принципе, способна причинить существенный ущерб инфраструктуре крупной компании или государства, или некоторым образом изменить ситуацию в мировой политике, похитив ценную информацию и передав ее заинтересованным сторонам.
- Развитие информационных технологий находится в большей степени под контролем индивидуумов, нежели государства, ввиду чего не совместимо с жестким контролем с его стороны. Контроль также усложняет-

1 - См. Владимир Бетелин, Владимир Галатенко. Информационная безопасность в России: опыт составления карты // Информационный бюллетень JetInfo № 1 за 1998 г.

2 - Под «информационной диктатурой» подразумевается ситуация отсутствия свободной реализации демократических прав человека в области информации.

ся прозрачностью границ, высокой ролью негосударственных образований, перманентным отставанием в развитии соответствующего законодательства.

Можно выделить два подхода к информационной безопасности в международных отношениях, условно называемые «реалистическим» и «либеральным».[3]

Данные подходы не связаны с соответствующими теориями международных отношений, т.е. с неореализмом и неолиберализмом, и отражают два отношения к проблеме информационной безопасности, распространенных среди различных групп лиц, «принимающих решения» и творящих государственную политику.

«Реалистический» подход характеризуется следующими аспектами и требованиями:

- Увеличение степени безопасности информационных систем внутри страны.
- Создание большого количества внутренних сетей, независимых друг от друга и от глобальных сетей.
- Постоянный мониторинг уровня информационной безопасности потенциальных противников, целенаправленный поиск «дыр» в их программном обеспечении, контроль над распространением информации и соответствующих технологий.
- Разработка средств ведения «информационной войны».
- Уменьшение взаимозависимости и открытости государств в информационной сфере, как следствие всего вышеперечисленного.

«Реалистический» подход, по сути, отражает современную политику обеспечения информационной безопасности, проводимую в США и, в какой-то мере, в ЕС и России. Принятые в США концепции «информационного превосходства» и «информационного сдерживания».[4]

выступают наглядной иллюстрацией применения подобного подхода. «Информационное превосходство» является военным термином, который обозначает ситуацию полной информированности о планах, действиях, намерениях противника. Технология, необходимая в военное время для достижения подобного результата, в мирное время легко позволит держать под контролем большинство электронных каналов передачи информации. «Информационное сдерживание» – наследие сдерживания эпохи Холодной войны. Оно подразумевает контроль над распространением потенциально опасных информационных технологий, разработку средств нанесения «ответного удара» и т.п. меры. Таким образом, политику США можно охарактеризовать, как стремление к созданию «информационно монополярного» мира, что являет-

3 - См. Matthew G. Devost. National Security in the Information Age.// The University of Vermont, 1995

4 - См. WHITE PAPER The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 May 22, 1998; Critical Foundations: Protecting America's Infrastructures // President's Commission on Critical Infrastructure Protection (PCCIP) 1997 Report; Practices for Securing Critical Information Assets.// Critical Infrastructure Assurance Office, 2000, Joint Vision 2020 // US Government Printing Office, Washington DC, June 2000

ся высшей точкой борьбы за собственную информационную безопасность по «реалистической» модели.

«Реалистический» подход хорош своей очевидностью, т.к. схож с различными концепциями «ядерной безопасности» и т.п. Действительно, предлагаемые в его рамках меры весьма разумны, и их применение способно снять ряд первостепенных угроз информационной безопасности, в частности, со стороны других государств и ряда индивидуумов. Вследствие этого «реалистической» точки зрения придерживаются представители спецслужб всех стран, военные, большое число политиков. Но подобный подход к обеспечению безопасности имеет ряд слабых мест. Во-первых, мониторинг активности в информационной сфере, помимо своей чисто технической сложности,[5] ряд прав человека и принципов демократии. Во-вторых, согласно известному постулату «можно сделать защиту от дурака, но только от неизобретательного», угрозы со стороны хакеров и террористических группировок не уменьшаются. Также следует упомянуть негативные последствия информационной изоляции государства для экономики, проблему международных и электронных СМИ и т.д. И наконец, «реалистический» подход требует наличия «врага», т.е. конкретной, а не абстрактной угрозы. Отсутствие «врага» ставит перед сторонниками «реализма» вопрос «от кого мы стараемся защититься?», и ответ на него является краеугольным камнем «реалистической» политики информационной безопасности.

«Либеральный» поход более расплывчатый, более идеалистичный, и его можно свести к следующему:

- Увеличение взаимозависимости государств в информационной сфере
- Обеспечение общей безопасности через создание сети международных организаций и договоров.
- Либерализация информационных отношений.

В защиту «либерального» подхода говорит отсутствие необходимости целенаправленного поиска «врагов». Общее признание «либерального» подхода позволило бы более эффективно, на основе совместных действий, бороться с компьютерной преступностью и контролировать распространение потенциально опасной информации. Однако этот подход имеет гораздо больше противников, чем сторонников, и причины подобного явления можно легко перечислить. В первую очередь, данная концепция предполагает, что отношения между государствами должны строиться в первую очередь на основе взаимного доверия и неуклонного следования заключенным договорам. Но соображения обеспечения национальной безопасности на сегодняшний день не позволяют межгосударственным отношениям выйти на тот уровень открытости, который сделал бы подобную политику эффективной. Любой государственный деятель, осмелившийся пропагандировать «либерализм», рискует быть обвиненным в преступлении против государства и т.д. Далее, «либе-

5 - По техническим аспектам данного вопроса см. Internet Law and Policy Forum Working Group on Content Blocking // http://www.ilpf.org/work/content/content.htm

ральный» подход априорно предполагает снижение ограничений на распространение информации, что однозначно не приемлют спецслужбы. И наконец, в условиях предполагаемого информационного доминирования одной державы проведение «либеральной» политики со стороны других государств выглядит, по меньшей мере, нелогично.

В принципе, можно было бы выделить третий подход к проблеме информационной безопасности, которого придерживаются люди, профессионально или на достаточно серьезном уровне занимающиеся информационными технологиями, но не участвующие в принятии решений на государственном уровне. Для них мало что значат слова о «национальных интересах», «безопасности государства» и т.д., но именно на ограничение их деятельности косвенно направлено большинство мер внутри- и межгосударственной политики обеспечения информационной безопасности. Они против любых ограничений на распространение информации и контроля над их действиями. Считается, что «спасение утопающих – дело рук самих утопающих», т.е. информационная безопасность – забота пользователей и создателей информационных технологий, а отнюдь не правительственных чиновников. Несмотря на кажущуюся дикость подобных взглядов, эти люди, несомненно, в чем-то правы, и их позицию следует учитывать.

Очевидно, что из приведенных подходов к проблеме информационной безопасности, «реалистический» заслуженно является наиболее распространенным, несмотря на все его недостатки. Идеи, выраженные в «либеральном» подходе, при всей их привлекательности для информационного общества в целом, не получают серьезной поддержки на уровне межгосударственных отношений. Казалось бы, в сложившейся ситуации нет ничего, что могло бы послужить поводом для пересмотра существующих подходов к информационной безопасности. Но необходимо еще раз подчеркнуть, что современная система международных отношений уже не та, что 10 лет назад. Слишком много новых факторов, акторов и взаимопротиворечащих тенденций появилось на международной арене, вследствие чего нельзя с уверенностью сказать, какие черты будет носить мировое сообщество еще через 10 лет. По всей вероятности, и учитывая ряд существующих тенденций, упомянутых в начале данной статьи, будущая система международных отношений, в отличие от той, что существовала последние 70 лет, будет носить мультиполярный характер с оттенком анархии. Разумеется, это лишь один из возможных вариантов развития; но в случае формирования монополярной системы все дальнейшие рассуждения теряют смысл. Гипотеза о мультиполярности кажется еще более убедительной, если принять во внимание потенциальное влияние информационных технологий на развитие международных отношений. Информационные технологии развились до современного глобального уровня только благодаря концу биполярной системы, и мультиполярность является для них оптимальной средой развития. Они, в свою очередь, диктуют мировому сообществу определенные черты новой системы международных отношений. Таким образом, будущее международное «информационное» сообщество должно

носить характер сложной саморегулирующейся системы, с минимизацией внутренних барьеров и относительно глобальной взаимозависимостью элементов. Аналогичную структуру имеет на современном этапе сеть Интернет, основное достижение современных информационных технологий.

Если принять за основу анархический системный характер развития будущей системы международных отношений и ее зависимость от информационных и т.п. быстро развивающихся технологий, напрашивается вопрос о совместимости современной «реалистической» модели информационной безопасности с чертами «информационного» общества. В информационном обществе безопасность по реалистической модели - не состояние, а ощущение, сродни проводимым в рамках гражданской обороны учениям по выживанию в условиях ядерного, химического и бактериологического поражения. Практическая значимость мер не имеет значения, важно осознание собственной защищенности. Даже создание «информационно-монополярного» мира, как уже говорилось, не принесет ситуации защищенности от информационных атак со стороны террористов и т.д., и это признают все аналитики, как российские, так и американские. Проведение «реалистической» политики информационной безопасности на международном уровне приведет либо к созданию «информационно – монополярного» мира с системой тотального контроля, либо к распаду мирового информационного общества на отдельные структуры, гонке «информационных вооружений», хаосу.

Для предотвращения возможного кризиса информационных отношений необходим радикальный отход от «реализма» в международных информационных отношениях. «Либеральная» концепция информационной безопасности, несомненно, более соответствует системному характеру развития информационного общества и международных отношений. Свобода развития информационных отношений на всех уровнях, несмотря на страхи и угрозы, связанные с ней, на глобальном уровне даст лучший результат, нежели политики «сдерживания», «нераспространения», «превосходства».

Либерализация межгосударственных информационных отношений не в коей мере не предполагает, как это может показаться на первый взгляд, полной открытости государств для получения информации о них извне. Доступ к государственным секретам, государственным и военным инфраструктурам должен оставаться максимально ограниченным, и спорить с этим нельзя. На фоне общей информационной открытости этого можно добиться путем полной независимости подобных структур и сетей, их связывающих, от общей глобальной сети и ужесточения права доступа к ним. Подобные меры не нарушают прав человека в области информации, не затрагивают ничьих интересов, и лишь незначительно усложняют управление ими. США, где множество подобных объектов соединены через Интернет, в обеспечении информационной безопасности пошли по пути ограничения доступа как непосредственно к этим узлам, так и к серверам Сети, находящимся внутри страны, создавая, условно говоря, второй Интернет.[6]

6 - Америке нужен второй Интернет // Газета.RU, 09.12.00

Подобный шаг по информационной изоляции страны нельзя считать удачным, и реакция на него однозначно не принесет пользы информационному обществу в целом.

С применением «либерального» подхода упроститься, как уже упоминалось, решение таких проблем, как компьютерная преступность, распространение «опасной» информации, регулирование электронной торговли. С «либеральной» точки зрения, информационная безопасность сравнительно близка, скажем так, экологической безопасности. Все государства рано или поздно сталкиваются с одними и теми же глобальными проблемами, и решение их в отдельно взятой стране не улучшает ситуацию в мире в целом. Только совместные усилия всех или большинства стран способны изменить сложившуюся ситуацию к лучшему.

Однако, на сегодняшний день переход к «либеральному» подходу затрудняется, во-первых, чисто технологическими трудностями, связанными с этим, и во-вторых, современной ситуацией неопределенности в международных отношениях. Под технологическими трудностями понимаются унификация национального информационного законодательства, формирование информационного права в самостоятельную отрасль международного права, разработка, принятие и имплементация соответствующих договоров. В этой области можно отметить как позитивные, так и негативные моменты, т.к. государства еще не отказались от попыток влиять национальным законодательством на наднациональные информационные процессы.

Что касается ситуации в международных отношениях, то она составляет проблему куда более сложную. Система международных отношений находится в стадии формирования, и государства еще не в состоянии выработать четкой политики по ряду вопросов. Не добавляют уверенности в завтрашнем дне действия США, которые являются образцом для подражания для стран Европы и в какой-то мере, для России. Кроме того, поскольку проблемы развития информационного общества являются прерогативой в основном развитых стран, развивающиеся страны своими действиями в этой области способны вносить дополнительный хаос в только начинающие формироваться международные информационные отношения.

Леваков А.

НОВЫЕ ПРИОРИТЕТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ США *

Трагические события, которые произошли в США 11 сентября 2001 года и повергли в шок весь мир, вновь напомнили человечеству об обратной стороне технического прогресса. Варварские террористические акты, совер-

* Информационные войны. Хрестоматия /Составители: Скиба Н.Е., Малыгин А.В., Бондаренко Е.И.. Учебное пособие для студентов высших учебных заведений, обучающихся по специальностям и направлениям «Международные отношения». – Хмельницкий. – 2003

шенные группой террористов-смертников в Нью-Йорке и Вашингтоне, стали суровым испытанием не только для правительства и спецслужб, но и для всего американского общества. К своему удивлению мы узнали, что США — это далеко не самая безопасная и благополучная страна в мире, а американцы — это не только прагматики и бизнесмены, но и патриоты своей Родины, за которую они готовы отдать жизнь, как это сделали пассажиры Боинга под Питсбургом. Сейчас, когда на волне гнева и мести, буквально захлестнувшего США, Пентагон и ЦРУ пытаются взять реванш в схватке с невидимкой Бен Ладеном в горах Афганистана, на повестку дня вновь и вновь встает вопрос о безопасности информационных технологий.

Впрочем, почему только информационных: попробуйте назвать хоть одну сферу деятельности человека (связь, транспорт, авиация, космос, энергетика, водоснабжение, финансы, торговля, наука, образование, оборона, охрана общественного порядка, медицина и др.), где сейчас не применяются эти технологии и вы поймете, насколько зависимы мы все стали от битов, чипов, модемов... — одним словом всего того, что превращает нас помимо нашей воли из "homo sapiense" в "homo informaticus". Фактически во многих развитых странах сегодня активно реализуется концепция так называемого "электронного правительства". Можно поспорить о том, что далеко не все страны и народы приемлют новый "цифровой" порядок, что высокие технологии для многих просто недосягаемы и миллионы голодных людей вообще не знают о том, что есть сотовые телефоны, спутники, персональные компьютеры и Интернет, но факт остается фактом — человечество шагнуло в новое тысячелетие, имея в своих руках инструмент столь же созидательный как и разрушительный по своим возможностям одновременно.

Как установило ФБР, террористы-камикадзе готовились к своим ударам с помощью широко доступных программ, имитирующих полет самолета над Нью-Йорком и Вашингтоном, а для передачи инструкций в процессе подготовки и планирования террористической операции по захвату самолетов — электронную почту Интернет. Разрушение комплекса зданий только в Нью-Йорке, помимо человеческих жертв повлекло за собой закрытие биржи, падение курса акций, потерю десятка тысяч каналов передачи данных, перегрузку трафика в Интернет, уничтожение информации в компьютерах сотен фирм и офисов...

Для того, чтобы лучше осознать масштабы распространения информационных технологий в современном обществе, а следовательно и степень его технологической уязвимости обратимся к опыту США — стране, откуда к нам и пришли эти высокие технологии вместе с новыми проблемами. Американцы любят повторять, что они — нация эмигрантов, страна равных возможностей, где уснув бедняком можно проснуться миллионером. Количество желающих приехать на постоянное жительство в одну их самых богатых и развитых стран мира неуклонно возрастает из года в год, несмотря на все строгости американского законодательства, жестко регулирующего въездные квоты.

США после распада СССР на протяжении последних десяти лет прочно занимают место государства-лидера со статусом мировой сверхдержавы. На земном шаре нет ни одного уголка, который не попадал бы в сферу американских национальных интересов.

Но вот парадокс – сегодня американцы вполне реально могут стать жертвами "кибернетического" Перл-Харбора, для подготовки и осуществления которого агрессору не понадобятся, как это было в прошлом, ни ракеты, ни самолеты, ни атомная бомба. Буквально в считанные минуты страна может оказаться парализованной, а через несколько часов стать ареной ужасающих по своим последствиям беспорядкам среди населения, где в охваченной паникой еще недавно благополучной демократии стихийно начнут провозглашаться новые государственные образования, до боли знакомые нам по опыту Северного Кавказа. Что это – бред сумасшедшего, сюжет фантастического триллера или очередная журналистская утка? Это – сценарий Пентагона, американского военного ведомства, по коридорам которого вот уже 10 лет витает зловещая тень угрозы информационной войны, нависшей над Америкой после войны в Персидском заливе. В ночь с 16-го на 17-ое января 1991 года, через сутки после истечения срока ультиматума ООН о выводе иракских войск с территории аннексированного 2 августа 1990 г. Кувейта, американские стратегические бомбардировщики и военные корабли нанесли удар крылатыми ракетами по военным объектам Ирака. Еще до подлета первых 50-ти крылатых ракет до целей группа армейских вертолетов внезапно на малой высоте атаковала и вывела из строя две главных иракских РЛС. Так началась операция многонациональных вооруженных сил по освобождению Кувейта "Буря в пустыне", которой суждено было войти в историю как война 21-го века. За 43 дня боевых действий Ирак потерял 4000 танков (95%), 2140 орудий (69%), 1856 БТР (65%), 7 вертолетов (4%), 240 самолетов (30%), 143 корабля (87%). Потери коалиции составили соответственно: 4 танка (0,1%), 1 орудие (0,03%), 9 БТР (0,2%), 17 вертолетов (0,9%), 44 самолета (1,7%). Общее количество убитых со стороны 700000 союзных войск составило 148 человек (0,021%), из которых примерно 30% стали жертвами "огня по своим". Потери Ирака, армия которого насчитывала свыше полумиллиона человек, оцениваются в 9000 убитых (2%), 17000 раненых (3%) и 63000 пленных (12%). Свыше 150000 солдат (28%) дезертировали из иракской армии в ходе наземного наступления.

Но не пройдет и года после внушительно одержанной военной победы, еще будут полыхать факелы нефтяных скважин Кувейта, как в Пентагоне забьют тревогу: на смену эйфории придет отрезвление. Хорошо спланированная и блестяще проведенная военная операция с применением новейшего высокоточного оружия, самолетов-невидимок, приборов ночного видения, беспилотных самолетов-разведчиков, спутников и компьютеров могла окончиться полным провалом: военно-техническое превосходство победителя в одночасье превратилось в его ахиллесову пяту.

В секретной директиве Пентагона S-3600.1 появится совершенно новое и непривычное понятие – "информационная операция", которому суждено будет совершить подлинную революцию в военном деле. Как ни парадоксально, но в основу "информационной операции" против Ирака, как это уже официально записано в уставах и наставлениях вооруженных сил США, был положен классический прием ведения войны — дезорганизация управления. Исход поединка "Давида и Голиафа" решил внезапный удар в "голову" противника, потерявшего "зрение", "слух" и "речь" почти одновременно.

За несколько недель до начала ведения боевых действий специально обученные агенты ЦРУ с помощью портативных компьютеров в Багдаде внедрили программные "вирусы-закладки", которые в назначенный день и час отключили телефонные станции и радиолокационные посты, парализовав уже в первые минуты воздушного налета систему ПВО Ирака. Есть сведения, что истребители "Мираж" иракских ВВС по этой же причине не могли использовать свои бортовые РЛС в ходе отражения налета. Это позволило союзной авиации в первые несколько часов уничтожить основные объекты иракской системы ПВО и через 10 дней завоевать превосходство в воздухе.

Оружие возмездия – баллистические ракеты "Скад", которыми Ирак будет обстреливать Израиль и Саудовскую Аравию в ответ на прицельные авиационные налеты американцев, в большинстве случаев окажется малоэффективным против зенитных ракет "Патриот" и спутников системы раннего предупреждения. На угрозы Хуссейна применить химическое оружие президент Буш хладнокровно отдаст приказ о приведении стратегической ядерной триады США в полную боевую готовность. Весь мир, затаив дыхание, будет смотреть на экранах телевизоров прямые репортажи с театра военных действий.

По иронии судьбы "непобедимой" иракской армии в январе-феврале 1991 г. было суждено получить от НАТО урок немецкого блицкрига, за который Красная армия летом 1941 г. заплатила миллионами убитых, раненных и пленных солдат и офицеров. Жесткая централизация системы военного руководства Ирака, большинство объектов которой было сосредоточено в Багдаде, а закрытые правительственные линии связи проложены через автомобильные и железнодорожные мосты, оказала Хуссейну медвежью услугу. Союзники, используя авиационные бомбы с лазерным наведением и крылатые ракеты со спутниковой системой навигации, к началу наземного наступления разрушили практически все коммуникации иракских войск.

Попытки отдавать приказы из Багдада с помощью посыльных мотоциклистов только усугубили положение иракской армии, которая за время воздушных налетов уже была фактически деморализована. Миллионы листовок, сброшенных на головы иракских солдат призывали их держаться подальше от своих танков, бронетранспортеров и орудий, как объектов поражения высокоточного оружия, эффективность которого уже не вызывала сомнения. Что же так напугало генералов в Пентагоне, пребывавших в зените своей славы?

Сегодня в США созданы самые оснащенные вооруженные силы в мире: около 3 млн. гражданских специалистов и военнослужащих, включая резервистов имеют в своем распоряжении вооружение, технику и имущество на общую сумму в 1000 млрд. $, на содержание которых выделяется свыше 300 млрд. $ в год. Для ведения такого большого разбросанного по всему миру "хозяйства", доставляющего немало организационных, технических и чисто человеческих хлопот, американцы содержат внушительный арсенал информационных ресурсов: свыше 2 млн. компьютеров, 100000 локальных сетей и 10000 информационных систем.

Для вооруженных сил США, где на одного военнослужащего приходится один персональный или бортовой компьютер, а количество информационных систем, в которых эти компьютеры интегрированы для решения боевых задач в ходе военных действий, исчисляется десятками тысяч, сценарий 1991 года означал бы полный крах. Обрушенные на головы иракцев 60 тыс. тонн боеприпасов, из которых 10% составили высокоточное оружие, включая 323 крылатые ракеты, не достигли бы своих целей, если бы противник вывел из строя хотя бы одну из этих систем, например, навигации или тылового обеспечения.

Если вспомнить, что во время американских бомбежек Югославии устаревшая информация ЦРУ привела к "точному" попаданию крылатой ракеты... в здание посольства КНР — нейтральной страны, обладающей ядерным оружием, то нетрудно представить возможные последствия замены всего нескольких байт в "ядерном чемоданчике" президента США.

Но это еще не все. В отличие от Ирака, где для управления войсками использовалось 60% гражданских линий связи, в США этот показатель достиг 95%, включая использование глобальной сети Интернет и спутников связи Интелсат. Известны случаи, когда недавние выпускники военных академий, корректировали огонь своих артиллерийских батарей, используя электронные карты Пентагона за тысячи миль от своих боевых позиций в пустыне. Для непрерывного, практически в течение каждого часа, уточнения данных воздушной и космической разведки, необходимо было задействовать сотни спутниковых каналов одновременно. Большинство пилотов после вылета на задание перенацеливались уже в ходе полета, поражая цели с ходу, что значительно снизило потери союзной авиации.

Общедоступность и высокая оперативность обновления информации о боевой обстановке, в сочетании с ее наглядностью и высокой достоверностью "единой цифровой картины поля боя", превращают информацию не только в мощное оружие, но и уязвимую цель для противника.

Планирование операций, разведка, навигация, связь, материально-техническое снабжение, инженерное оборудование, транспортировка грузов, медицинское обеспечение, финансирование и расквартирование войск, заказ вооружений и электронная торговля прочно обосновались в паутине компьютерных сетей, в которые то и дело заглядывают через Интернет любознатель-

ные хакеры, где им есть что посмотреть в секретных файлах американских военных.

Военный флот выходит в Интернет. Америка — крупнейшая военно-морская держава. Сегодня в боевом строю военного флота США находятся свыше 300 военных кораблей, 4000 самолетов и вертолетов. Общая численность ВМС и морской пехоты составляет примерно 900 тысяч военнослужащих и гражданского персонала, из которых 88 тыс (10%) находятся за пределами США. Годовой бюджет ВМС — это 90 млрд. $ или 30% всего военного бюджета Пентагона. Ежегодно военно-морское ведомство тратит около 1.6 млрд. $ на автоматизацию и информационные технологии.

Американские ВМС в тандеме с морской пехотой начинают грандиозную и беспрецедентную по своей стоимости и масштабу охвата программу создания глобальной информационной сети NMCI (Navy Marine Corps Intranet). По данным военно-морского ведомства США стоимость программы оценивается в 7 млрд. $. В ходе ее выполнения в период 2001-2008 гг. предполагается объединить около 100 разрозненных в настоящее время ведомственных информационных сетей и ликвидировать порядка 200 телекоммуникационных шлюзов, задействованных в системе оперативного планирования и боевого использования кораблей, авиации и подразделений морской пехоты США. Общее количество компьютеров (серверов, настольных рабочих станций, портативных и карманных компьютеров) может достичь 360 тысяч ед., при этом они будут разбросаны по всему земному шару на 300 военных базах (Аляска, Исландия, Пуэрто-Рико, Гуам, Окинава, Гавайи, Куба и др.), включая континентальную часть США.

Сама идея создания подобной сети появилась как результат обобщения опыта совместного боевого использования разнородных (авиационных, морских и сухопутных) смешанных группировок вооруженных сил в так называемых конфликтах низкой интенсивности (Косово, Сомали и др.). В итоге военно-морские силы в рамках концепции Пентагона по реформированию и автоматизации ВС "общее видение 2020" выдвинули свою инициативу — "информационные технологии 21-го века", одной из важнейших составляющих которой и является данная программа.

Создаваемая сеть объединит все потоки информации, передаваемые в направлении "корабль-берег" и "берег-корабль", за счет использования универсального мультимедийного интерфейса и технологии Интранет. Пользователи сети будут иметь выход на все важнейшие правительственные, военные и коммерческие информационные системы, что позволит им оперативно решать задачи не только в интересах планирования и проведения военных операций, но и в личных целях (заказ авиабилетов, оплата счетов, медицинская диагностика и др.).

Пехотинец 21-го века. По оценкам Пентагона в текущем десятилетии 50% всех боевых действий будут вестись в условиях городских застроек (населенных пунктах), а к 2025 г. этот показатель может достигнуть 75-80%.

Мировой опыт вооруженных конфликтов низкой интенсивности (Ливан, Гренада, Сомали, Косово, Чечня) показывает, что ведение боя в населенных пунктах характеризуется высокими потерями, быстрой сменой обстановки, неустойчивостью связи, плохой видимостью, низкой эффективностью применения тяжелых вооружений (авиации, танков), затрудненным тыловым снабжением и медицинским обеспечением войск. Вот почему сухопутные войска активно разворачивают работы по созданию собственного армейского тактического Интранета по программе WIN-T, в ходе которой американские солдаты получат не только новую экипировку со шлемом-дисплеем, компьютером, радиостанцией, датчиком космической системы навигации и автоматической винтовкой, позволяющей с помощью специального прицела-перископа стрелять из-за укрытия ночью и в тумане, но и уникальным доступом к информационным системам планирования и ведения боевых действий.

Подсистема личной связи CRS, сопряженная с портативным компьютером и индивидуальным датчиком глобальной навигационной системы GPS, должна максимально облегчить солдату в бою все его действия, связанные с ориентированием на местности, оценкой обстановки, ведением переговоров в звене отделение-взвод, передачей и получением видео изображений, опознаванием целей, ведением химической разведки, обнаружением мин и другими задачами. Вычислительная система состоит из двух компьютеров: ранцевого портативного и универсальной шины USB, которая обеспечивает обмен данными между основными подсистемами. Для удобства пользования портативный компьютер оснащен индивидуально настраиваемой системой распознавания голоса. Связь солдата с его отделением в бою поддерживается с помощью двух радиостанций: индивидуальной типа Motorola (1755-1850 МГц) и общей, сопрягаемой с системой одноканальной цифровой связи "Sincgars" (30 – 88 МГц), что позволяет командиру в случае необходимости ставить ему задачи и получать от него донесения. Подсистема связи обеспечивает одновременный разговор трех абонентов и передачу данных (64 Кбит) в режиме засекречивания на расстоянии до 5 км. Для связи вне зоны видимости используется ретрансляция с автоматическим поиском ближайших радиостанций других пехотинцев или воздушных ретрансляторов (самолетов или вертолетов). Общий вес двух радиостанций составляет 656 г., а габариты — 14 см х 8 см х 2,5 см.

В качестве вычислительной платформы используется IBM совместимый портативный мультимедийный компьютер с упрощенной операционной системой Windows-2000, процессором Пентиум-75 Мгц, оперативной памятью 32 Мбайт, жестким диском объемом 340 Мбайт и сменной флэшпамятью 85 Мбайт, сетевой картой Ethernet. Для подключения периферийного оборудования в компьютере имеются шины PCI и ISA, с двумя разъемами RS-232. Общий вес портативного компьютера составляет около 1200 г, а габариты без внешних соединителей — 4 см х 18 см х 27 см. Диапазон рабочих температур от -15 до 49 град Цельсия. Предусмотрено несколько типовых вариан-

тов установки вычислительной системы в зависимости от выполняемых боевых задач: для командира, солдата, инженера, разведчика, корректировщика огня. В командирском варианте предусмотрено подключения клавиатуры с трекболом и дисплеем VGA.

Общая стоимость программы "пехотинец" оценивается в 2 млрд. $, полномасштабная реализация которой предполагает поставку в войска в течение 2001-2010 гг. 34 тысяч комплектов. По оценкам Счетной палаты Конгресса США стоимость одного комплекта снаряжения оказалось завышенной от первоначальной более чем в 2,5 раза.

В январе — феврале 2001 г. в шт. Калифорния были проведены первые полевые учения в ротном звене с использованием нового комплекта снаряжения пехотинца. В ходе учений за счет использования нового снаряжения условные потери противника возросли с 55% до 100%, а собственные потери снизились с 28% до 17%. По отзывам солдат снаряжение их вполне устраивает. Все электронные компоненты безотказно работали даже в воде. Каждый боец точно знал расположение своих товарищей и всегда мог выйти на связь.

Электронная торговля. Еще в мае 1998 г. в рамках широкомасштабной и долгосрочной инициативы по реформированию вооруженных сил Пентагон открыл новую программу по созданию единой системы электронной торговли EMALL, в рамках которой предполагается упорядочить процесс закупки вооружений и предметов материально-технического снабжения войск через Интернет. Для реализации этой программы в Агентстве материально-технического снабжения (тыла) ВС США DLA было создано управление электронной коммерции JECPO. Система электронной торговли создается по принципу Интернет-портала, который связывает сайты видов вооруженных сил и коммерческих фирм-производителей в интересах создания эффективной и безопасной торговли на основе рыночного механизма через прямую продажу-покупку, что обеспечит пользователям свободный доступ к предметам военных поставок посредством электронных каталогов и электронных биржевых операций.

За счет использования системы электронной торговли Пентагон предполагает сократить от 30 до 40 промежуточных этапов закупки вооружений, сведя их фактически до 10 он-лайн операций.

Например, в классической бумажной системе при закупке на сумму в 500$ только на административные расходы тратится от 150$ до 200$, в то время как в электронной системе эти расходы составят всего 2$. При этом сама процедура бумажного оформления заказа может занимать от 1 до 3 месяцев бюрократических согласований в различных инстанциях.

К основным преимуществам создаваемой системы электронной торговли EMALL можно отнести следующие: объединение системы электронной торговли с системами тылового снабжения и финансирования войск, все предметы снабжения будут постоянно находиться под контролем по мере их

заказа, оплаты и поставок, устранение дублирования в заказах, централизованная регистрация покупателей и производителей, поиск по всем правительственным источникам информации, коммерческим каталогам и электронным торговым биржам, автоматический сбор статистики и формирование отчетов, эффективный маркетинг и реклама, стандартизация заказов вооружений, налаживание контактов и взаимопонимания между видами вооруженных сил в интересах снижения стоимости программ перевооружения и их реализации.

Однако, у электронной торговли есть и свои минусы, о которых следует помнить. Это, прежде всего, безопасность транзакций при проведении покупок и продаж через Интернет, где хакеры чувствуют себя как рыба в воде.

В 1999 г. было отмечено всего около 22 тысяч попыток проникновения и снятия информации с систем Пентагона; за первые 11 месяцев 2000 г. количество таких попыток возросло до 26 500. В целях обеспечения безопасности доступа к информационным ресурсам и секретным объектам Пентагон проводит полномасштабную замену личных номеров военного и гражданского персонала с использованием технологии пластиковых электронных карт — "smart-cards". Каждая такая карта стоимостью 6$ будет иметь микросхему с аппаратной реализацией криптографического алгоритма, индивидуальный магнитный и штрих код владельца. В период с 2000 по 2005 гг. ВМС как головная организация этой программы получит 145 млн. $ для закупки электронных карт, компьютеров, программного обеспечения и электронных замков для установки на 800 военных объектах по всему миру.

В 2000 г. в системе электронной торговли Пентагона было зафиксировано свыше 5 миллионов наименований товаров и услуг, которые были задействованы по операциям купли-продажи в общей сложности на сумму 80 млн. $. По предварительным оценкам в 2001 г. каталоги баз данных электронной торговли МО США должны расширится до 12 млн. наименований, а объем торговых сделок по военным программам должен достигнуть 143 млн. $. В настоящее время в этой системе зарегистрировано около 175 тыс. фирм-производителей, заинтересованных в работе по военным контрактам. Для сравнения: в 2000 г. в общей сложности было сделано покупок через Интернет на сумму 33 млрд. $, в которых участвовали 20000 чел. При этом общие расходы из федерального бюджета на информационные технологии за этот же период составили 37.6 млрд. $.

Заказ вооружений. По оценкам Пентагона к 2005 г. свыше 120 тысяч (50%) госслужащих, занятых в программах приобретения (заказов, закупок и поставок) военной техники и имущества для вооруженных сил США, достигнут пенсионного возраста и могут быть уволены. Под угрозу будут поставлены сотни долгосрочных военных программ, от которых зависит не только национальная безопасность, но и экономика, а также благосостояние самой богатой нации в мире. Эта тревожная тенденция вынуж-

дает американцев активно внедрять информационные технологии в военно-промышленном бизнесе.

Параллельно с развитием системы электронной торговли Пентагон активно внедряет передовые информационные технологии непосредственно в систему приобретения вооружений по военным контрактам, которых сегодня насчитывается до 332500 на общую сумму 852 млрд. $. За пять лет было оборудовано свыше 20000 удаленных терминалов автоматизированной системы военных контрактов SPS. К 2003 г. система должна охватить 43000 пользователей в 1100 районах земного шара. По данным за 2000 г. Пентагон осуществил закупку на 32 млрд. $ товаров и услуг с помощью системы SPS. Когда система будет полностью развернута и интегрирована в сеть Интернет, американские военные рассчитывают ежегодно экономить до 1.4 млрд. $ на закупках по военным контрактам.

Космическая фотосъемка. Не секрет, что основные функции современных космических аппаратов (спутников) связаны в основном с навигацией, метеорологией, связью и разведкой. Последняя является в настоящее время одним из приоритетных направлений в обеспечении информационного превосходства практически во всех сферах жизнедеятельности современного общества: военной, политической, научно-технической и экономической.

В ближайшие несколько лет предполагается перейти полностью на систему электронной торговли продуктами космической видовой разведки через Интернет.

Министерство обороны и разведывательное сообщество США в настоящее время начинают осуществлять широкомасштабные долгосрочные программы, направленные на полную замену их спутниковых арсеналов в ближайшие десять лет, стоимость которых оценивается в 60 млрд. долларов. Одновременно ставиться задача по увеличению окупаемости капиталовложений за счет реализации коммерческих проектов в этой области. После долгих колебаний Конгресс США санкционировал возможность коммерческого доступа к изображениям, получаемым со спутников IKONOS с разрешением в 1 м. Такая точность фотосъемки использовалась американскими военными во время войны в Персидском заливе для определения позиций иракских баллистических ракет. По некоторым оценкам Национальное агентство космической фотосъемки и картографии (NIMA) планирует получить от продажи своей продукции до 1 млрд. $ в год.

Для этого планируется создать распределенную базу данных с послойным отображением участков земной поверхности в цифровом формате, доступ к которой будет осуществляться на платной основе избирательно: каждый пользователь сможет увидеть только то, что ему можно будет увидеть без ущерба национальной безопасности США и их союзникам. Информация будет накапливаться не только за счет национальных, но и иностранных орбитальных ресурсов, что позволит иметь наиболее точное и полное представле-

ние об интересующих покупателя участках в различных спектрах (видимом, инфракрасном, ультрафиолетовом), ракурсах (черно-белом, цветном, двухмерном, трехмерном) и масштабах обзора (по углу, высоте и ширине полосы съемки). Эта же информация наряду с данными агентурной и радиоэлектронной разведки будет постоянно отслеживаться в базах данных разведывательного сообщества в интересах национальной безопасности.

Разведка. В США разведкой занимаются 14 спецслужб, входящих в так называемое разведывательное сообщество: ЦРУ, Разведуправление Министерства обороны (РУМО), Агентство национальной безопасности (АНБ), органы космической разведки Пентагона, разведуправления видов вооруженных сил, бюро разведки и исследований госдепартамента, занимающиеся разведывательной деятельностью подразделения министерств юстиции и финансов, а также Федеральное бюро расследований (ФБР).

Всего на нужды разведывательного сообщества из бюджета выделяется около 28 — 30 млрд. $. Большая часть этих средств идет на технические системы сбора, обработки и распределения информации.

Информационное превосходство при проведении информационных операций стало основной задачей разведки в 21-ом веке. Из опубликованных в открытой печати материалов следует, что многие вопросы реорганизации разведки касаются в основном информационных технологий.

Анализ боевых действий в Персидском заливе, в ходе которых широко использовалось высокоточное оружие, поставил на повестку дня вопрос об эффективности использования информации, добываемой разведывательным сообществом. Были проведены комплексные исследования по проблеме реформирования и реорганизации разведки, в которых участвовали свыше шести правительственных и частных научно-исследовательских организаций.

Разведывательное сообщество стало сильно зависеть от технических систем, используемых для сбора, обработки и распределения информации. В свою очередь новые технологии оказывают влияние на работу персонала и качество самих систем.

В силу того, что каждое шпионское ведомство США по соображениям безопасности создавало свои собственные системы сбора и распределения информации (АНБ — КРИТИКОМ, РУМО — ДЖЕЙ-ВИКС, ДОДИИС, АМХС) с течением времени назрела острая необходимость в их объединении, и уже в начале 90-х годов была поставлена задача создать в ИНТЕРНЕТ невидимый для большинства пользователей специальный закрытый или как его еще называют секретный ИНТЕРНЕТ.

Хотя в этой секретной сети, получившей название ИНТЕЛИНК, также используется традиционный протокол TCP/IP, непосредственный доступ к секретной информации осуществляется через специальный протокол HTTPS при наличии специального броузера с набором криптографических алгоритмов, поставляемого только для зарегистрированных пользователей ИНТЕЛИНК.

Сеть ИНТЕЛИНК имеет четыре уровня доступа к разведывательной информации по степени секретности: первый уровень представляет особо важная информация для принятия политических решений, которую готовит и распределяет только ЦРУ через специальную сеть ПОЛИСИНЕТ для президента и Совета безопасности; второй – информация, имеющая гриф совершенно секретно, к которой имеют доступ около 50 тыс. пользователей, среди которых в свое время была и Моника Левински, когда она работала в Пентагоне; третий – секретная информация, связанная с планированием военных операций, к которой имеют доступ 265 тыс. пользователей сети СИПРНЕТ; четвертый — несекретная информация из открытых источников (печать, ИНТЕРНЕТ, телевидение, радио), которая составляет свыше 95% всей добываемой разведкой информации.

Как считают американские специалисты пользователи разведывательной информации ожидают, что они смогут получать информацию непосредственно по своему запросу, предпочитая иметь прямые контакты с источником информации.

В случае, если такой контакт невозможен, пользователь должен знать как его информация собирается для того, чтобы оценить ее достоверность. В настоящее время уже ведутся работы по созданию соответствующей "виртуальной аналитической среды" в рамках разведывательного сообщества, которая соединит в одно целое тех, кто собирает, распределяет, анализирует и потребляет информацию в целях повышения производительности и отдачи каждого аналитика. В рамках "виртуального аналитического сообщества", все участники которого будут интегрированы в единую информационную систему предполагается повысить требования к стандартизации информационных технологий, включая создание единого органа закупок и механизма регулирования бюджета для модернизации систем в течение всего жизненного цикла.

Борьба со шпионажем и терроризмом. Арест высокопоставленного офицера ФБР Роберта Хансена, обвиняемого в сотрудничестве с КГБ/СВР с 1986 г., вызвал самый настоящий шок в разведывательном сообществе США, где еще не успели забыть скандального разоблачения офицера ЦРУ Олдрича Эймса в 1994 г. В деле Хансена, пожалуй впервые в мировой практике шпионажа, можно говорить о прецеденте: "крота вычислил" компьютер.

Роберта Хансена без всякого преувеличения можно назвать шпионом 21-го века, который не просто использовал современные информационные технологии, но делал это виртуозно, как настоящий профессионал.

Из представленного ФБР обвинительного заключения следует, что в своей шпионской деятельности Хансен, практически избегал прямых контактов с сотрудниками российской разведки, используя для оперативной связи флэш-карты, дискеты, карманный органайзер Palm Pilot, беспроводный удаленный доступ в Интернет и криптографические программы. Как установили следователи, Хансен постоянно набирал в графе поиска специальной базы данных ФБР не только собственное имя, но и такие ключевые слова, как

"Россия", "КГБ", "шпионский тайник", а также свои кодовые обозначения для связи, чтобы установить, не попал ли он под подозрение. Все запросы, которые периодически делал Хансен компьютер неумолимо записывал в специальный журнал, по которому его в конце концов и "расшифровали" сотрудники ФБР.

В настоящее время ФБР совместно с АНБ ведут работы по созданию системы контроля за электронной почтой в Интернет. На программу технического перевооружения АНБ "GroundBreaker" Конгресс выделил свыше 5 млрд.долл. и еще около 1 млрд. долл. дополнительно на переоснащение многоцелевой атомной подводной лодки класса "Sea wolf" для прослушивания подводных кабелей связи с помощью специальной аппаратуры. Названная в честь президента США Джими Картера новая субмарина SSN-23 должна была быть спущена на воду в декабре этого года, но по настоянию АНБ было принято решение провести ее переоборудование, а спуск лодки отложить до июня 2004 г. По сведениям, просочившимся в печать, после ввода в строй новой субмарины АНБ рассчитывает прослушивать не только обычные электрические кабели связи, что оно делало и раньше, но и ... волоконно-оптические! Как это удастся сделать американцам - пока не ясно: для бесконтактного перехвата экранированного светового луча еще не придуман способ. Между тем, подводная лодка-шпион будет нести на своем борту специальный контейнер-камеру, из которой может быть осуществлен беспрепятственный доступ к любым подводным объектам.

Рожденный в кабинетах американского военного ведомства таинственный призрак-невидимка информационной войны за десять лет своего виртуального существования уже успел породить не мало проблем для тех, кто его создал. Сегодня без всякого преувеличения можно утверждать, что главная из них - защита информации. По оценкам ЦРУ не менее 100 стран располагают в той или иной мере возможностями ведения информационной войны, при этом доля компьютерных вирусов в Интернете, разрушающих информацию и ее носители выросла до 30%. Однако завеса глубокой тайны и строгой секретности, первоначально опущенные Пентагоном над собственными планами информационных операций создали явную диспропорцию между желаемым и достигнутым. Для страны, все сферы жизнедеятельности которой столь прочно связаны с информационными технологиями, грань между государственными и коммерческими, военными и гражданскими системами более чем условна.

Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд. $, из которых около 20 млрд. $ (более 50%) составляют расходы военного ведомства. И это без учета десятков млрд. $., затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей. Сегодня Пентагон это не только один из крупнейших владельцев, арендаторов и пользователей информационных и телекоммуникационных ресурсов, ведущих заказчиков программного обеспече-

ния, компьютерного оборудования и средств цифровой связи, но и, по сути дела, законодатель государственной политики и промышленных стандартов в области информационной безопасности. Только в 2000 г. на защиту национальных информационных ресурсов в США было выделено 1,5 млрд. $, в то время как Пентагон истратил на защиту военных информационных систем 1,1 млрд. $.

В определенной степени это сказывается и на самих понятиях, связанных с защитой информации, которые постепенно трансформируясь из чисто военных терминов приобретают характер общегосударственных и промышленных стандартов. Производители оборудования и разработчики программных продуктов, заинтересованные в крупных государственных и военных заказах, начинают прислушиваться к тому, что говорят в коридорах Пентагона об информационной безопасности.

Осознав на собственном опыте бессмысленность защиты информационных ресурсов без участия всех заинтересованных сторон, каковыми в США являются фактически не только все государственные структуры, промышленность, частный капитал, но и рядовые граждане, военное ведомство в буквальном смысле пошло в народ, активно пропагандируя свое видение общенациональной проблемы №1. Одним из примеров такого новаторского подхода является программа DIAP (Defense Information Assurance Program), в рамках которой с участием таких ведущих фирм как Lucent Technologies, IBM, Microsoft, Intel, Cisco, Entrust, HP, Sun, GTE, Bay Networks, Axent, Network Associates, Motorola закладывается фундамент информационной безопасности не только военной инфраструктуры, но и всего американского общества в целом на ближайшие 10 лет.

Когда в декабре 1996 г. в одной из секретных директив американские военные ввели в обращение новый термин - "гарантия информации" (IA - information assurance), на это мало кто обратил внимание, учитывая первоначально ограниченный круг лиц допущенных к документу. Однако лингвистическая причуда Пентагона имела далеко идущие последствия, с которыми сегодня вынуждено считаться все большее число пользователей и производителей высоких технологий.

В соответствии с секретной директивой Пентагона S-3600.1 гарантия информации определяется как "информационная операция или операции, связанные с защитой информации и информационных систем за счет обеспечения их готовности (доступности), целостности, аутентичности, конфиденциальности и непротиворечивости. Данные операции включают в себя восстановление информационных систем за счет объединения возможностей защиты, обнаружения и реагирования. При этом информация не будет раскрыта лицам, процессам или устройствам, не имеющим к ней прав доступа, будет обеспечена полная достоверность факта передачи, наличия самого сообщения и его отправителя, а также проверка прав на получение отдельных категорий информации, данные остаются в исходном виде и не могут быть случай-

но или преднамеренно изменены или уничтожены, будет обеспечен своевременный и надежный (по требованию) доступ к данным и информационным службам установленных пользователей, а отправитель данных получит уведомление факта доставки, также как получатель – подтверждение личности отправителя, и таким образом никто не сможет отрицать своего участия в обработке данных."

Тем самым классическое понятие информационной безопасности (INFOSEC - information security) как состояние информационных ресурсов было расширено и дополнено гарантированием их надлежащего использования даже в том случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри. Иными словами в политике информационной безопасности четко обозначился сдвиг в сторону активных организационно-технических мероприятий защиты информационных ресурсов. Похоже, что американцы взяли за основу пропаганды знаний в области информационной безопасности советскую систему гражданской обороны 60-х, 70-х годов, когда население учили не только тому как надевать индивидуальные средства защиты и укрываться в бомбоубежищах, но и как вести радиационный, химический и бактериологический контроль и восстанавливать объекты народного хозяйства после применения оружия массового поражения.

Заметим, что это не единственное нововведение Пентагона в лексиконе информационных технологий, которое стало достоянием общественности несмотря на гриф секретности первоисточника. К числу таковых можно отнести следующие: "*информационное противоборство*", "*информационное превосходство*", "информационные операции (общие и специальные)", "информационная среда", "атака на компьютерные сети", "вторжение в информационные системы" и др. С некоторых пор американское военное ведомство считает полезным публиковать отдельные несекретные фрагменты из своих засекреченных официальных нормативных документов (директив, инструкций, меморандумов, уставов и наставлений), повышая информированность общества о потенциальных угрозах национальной безопасности. Военные терпеливо и настойчиво приучают все слои населения к своей терминологии, постепенно стирая грань между государством и обществом, обороной и производством, разведкой и предпринимательством, учебой и досугом.

Как результат, американское общество начинает пожинать плоды информационной революции в виде единых универсальных стандартов, применимых как в гражданском, так и в военном секторе.

В качестве примера можно привести стандарт электронной подписи (PKI - public key infrastructure) X.509, разработанный Агентством национальной безопасности для применения не только в военных, но и гражданских информационных сетях и системах. В соответствии с принятым стандартом в США к 2003 г. будут выдаваться пять классов сертификата PKI, гарантирующих информационную безопасность на основе криптографических алгоритмов с открытым ключом в зависимости от степени секретности информации.

Каждый сертификат будет включать такие сведения как разновидность класса, порядковый номер, криптографический алгоритм инстанции выдавшей сертификат, наименование инстанции, срок действия (до 10 лет), ключ (до 1024 бит), цифровую подпись и др. К концу 2001 г. Пентагон должен полностью перевести свою электронную почту на стандарт PKI.

Профессиональная подготовка персонала в соответствии с новыми требованиями в области информационной безопасности является ключевым направлением реализации программы DIAP, в рамках которой на учебный процесс выделяется в общей сложности около 80 млн. $ на период до 2005 г. При этом предполагается открыть специализированные курсы дистанционного обучения (свыше 20) в так называемом "виртуальном университете информационной мом "виртуальном университете информационной безопасности" на базе сайтов в Интернете, в которых будут обучаться основам "стратегии глубокой эшелонированной защиты информационных ресурсов" администраторы (2 недели) и специалисты (3-5 дней) практически из всех федеральных ведомств, включая ЦРУ, ФБР, НАСА, Минфина, Минюста, Минэнерго и др. Ожидается, что за 5 лет будет подготовлено в общей сложности не менее 100 тыс. дипломированных специалистов в области информационной безопасности, готовых к любым неожиданностям в киберпространстве.

В каждом штате на период чрезвычайных условий (землетрясений, ураганов, наводнений, катастроф, террористических актов) создаются так называемые резервные центры обработки информации, в которых периодически собирается, накапливается и обновляется наиболее важная информация, необходимая для организации управления всех жизненно важных служб (полиции, скорой помощи, пожарной охраны и др.) в случае выхода из строя основных центров обработки информации и телекоммуникационных систем. Как правило такие центры оснащаются автономными источниками энергоснабжения (дизель - генераторами), способными поддерживать нормальный режим функционирования резервных информационных центров в течение нескольких суток до восстановления стационарной системы энергоснабжения. В повседневных условиях работу таких центров обеспечивает ограниченный по численности технический персонал, имеющий все необходимые навыки для организации работы центра в чрезвычайных условиях.

Краткий обзор только некоторых наиболее важных и дорогостоящих программ развития информационных технологий в США на примере Пентагона показывает, что проблема информационной безопасности отдельно взятого ведомства по своему масштабу уже давно является общенациональной и для своего решения требует пересмотра устоявшихся подходов, принятия единых стандартов как в промышленности, так и в бизнесе, создания национальной системы подготовки специалистов соответствующего профиля, широкого информирования населения об угрозах и мерах по их предотвращению.

ЛЕЙТІ М.
БОРОТЬБА НА ІНФОРМАЦІЙНОМУ ФРОНТІ *

"Годі вам, будьмо реалістами... Такі вигадки, які я щойно почув, треба приберегти для коміксів; це не робота серйозного журналіста". (Речник НАТО на прес-конференції Альянсу в Скоп'є, 4 вересня 2001 року.)

Така відверта критика засобів масової інформації, як правило, не є найкращою тактикою, якщо треба довести свою думку. Вже те, що була необхідність вдаватися до такої "шокової тактики" свідчить про те, наскільки нелегкою була робота прес-групи НАТО минулого року, в дуже важкий час для Югославської Республіки Македонія. Після шести місяців постійної загрози громадянської війни головні політичні партії підписали досить суперечливу політичну угоду, а в цей час НАТО надіслало до країни тисячі військових, що мали зібрати зброю, яку здавали етнічні албанці – бойовики Національної визвольної армії. Проте саме в цей історичний для країни період прихильники жорсткої політики скористалися своїм впливом на засоби масової інформації для відвертої критики НАТО і мирної угоди.

З точки зору НАТО, ця хвиля дезінформації в пресі могла серйозно зашкодити нашій діяльності, успіх якої залежав від взаєморозуміння і співпраці, а не від застосування сили. Велике значення мало бажання албанських вояків здати зброю добровільно, що, в свою чергу, мало безпосередній вплив на готовність македонських парламентарів проголосувати за радикальні політичні зміни, які багатьом були не до вподоби. Нас запросив до країни уряд, який перебував в стані глибокого розколу; не можна було недооцінювати вплив засобів масової інформації на громадян Македонії, що були налякані і ставились до НАТО з підозрою, а тому були готові повірити в найгірше. За таких обставин ЗМІ відігравали ключову роль і на тому етапі ми програвали боротьбу за громадську підтримку.

Минув рік. Національну визвольну армію розформували, а Рамкова угода, підписана в серпні 2001 року, набула сили закону. Значно послабилась політична напруга, успішно пройшли вільні й демократичні вибори. Попереду ще багато роботи, але колишня Югославська Республіка Македонія здійснила історичний поворот. Звичайно, передусім це успіх громадян країни. Але і міжнародна спільнота доклала багато зусиль для досягнення цього успіху. Міжнародне втручання в ситуацію у колишній Югославській Республіці Македонія вже тепер сприймають як класичний (і рідкісний) приклад успішної превентивної дипломатії. Важливою складовою цього успіху була зміна позиції засобів масової інформації.

Інформаційна кампанія. Інформаційна кампанія НАТО в колишній Югославській Республіці Македонія дуже відрізнялась від аналогічної діяльності Альянсу в Боснії і Герцеговині, а також в Косові. Операції НАТО в тих

* http://www.nato.int/docu/review/2002/issue4/ukrainian/art3_pr.html

країнах були більш зосереджені на військових аспектах і демонстрували силу міжнародного співтовариства. В колишній Югославській Республіці Македонія* місія НАТО мала переважно політичний характер, а уряд в Скоп'є зберігав свій суверенітет. НАТО було і залишається партнером уряду і може діяти тільки за його згодою.

Спочатку інформаційна кампанія НАТО була досить обмеженою. Йшлося тільки про зв'язки з громадськістю в межах тилової підтримки сил КФОР в колишній Югославській Республіці Македонія, яку забезпечувала так звана група "КФОР-Тил", що не мала місії в самій країні, а контролювала постачання ресурсів для КФОР з Греції до Косова. Коли НАТО почало розширювати межі своєї діяльності в колишній Югославській Республіці Македонія, інформаційна кампанія ставала дедалі більше переобтяженою новими завданнями.

Загроза громадянської війни в колишній Югославській Республіці Македонія виникла навесні 2001 року, коли було сформовано Національну визвольну армію. Але серйозні проблеми в роботі із засобами масової інформації виникли влітку, коли НАТО призначило Пітера Файта на посаду офіційного представника Альянсу для контактів з Алі Ахметі, лідером Національної визвольної армії. На той момент, завдяки посередництву Європейського Союзу, було створено правлячу коаліцію, яка об'єднувала представників головних політичних партій етнічних албанців і македонців. Це був єдиний можливий шлях досягнення угоди щодо болісних політичних змін, необхідних для запобігання громадянській війні, проте, розкол і протистояння продовжували впливати на роботу уряду.

Головним джерелом незлагоди була розбіжність позицій прихильників жорсткої політики і "поміркованих" щодо долі бійців Національної визвольної армії. "Жорсткі" політики вимагали військового вирішення цієї проблеми і вважали солдатів Національної визвольної армії терористами, з якими необхідно воювати. "Помірковані", в свою чергу, обстоювали ідею політичної домовленості, яка мала задовольнити законні політичні прагнення етнічних албанців і усунути можливі причини майбутніх конфліктів. Західні військові вважали, що державні сили безпеки неспроможні виграти партизанську війну, а дипломати були впевнені, що політична угода це єдина альтернатива громадянській війні та розколу країни.

За таких обставин пан Файт, який вів переговори з Алі Ахметі щодо припинення вогню і розформування Національної визвольної армії, опинився в епіцентрі "інформаційного шторму". Його контакти з лідером Національної визвольної армії здійснювались на прохання уряду, але це не захистило НАТО від критичних нападів, оскільки в уряді не було єдності. Прихильники жорсткої політики відверто критикували НАТО, але навіть македонські міністри, які визнавали необхідність переговорів з Ахметі, не наважувались відкрито захищати таку непопулярну позицію.

Ситуація погіршилась ще більше в червні, коли НАТО організувало виведення бійців Національної визвольної армії з міста Арачиново, поблизу

Скоп'є. Військові зусилля, спрямовані на виведення формувань Національної визвольної армії, виявились неефективними, політично-військова ситуація швидко погіршувалась, і уряд Скоп'є звернувся до НАТО і пана Файта з проханням переконати командування визвольної армії в необхідності залишити район дислокації. Це було важке і ризиковане завдання, проте, його успішно виконали, хоча і ціною урядової кризи та масованої атаки засобів масової інформації. Громадськість переконували, що НАТО не запобігло кризі, а рятувало Національну визвольну армію від поразки. Водночас прихильники жорсткої політики в уряді критикували дії, на які вони ж самі й погодились.

Це поставило НАТО перед дилемою, яку йому довелось вирішувати в наступні місяці: як реагувати на критику з боку тих членів уряду, що самі просили присутності НАТО і визнавали необхідність саме таких кроків, які робив Альянс. Тим часом засоби масової інформації, які підтримували жорстку політику, роздмухували полум'я етнічної ненависті та військової істерії. У звіті Європейської комісії зазначалося: "Позиція засобів масової інформації під час кризи 2001 року серйозно вплинула на погіршення політичної ситуації".

Впродовж літніх місяців НАТО постійно звинувачували в активній військовій співпраці з Національною визвольною армією; в тому, зокрема, що Альянс надавав їй гелікоптери для перевезення вантажів і транспортування особового складу. Офіційний речник уряду неодноразово звинувачував представників НАТО в тому, що вони "зловживають довірою" уряду і "брутально поводяться", що було частиною загальної кампанії на користь початку військових дій. Треба віддати належне мужності тих представників уряду Скоп'є, які домоглися підписання Рамкової угоди у серпні, попри величезний тиск, що чинився на них. Незважаючи на невдоволення громадськості та агресивну критику засобів масової інформації, вони прийняли багато важливих рішень.

До вересня 2001 року, коли були розгорнуті спеціальні сили „Харвест", НАТО не прагнуло особливої уваги засобів масової інформації. Успіх дипломатичних зусиль в кризовій ситуації, і, зокрема, успіх контактів групи пана Файта з Алі Ахметі, багато в чому залежав від обачливості й розсудливості. Оскільки Альянс сам не намагався широко висвітлювати свою діяльність, він став жертвою потоку дезінформації в пресі. Зусилля НАТО не отримали підтримки і розуміння з боку етнічних македонців. Прибуття до країни кількох тисяч військових НАТО викликало бурхливу реакцію преси і спричинило сплеск ворожих почуттів до Альянсу, що вплинуло і на роботу групи із зв'язків з громадськістю, попри всі зусилля військового речника майора Беррі Джонсона, який бездоганно виконував свої обов'язки.

Ситуація остаточно погіршилась на початку вересня, коли візит Генерального секретаря збігся з достроковим завершенням першого етапу збирання зброї Національної визвольної армії. Це мало б стати свідченням успішності наших зусиль, але вийшло навпаки. Хоча ми зібрали багато справного, придатного для активного використання озброєння, так сталося, що

найближче до представників засобів масової інформації ми склали саме застарілу зброю, вкриту брудом. Натовп журналістів оточив Генерального секретаря біля місця, де було зібрано вилучену зброю, прес-конференція перетворилась на хаос. Місцева преса писала, що весь процес був фальсифікований, а міжнародні засоби масової інформації передрікали нам повну поразку.

Перелом у ситуації. Перелом у ситуації настав, коли ми повністю реорганізували і збільшили групу працівників, що відповідали за зв'язки з громадськістю, а також прийняли рішення щодо активної протидії дезінформації і брехні в ЗМІ. Дуже важливим кроком стало призначення цивільного речника (мене) для відповідей на політичні питання і критичні напади, що було неможливим для військового речника.

Для представників засобів масової інформації це стало справжнім шоком. Журналісти, що ставились до нас з відвертою ворожістю, тлумачили нашу неагресивну і "неголосну" позицію як прояв слабкості і невпевненості, а на наші ввічливі заперечення проти обурливих звинувачень просто не звертали уваги. Наші попередні відмови від обговорення важливих політичних питань також сприймалися журналістами як свідчення слабкості, оскільки вони не розуміли, що офіцери західних країн мають певні обмеження щодо публічних виступів. І раптом цим журналістам було кинуто виклик: оскільки щоденні прес-конференції НАТО стали головною інформаційною подією, їм не залишалось нічого іншого, як публікувати те, що ми говорили. Щовечора прес-конференції НАТО отримували велику частку ефірного часу на телебаченні.

Було багато необ'єктивних коментарів, але ідеї і діяльність НАТО оприлюднювались так, як ніколи раніше, що дало можливість розвіяти найбезглуздіші вигадки. Це була важка робота, але, коли впливові прихильники жорсткої політики почали вимагати припинення щоденних прес-конференцій НАТО, ми зрозуміли, що наші зусилля дали бажаний результат. Нам вдалося уникнути відвертої конфронтації з "жорсткими" міністрами, проте ми постійно нагадували в своїх виступах, що саме вони запросили нас до країни і, отже, несуть відповідальність за це рішення.

Щоденні прес-конференції були тільки частиною нашої стратегії спілкування із засобами масової інформації. Додаткові ресурси, ретельніше планування і активне реагування на запити преси відразу дали наочний результат: журналісти почали частіше відвідувати місця діяльності сил спеціального призначення „Харвест". Наприклад, наступна демонстрація зібраної зброї дала можливість продемонструвати наші успіхи; ми надали для зйомок гелікоптер; зібрану зброю відчистили від бруду, аби всі могли побачити: це ефективні бойові знаряддя, а не якийсь непотріб.

Стратегія роботи із засобами масової інформації стала темою обговорень на ранкових нарадах командувача як складова нашої загальної політики; радники з питань преси та інформації робили вагомий внесок у нашу спільну роботу. Відразу після головних нарад навіть проводили додаткові обговорен-

ня, присвячені конкретним питанням інформаційної політики, в яких активну участь брали військові командувачі й політичні представники, що допомагали у спрямуванні нашої стратегії на виконання головного завдання сил НАТО в країні.

У деяких випадках наша стратегія передбачала свідоме поєднання громадського тиску і дипломатії з публічними заявами. Наприклад, ми змогли переконати прихильників жорсткої політики в Македонії вивести озброєні формування, які свідомо провокували збройні сутички, саме завдяки тому, що наші переговори з політиками доповнювались оприлюдненням відповідної інформації в пресі. У цьому випадку, як і в усіх інших, ми керувались головним правилом: ніколи не подавати неправдивої інформації.

Тепер нашим спеціалістам з питань контактів з представниками ЗМІ стало легше отримувати необхідну інформацію з приводу певної події. Швидке отримання інформації є принципово важливим для успішної роботи з пресою, але коли йдеться про військову операцію, з цим часто виникають проблеми, пов'язані з особливостями системи командного підпорядкування. Однак щира підтримка наших зусиль з боку командування дала нам можливість отримувати потрібну інформацію вчасно. Наша спроможність надавати своєчасну і точну інформацію дала НАТО важливі переваги в боротьбі за адекватне висвітлення її діяльності в засобах масової інформації.

Міжнародна співпраця. Співпраця з іншими міжнародними організаціями також була для нас важливою. Особливе значення мав зв'язок між НАТО і ЄС; Генеральний секретар НАТО лорд Робертсон і Верховний представник ЄС Хав'єр Солана не тільки виконували роль головних посередників у врегулюванні політичного конфлікту, але і забезпечували засоби масової інформації "важкою артилерією", оскільки озброювали журналістів інформацією з питань міжнародної політики, яка мала особливу вагу завдяки загальновизнаному авторитету цих політиків. До того ж їх візити, як правило, відбувалися у вирішальні моменти. Але і ті політичні діячі, що працювали в Скоп'є, також почали дедалі більше координувати між собою роботу із засобами масової інформації. НАТО завжди докладало зусиль, аби представники інших міжнародних організацій також брали участь в щоденних прес-конференціях Альянсу. Коли ми виступали разом, це завжди посилювало ефективність наших зусиль; в той час як брак координації завдавав подвійної шкоди, оскільки прибічники жорсткої політики завжди шукали слабкі місця в нашій роботі.

Проте найважливішою складовою успіху була дуже проста умова (яку, однак, було нелегко виконати): ми мали заслужити довіру. Головною причиною проблем, які ми мали минулого літа, була відсутність довіри до нас з боку етнічних македонців. Ми знали, що говоримо правду, але треба було переконати в цьому журналістів, які ставились до нас вкрай скептично. Спростування брехні та дезінформації мало підкріплюватись доказами надійності нашої інформації; ми мали переконати громадськість у тому, що наша стратегія

є, щонайменше, чесною і відвертою, навіть, якщо дехто і не погоджується з нею.

Успіх операції, виконаної силами спецпризначення „Харвест", допоміг нам забезпечити довіру, якої ми потребували. Ми заявили, що зберемо зброю і ми зібрали її. Ми сказали, що Національну визвольну армію буде розформовано і це було зроблено. Ми стверджували, що озброєні формування етнічних македонців провокують збройні сутички і коли їх вивели з району дій, такі випадки припинилися. Навіть після закінчення прес-конференцій ми спілкувалися особисто з журналістами, обговорювали з ними складні питання за чашкою кави, обмінювались думками. Головною проблемою журналістів було те, що вони не знали, чому вірити — довгі місяці вони отримували спотворену і суперечливу інформацію. Але попри це і незважаючи на упередженість організацій, на які вони працювали, багато з них щиро бажали розібратися в реальній ситуації. Деякі з журналістів мали достатньо інформації, проте їм не дозволяли оприлюднювати ті факти, які були їм відомі. За таких обставин особисті стосунки мали особливе значення: ми вчилися довіряти один одному, навіть ставали друзями.

Стратегія роботи із засобами масової інформації, яку застосовувало НАТО, допомогла нам налагодити зв'язки з журналістами, а широке і вчасне висвітлення успіхів Альянсу в країні допомогло розбудувати довіру до НАТО. Сили спеціального призначення „Харвест" завершили свою операцію в жовтні 2001 року і на той час більшість провідних журналістів вже довіряла НАТО і вважала нашу інформацію надійною. Протягом наступного року це неодноразово підтвердилось роботою македонських ЗМІ, які в процесі нормалізації політичної ситуації розділились на "поміркованих" і "жорстких".

Минулого року засоби масової інформації колишньої Югославської Республіки Македонія сприймалися як одна з тих сил, що підштовхували країну до громадянської війни. Під час успішних виборів у вересні, хоча і траплялися випадки подання упередженої і неправдивої інформації, більшість засобів масової інформації працювали конструктивно. Попри окремі випадки залякування і погроз, багато мужніх журналістів і видань намагалися своїми публікаціями вирішувати проблеми, а не створювати їх. Слід зазначити, що дехто з журналістів, яким погрожували, звернулися по допомогу до НАТО і ми відкрито виступили на їх захист. Ми справді пройшли довгий шлях.

Леонов О.В. КІБЕРВІЙНИ ПОСТІНДУСТРІАЛЬНОГО СВІТУ *

Інформаційні технології завжди викликали підвищенну увагу з боку військових. Варто лише згадати, що сам Інтернет своєю появою зобов'язаний аналітикам Пентагона. У розпал Холодної війни дуже гостро постало питання

* Манипулятивные стратегии в политике, экономике, бизнесе и методы противодействия. Материаллы конференции. – К., 2001

про забезпечення зв'язку та координації дій збройних сил США та їх союзників у випадку глобального застосування ядерної зброї. Відомо, що в цих умовах звичайні системи комунікації стають катастрофічно неефективними. Саме тоді американські військові експерти запропонували вирішити цю проблему за допомогою інформаційних технологій, що тільки почали розвиватися. Саме так виникла ідея створення глобальної комп'ютерної мережі. А вже сьогодні, на думку заступника глави космічних сил армії США генерал-лейтенанта Едварда Андерсона, існує три основних форми сучасної війни: застосування балістичних ракет, контроль над космічним простором і ведення інформаційної війни, значною частиною якої є війна в кіберпросторі. В першу чергу мова йде про здійснення широкомасштабних руйнівних атак на військову і цивільну інформаційну й комунікаційну інфраструктуру ворога. Більше того, в епоху Інформаційної війни системна кібернетика прагне захопити владу не тільки над економічним і політичним життям націй, але, насамперед, над геополітикою усього світу. Тому огляд ворожої інформації виявляється набагато більш значимим, ніж звичайне глушіння його передач, оскільки він знищує всяку телекомунікацію між ворожою державою і його власним народом, чи йде мова про діючу пропаганду чи звичайну інертну інформацію, що необхідна для повсякденного життя нації...

Технологія кібервійни. Напередодні атаки на Ірак Джордж Буш підписав таємну директиву, що доручає урядові розробити концепцію нанесення кіберударів по комп'ютерних мережах ворогів, передає "The Washington Post". Концепція кібернетичної війни буде подібна стратегічній ядерній доктрині, у якій описані умови застосування ядерної зброї після Другої світової війни. У кібернетичній військовій доктрині будуть описані правила проникнення в іноземні комп'ютерні системи і їхнє знищення. Посилаючись на чільних представників уряду, "The Washington Post" пише, що досі США не проводили масштабних стратегічних кібератак (хоча це твердженя можна піддати сумніву, про що мова буде йти нижче). Проте, Пентагон активно займається створенням кібернетичної зброї. Військові сподіваються, що коли-небудь електроніка прийде на зміну бомбам, що дозволить наносити більш швидкі і меньш криваві удари по ворожих об'єктах, не жертвуючи літаками й солдатами. Солдати сидітимуть за комп'ютерами і безшумно проникатимуть в іноземні комп'ютерні мережі, відключатимуть радари, позбавлятимуть ворогів електрики і телефонного зв'язку. Адміністрація дуже зацікавлена в створенні такого виду зброї - багато фахівців вважають, що вона зможе різко змінити характер воєнних дій. Але рух у цьому напрямку йде повільними темпами, тому що у військових немає президентської директиви про те, за яких обставин можна застосовувати такі атаки, хто буде їх санкціонувати і проводити, по яких цілях можна буде завдавати удари.

Отже, що ж являє собою кібернетична війна? Вона заснована на діях, що спрямовані на знищення, блокування чи модифікацію інформації, інфор-

маційних і телекомунікаційних систем. Найважливішою ознакою кібервійни можна назвати те, що ворог може до визначеного часу може навіть не здогадуватися про те, що війна проти нього вже в повному розпалі. Кібервійна дає можливість ведення воєнних дій малими силами, які, крім цього, можуть бути децентралізовані і ретельно замасковані, істотно ускладнюючи тим самим їхнє виявлення і знищення. Кібервійна — це війна без кордонів. Атаки в ній можуть вестися як з території нападаючого, так і з інших (зовсім не суміжних) територій.

Інструментарій ведення кібернетичної війни можна умовно розподілити на інформаційний, програмно-математичний, фізичний, радіоелектронний та організаційно-правовий.

Інформаційний:

- Порушення адресності та своєчасності інформаційного обміну, протизаконний збір і використання інформації.
- *Несанкціонований доступ до інформаційних ресурсів.*
- Маніпулювання інформацією (дезінформація, приховування чи викривлення інформації).
- Незаконне копіювання даних в інформаційних системах.
- Порушення технології обробки інформації.

Програмно-математичний:

- Застосування комп'ютерних вірусів.
- Застосування спеціальних програмних та апаратних приладів.
- Знищення чи модіфікація даних в автоматизованих інформаційних системах.

Фізичний:

- Знищення чи руйнування засобів обробки інформації чи зв'язку.
- Знищення, руйнування чи розкрадання машиних чи інших оригінальних носіїв інформації.
- Розкрадання програмних чи апаратних ключів та засобів криптографічного захисту інформації.
- Вплив на персонал.
- Постачання "зараджених" компонентів автоматизованих інформаційних систем.

Радіоелектронний:

- Перехоплення інформації в технічних каналах її можливого витоку.
- Упровадження електронних приладів перехоплення інформації у технічні засоби та приміщення.
- Перехоплення, дешифрування та нав'язування неправдивої інформації у мережах передачи даних та лініях зв'язку.
- Вплив на парольно-ключеві системи.
- Радіоелектронне придушування ліній зв'язку та систем керування.

Організаційно-правовий:

- Невиконання вимог законодавства.

- Неправомірне обмеження доступу до інформації, що має важливе для громадян та суспільства значення.

Треба зазначити, що США заздалегідь розпочали підготовку до військових дій у кіберпросторі. Цей процес знайшов своє відображення в Єдиній доктрині інформаційних операцій, яка була затверджена головою об'єднаного комітету начальників штабів (ОКНШ) Генрі Шелтоном та опублікована ще у 1998 році. У цьому документі сформульовані основні принципи кібернетичної війни.

Заступник директора інформаційних операцій в ОКНШ бригадний генерал ВПС Брюс Райт зазначив, що складовою інформаційних операцій є застосування психологічних операцій, обману, перешкод, зламу та захисту'ютерних мереж. Також треба згадати про забезпечення режиму секретності та радіоелектронну боротьбу. Брюс Райт також відзначив, що для адекватної відповіді на інформаційний вибух необхідно сінхронізувати зміни у військовому середовищі із технічним прогресом, а також із постійною загрозою від ймовірного супротивника, яка збільшується.

Для досягнення успіху в інформаційному протиборстві були передбачені й оперативні заходи:

- У спеціально створеній об'єднаній оперативній групі по захисту комп'ютерних мереж (Joint Task Force on Computer Network Defence) ведеться цілодобовий моніторинг стану найбільш важливих об'єктів інформаційного ресурсу.
- На ключових комунікативних вузлах цих об'єктів встановлені системи виявлення спроб несанкціонованого доступу.
- Сформовані додаткові групи реагування на надзвичайні ситуації у інформаційно-обчислювальних системах для екстреного відновлення їх працездатності.
- Розроблені та узгоджені із всіма зацікавленими відомствами плани локалізації наслідків програмних атак ймовірного супротивника.
- Налагоджена оперативна взаємодія в цій галузі між Міністерством оборони та правоохоронними відомствами країни.

Великі надії покладаються на програму GNIE (Global Networked Information Enterprise), реалізація якої істотно підвищить захищеність відомчих інформаційно-обчислювальних мереж, покращить їх технологічні характеристики та забезпечить зручне взаємне поєднання.

Загроза «Цифрового ПЕРЛ-ХАРБОРУ». Саме такими словами представник Національної Ради Безпеки США Ричард Кларк ще у 2000 році охарактеризував стан безпеки у кіберпросторі у своему виступі на конференції по безпеці, що була організована компанією Microsoft. Високопосадовець намагався застерегти Сполучені Штати про прийдешні потрясіння: «Багато націй створюють військово-інформаційні підрозділи, головною метою яких є знищення комп'ютерних мереж. Війна в кіберпросторі здається неможливою річчю, але насправді вона може стати цілком реальною».

Справедливості заради варто зазначити, що попередження Ричарда Кларка не для усіх стали несподіванкою. Він лише привселюдно озвучив побоювання американських військових, котрі раніше за інших усвідомили небезпеки інформаційної епохи і зробили все можливе для їхньої нейтралізації. Саме Пентагону у своїй діяльності доводилося і доводиться щодня зіштовхуватися з загрозами та викликами, джерелом яких є кіберпростір. За повідомленням прес-служби Збройних Сил (ЗС) США, американська армія постійно піддається агресії з Мережі. Міністерство оборони щодня фіксує від 80 до 100 електронних нападів на свої комп'ютерні системи. До останнього часу самими серйозними вважалися початі в січні – лютому 1999 року спроби проникнення на об'єкти інформаційних ресурсів ЗС США. Американські військові дотепер відмовляються повідомляти про винуватця цієї серії програмних атак. Відомо тільки те, що в ході розслідування були встановлені ознаки єдиного методичного підходу до планування і проведення спеціального програмно-математичного впливу. Фактично це виключає версію про злочинну діяльність хакера-одинака і свідчить про роботу спеціально організованої групи.

Особливе занепокоєння у контролюючих органів викликала думка військових експертів про наявність у військовому відомстві одного чи декількох агентів, завчасно завербованих стороною, що нападала. Фахівці вважають малоймовірним, що без відповідної допомоги зсередини зовнішні оператори змогли б перебороти захист на критично важливих інформаційних вузлах військового відомства США. Але впровадження в Пентагон агента, що має прямий доступ до систем безпеки цієї організації, являє собою дуже складну, коштовну і тривалу операцію, яку в змозі здійснити розвідки лише дуже нешироко кола країн. Таким чином, підтверджується теорія зовнішнього ворога, що має відповідні матеріальні та кадрові ресурси.

По гарячих слідах ще наприкінці лютого 1999 року заступник міністра оборони Джон Хамре, виступаючи на слуханнях у профільному комітеті палати представників, зробив сенсаційну заяву про те, що американська армія «вже зараз» утягнута в справжню інформаційну війну. Правда, варто сказати, що дуже часто хвиля кібератак на інформаційні ресурси Сполучених Штатів дивним чином збігається з активними діями того ж Пентагона, зайвий раз підтверджуючи міждержавний рівень баталій в Інтернеті. Першим подібним зіткненням можна вважати ряд програмних атак на США, що одержали кодову назву «Солар санрайз». Особливий інтерес і занепокоєння військово-політичного керівництва країни вони викликали тому, що саме в той період ЗС закінчували підготовку до нанесення ударів по території Іраку.

Також варто згадати про електронне протистояння країн НАТО з югославськими хакерами під час воєнної операції Альянсу на Балканах. В остаточному підсумку воно звелося до декількох вдалих спроб активістів із СРЮ знизити швидкість проходження інформації в комп'ютерних мережах. Подібний ефект досягався за рахунок відправлення на адресу одержувачів

електронної пошти міністерства оборони США величезної кількості повідомлень чи цілого вала викликів відповідних сайтів. Американські військові особливо виділяють випадок, коли один белградський рекордсмен посилав більш 2000 повідомлень у день. Однак особливої шкоди дії сербських хакеров принести не могли і виглядали небезпечними тільки завдяки особливій увазі численних засобів масової інформації. Водночас вищі чини ЗС США підтвердили, що в 2000 р. під час військової кампанії в Косово Пентагон використовув хакерські методи для проникнення у комп'ютерні системи державних структур Югославії.

Однак навіть певний політичний затишок у міжнародних відносинах не може гарантувати Вашингтонові відсутність неприємностей у цифровому світі. За повідомленням сайту Wired News, глава розвідувальної служби міністерства оборони США адмірал Том Вильсон на публічному засіданні комітету зі справ розвідки в Сенаті заявив, що Фидель Кастро готує кібератаку проти комп'ютерних систем Пентагона. Після публічного засідання комітет залишився на закрите обговорення секретних матеріалів. Сенатори поцікавилися, чи є реальні шанси, що кубинський лідер боротиметься з Америкою саме в такий спосіб. Вильсон відповів, що для Гавани цей шлях, безсумнівно, є найбільш багатообіцяючим, тому що у військовому конфлікті кубинська армія не зможе протистояти ЗС США. На думку адмірала, у Куби є гарний апарат розвідки, сильна служба безпеки і чудовий потенціал для застосування так званої асиметричної тактики ведення бойових дій. Ця тактика використовується у боротьбі із супротивником, який багаторазово перевершує силу іншої сторони. Її основою є саме терористичні акти, як у реальному світі, так і в Мережі.

Всі ці випадки є тільки частиною величезної картини неоголошеної війни, що бушує на просторах Інтернету. За заявою офіційних осіб на засіданні підкомітету конгресу США по розслідуванню надзвичайних подій, віртуальні злочинці є серйозною загрозою для національної безпеки.

Кіберфронти інформаційної ери. Можливо, вищенаведені факти можуть створити ілюзію, що всі бої в кіберпросторі обов'язково відбуваються за участі США. Це не так. Дуже часто кибербої у різних куточках планети дивним чином збігається з різного роду конфліктами, що зайвий раз підтверджує міждержавний рівень баталій в Інтернеті.

Дійсно, зростання політичної напруги у світі обов'язково позначається на характері діяльності хакерів. Так, дослідницький підрозділ компанії mi2g встановив, що у Великій Британії число атак на урядові сайти збільшилось на 378%. В абсолютному вираженні цифри трохи менш вражаючи - у 2001 р. було зафіксовано 43 атаки проти 9 у 2000, однак ріст усе рівно можна назвати значним. Що стосується атак на комерційні домени в зоні co.uk, то їх чисельність зросла із 137 до 385 чи на 187%. Як вважають у mi2g, за збільшення кількості атак відповідальність несуть антиглобалисти, супротивники НАТО, а також і звичайні злочинці.

Як і раніше, найбільше число атак - близько 30% - припадає на зону .com. Тут необхідно зазначити, що й кількість доменів у цій зоні значно більша, ніж в інших. Кількість атак на сервери в американській урядовій зоні .gov зросло на 37%, а у військовій зоні .mil - на 128%.

Серед національних доменів по числу атак лідирували китайський .cn і тайваньский .tw. На їхню частку припадає 9% від загальносвітової кількості хакерських атак, що можна пояснити "протистоянням двох Китаїв" - КНР та Тайваню. Найбільший ріст числа хакерських атак у відносному вираженні був відзначений в Ізраїлі (на 220%), Індії (205%) і Пакистану (300%). Аналитики mi2g пояснюють цей ріст насамперед ростом політичної і військової напруженості у відповідних регіонах.

Яскравим прикладом цієї інформаццїї служить ситуація на Близькому Сході й в Азії. Так, сучасний конфлікт між палестинцями й ізраїльтянами супроводжується потужним протиборством у Мережі. Наприклад, конфлікт між палестинцями й ізраїльтянами супроводжується могутнім протиборством у четвертій сфері, характер якого свідчить про розгортання між двома народами повномасштабної інформаційної війни. Особливої уваги заслуговують сутички в Інтернеті. Арабські фахівці ведуть їх по двох напрямках: виводять з ладу інформаційні сторінки супротивника по сценарію югославських хакерів, у результаті чого сайти ізраїльських державних установ виявляються перевантаженими чи заблокованими (особливо дісталося веб-сторінкам канцелярії прем'єр-міністра Ізраїлю і міністерства фінансів) чи використовують комп'ютерний вихід на мобільні телефони ізраїльтян, на які масово відправляються текстові повідомлення загрозливого характеру.

Подібний розвиток подій зовсім не влаштовує Тель-Авів, який у відповідь на арабські інформаційні атаки терміново вишукує контрзаходи для переламу ходу війни в кіберпросторі на свою користь. Для цього в Інтернеті блокуються веб-сторінки палестинських рухів і організацій, знищуються їх сайти, спотворюється інформація на них, поширюються погрози по опублікованим у Мережі номерам телефонів палестинських лідерів. Нарешті, в Ізраїлі в терміновому порядку було створено загальнонаціональне управління по захисту інформації. За повідомленням агентства Reuters, лідери ісламського угруповування "Хізболла" стверджують, що їх сайт неодноразово припиняв роботу із-за дій ізраїльських хакерів.

Сайт "Хізболли" вміщує докладну інформацію й новини про діяльність угрупування. При нормальній роботі його відвідують 300 тис. користувачів. Але після повідомлень про загибель палестинських солдат на Західному березі річки Іордан і у секторі Газа кількість відвідувачів сайту зросло, за словами веб-мастера, до 9 млн. (!).

Для уявлення більш повної картини великого протистояння у Мережі слід згадати про кібербої між Індією та Пакистаном. Останніми жертвами цієї війни у Мережі стали сайти готелів, медичних компаній, астрологічних прогнозів і путівника по магазинах Делі. Так звані "пакистанські кібервоїни" за-

повнили індійські сайти символами смерті, написами "Аллах Акбар!" та вітаннями на адресу Усами бен Ладена. Від цієї інтернет-агресії постраждали 197 сайтів, а всього за 2001 рік їх було атаковано 333. Насправді ж число атак хакерів може бути набагато більшим, тому що жертви воліють зберігати мовчання. У середньому повідомляється тільки про один випадок вторгнення з десяти. Особливо намагаються уникати розголосу корпоративні сайти, що бояться негативної реклами.

Для оперативного реагування на подібні атаки було створено проект "зламана Індія", що відслідковує вторгнення на сторінки індійської тематики. Аналітики проекту зауважують, що, хоча стовідсоткову безпеку не може гарантувати ніхто, більшість індійських компаній зневажають інвестиціями в захист мереж: усього 0,8 % інтернет-витрат приходиться на електронну безпеку, тоді як в усьому світі цей показник складає 5,4 %. До того ж, застосування індійських законів про злочини у кіберпросторі обмежується групами усередині країни, тоді як у більшості випадків атаки відбуваються з-за меж державного кордону.

У інформаційному протистоянні між Делі та Ісламабадом дійшло навіть до блокування Індією доступу до Інтернету на території Кашміру, з метою зашкодити комунікації мусульман, що складають більшість населення провінції, із Пакістаном.

Перша мережева війна. Ще більш масштабно і фундаментально в силу низки суспільно-політичних особливостей до питання ведення кібервійн підходять у Китаї. Пекін, що жорстко контролює національний сегмент Інтернету і дає величезні тюремні терміни необережним юзерам за поширення «підривної інформації» у Всесвітній мережі, своїх хакерів не тільки не торкає, але і всіляко їм потурає. У відповідь на державну турботу вони, об'єднані у союз Honker Union of China (honker — гібрид англійського hacker і китайського hong — червоний, завдяки чому «Союз хакеров Китаю» відомий ще і як «Альянс Червоного Гостя»), удосконалюють свою апаратну і програмну базу і підвищують професійну майстерність для майбутнього підкорення світового віртуального простору. Яскравим прикладом сили, організованості й ефективності китайської кіберармії служить цифровий бліцкриг проти Країни сонця, що сходить.

Ще наприкінці лютого 1999 року голова бюджетної комісії нижньої палати японського парламенту Хосэй Норота заявив, що в роки експансії першої половини XX століття Японія не була агресором, а допомагала народам Азії звільнитися від західних колонізаторів. Цей пасаж був сприйнятий Пекіном украй болісно. МЗС КНР направив Токіо ноту протесту, а китайські хакери оголосили Японії війну в Мережі. Практично миттєво були зламані більш 70 серверів найбільших промислових компаній і університетів. На сайтах цих організацій була розміщена інформація про злочини імператорської «визвольної» армії. У відповідь японцям залишилося тільки визнати свою повну і беззастережну поразку, констатуючи появу в Мережі могутньої і безжалісної сили.

Однак, все ж таки треба визнати, що цифрові сутички зазвичай мають локальний характер, не набуваючи розмірів повномасштабних бойових дій. В основному всі зафіксовані інтернет-атаки будувалися за схемою подія — удар — відступ.

Так продовжувалося до квітня 2001 року, коли в кіберпросторі зіткнулися китайські й американські професіонали. Саме це зіткнення поступове набуло рис першої мережевої війни — війни високих технологій нового тисячоріччя.

Нагадаємо, що стрімке погіршення американо-китайських відносин почалося відразу після 1 квітня 2001 року, коли літак ВПС США, що робив розвідувальний політ неподалік від кордонів Піднебесної, був примусово посаджений на один із аеродромів, а його екіпаж заарештований. Китайський пілот, що повернувся на базу, повідомив, що винищувачі КНР прямували за американським розвідником приблизно на відстані 400 метрів, як раптом той зненацька пішов убік і зачепив пропелером лівого крила один з китайських літаків, що потім впав у воду. Льотчик Вонг Вей загинув.

Наступного ж після інциденту дня китайські хакери з вже згадуваного Honker Union of China (HUC) атакували ряд американських сайтів. До 13 квітня нападу було піддано 9 урядових веб-сторінок. Якийсь час події розвивалися за вже звичною схемою — хакери з Піднебесної «ламали» американські сайти і залишали на них послання протесту. Однак цього разу хонкеры не побажали діяти за загальноприйнятою схемою, і на початку травня інформаційне протистояння Китаю і США придбало характер дійсної війни.

За повідомленням авторитетного китайського порталу www.chinabyte.com, першотравневий наступ було сплановано в ході онлайнової конференції учасників HUC, що відбулась 30 квітня. У результаті масованої атаки на інформаційні ресурси США нападу піддалися біля тисячі (!) американських серверів. До успіхів китайських товаришів можна віднести шестигодинне блокування сайта Білого дому і часткове позбавлення доступу до вебсторінки ЦРУ. Серед постраждалих називалися сайти міністерства енергетики, Геологорозвідувального товариства і штаб-квартири командуючого наземними службами Атлантичного флоту Америки. Однак найбільш сильний удар чомусь був нанесений по сайтам Міністерства праці і Міністерства охорони здоров'я і соціального захисту населення.

Слід зазначити, що китайські хакери діяли з особливою жорстокістю. За міжнародною хакерською конвенцією метою атаки є або «підвішування» сервера, або розміщення на ньому своєї інформації. Знищення інформації, що зберігається на дисках супротивника, неприпустимо. Але активісти HUC у кожному випадку зламу намагалися саме безповоротно знищити весь вміст американських серверів.

Американці теж не сиділи, склавши руки. Ще 4 квітня вони почали операцію ChinaKiller, назва якої говорить сама за себе. На відміну від своїх китайських колег, хакери із США зламували сайты вибірково й акуратно. Це ви-

глядало не так ефектно, зате було дуже ефективно. По визнанню головного друкованого органа Китайської комуністичної партії газети «Женьминь жибао», у результаті американського контрудару сотні сайтов урядових відомств, навчальних закладів, а також комерційних структур КНР на тривалий термін були виведені з ладу. У Пекіні дійшли до невтішного висновку, що «системи комп'ютерної безпеки КНР поступаються аналогічним системам США». За оцінками американської компанії iDefence, у ході кібервійни була серйозно порушена робота 350 китайських сайтів, тоді як у доменій зоні Сполучених Штатів по-справжньому постраждало лише 37.

На думку тієї ж «Женьминь жибао», акції «червоних хакерів» дозволили лише «відвести душу», але не призвели до реального множення міці Китаю і не підірвали могутності США. У результаті дії HUC звелися до різновиду «терористичної діяльності в Мережі через підрив її режиму роботи і безпеки». Після такої оцінки з боку керівництва країни Honker Union of China, який потерпів першу у своїй історії поразку, оголосив про перемир'я «у кібервійні зі США» і саморозпустився. Перша мережева війна юридично була закінчена. Однак на цілий ряд питань відповідь так і не була отримана. Чому поодинокі атаки на інформаційні системи Китаю й Америки, більш схожі на хуліганські витівки окремих політично заклопотаних громадян, раптом набули злагодженності, організованості й масштабності? Звідкіля у простих хакерів з'явилась надсучасна техніка, дивним чином немов спеціально створена для вирішення бойових завдань у Мережі? А чим можна пояснити найвищий рівень координації та планування атак, більш характерний для Генерального штабу, ніж для неформального об'єднання навіть дуже гарних програмістів? Ці і десятки інших питань підштовхують до досить незвичайного висновку — на другому етапі американо-китайського протистояння в кіберпросторі за справу узялися військові відомства обох країн. Можна сказати, що світ був свідком тестування нового Інтернету — бойового.

Загроза із мережі. Уроки першої мережевої війни для керівництва США не пройшли даром. Практично одразу ж по гарячих слідах були скореговані численні військові програми в області інформаційних і комунікаційних технологій. За повідомленням служби новин CNN, Пентагону було доручено готуватися до кібератак проти потенційних супротивників, які вже зараз посилено готуються до війн у Мережі.

Генерал-лейтенант Эдвард Андерсон, заступник глави космічних сил армії США, повідомив журналістам, що його підрозділ отримав наказ розробити стратегію ведення кібервійни. Таким чином, планувати послідовність дій армії США після наказу Верховного командування про початок війни в Мережі буде Агентство супутникових телекомунікацій.

Стратегія, яку планується назвати OPLAN 3600, має на увазі «безпрецедентне об'єднання комерційних і державних структур країни». До розробки нових стратегій приєдналося і ФБР, тому що, на думку представників цього відомства, ситуація вимагає рішучого об'єднання зусиль для протидії можли-

вим атакам через Інтернет. Генерал-лейтенант підкреслив, що розробка цього проекту може завершитися створенням нових типів зброї для масованих кібератак і поширення комп'ютерних вірусів. За словами Андерсона, командування ЗС США отримало інформацію про те, що китайська армія вже розвиває такі види зброї.

Урядовці США недарма настільки схвильовані цією проблемою. Яскравою ілюстрацією руйнівних можливостей кібервійни є події на півдні США під час американо-китайської війни в Інтернеті. Тоді фахівці американської енергетичної компанії California Independent Systems Operator (Cal-ISO), що забезпечує енергопостачання штату Каліфорнія, досить випадково викрили, що їхні комп'ютерні системи осаджувалися невідомими хакерами протягом щонайменше 17 днів.

Відповідно до припущень, атака почалася ще 25 квітня і залишалася непоміченою до 11 травня. Анонімні джерела в компанії заявили агентству Reuters, що невідомі хакери практично взяли у свої руки контроль над системою розподілу електроенергії, у той час як офіційні представники Cal-ISO стверджували, що серйозної загрози не було, тому що хакери не зуміли перебороти захист.

7 і 8 травня близько 400 тисяч каліфорнійських споживачів були відключені від енергопостачання в результаті неполадок у системі. У компанії заперечують зв'язок цих подій і вищезгадуваного хакерского нападу.

Однак до рук журналістів газети "The Times" потрапили фрагменти внутрішнього звіту Cal-ISO, в якому вказується на катастрофічний характер можливих збитків. Крім того, технічні фахівці встановили, що хакери під час атаки скористалися мережею китайського провайдера China Telecom, що розміщений в провінції Гуаньдун.

За заявою офіційних осіб на засіданні підкомітету конгресу США з розслідування надзвичайних подій, віртуальні злочинці все частіше захоплюють контроль над обчислювальними системами державних установ США, створюючи тим самим серйозну загрозу національної безпеці. Залишається тільки здогадуватися, що буде, якщо їм вдасться пробитися крізь захист ядерних об'єктів, систем керування супутниками і ще багатьох інших техногенно небезпечних об'єктів.

Тільки за 2000 рік 155 комп'ютерних систем 32-х федеральних установ, постраждали від захоплення хакерами адміністраторського контролю над комп'ютерними системами. У 1998 році таких випадків було 64, а в 1999 - 110. У зв'язку з цим, державні чиновники можуть тільки здогадуватися про те, яка інформація могла потрапити в руки злочинців.

Офіційні особи вважають, що уряд може зіштовхнутися із серйозними проблемами, якщо рівень безпеки обчислювальних систем не буде кардинально підвищений. За словами представників ФБР, багато спроб зламу державних комп'ютерних систем відбувалися із-за кордону.

Саме вирішенню питання забезпечення належного рівня безпеки кібер-

простору приділяють левову частку своїх зусиль держави-лідери інформаційного світу. Так, комісія з боротьби з тероризмом Палати представників США має намір внести пропозицію про створення спеціального закритого кібер-суду для нагляду за розслідуванням комп'ютерних злочинів. Пропозиція комісії особливо знаково виглядає у світлі прийнятого "Закона про об'єднання і зміцнення Америки" (Uniting and Strengthening America Act, чи просто USA Act), що, зокрема, наділяє поліцію спеціальними повноваженнями в справі прослуховування Інтернету й обшуку електронних носіїв. У визначених ситуаціях поліція може встановлювати пристрої, що підслухують, і без схвалення суду. Деякі члени Сенату пропонують також набагато посилити покарання за хакерство, дорівнявши комп'ютерні злочини до тероризму. Деякі законопроекти, що передбачають, зокрема, довічне покарання за комп'ютерні злочини, уже знаходяться на розгляді Конгресу.

А 10 жовтня радник президента США з безпеки кіберпростру Ричард Кларк запропонував комп'ютерним компаніям допомогти в створенні спеціальної урядової мережі GOVNET, незалежної від Інтернету. Автономне існування такої мережі, на думку Кларка, охоронить її від вторгнення хакеров і терористів, повідомляє Associated Press. Урядові заклади могли б використовувати GOVNET для телефонних переговорів, передачі даних і відеоконференцій. Після 11 вересня саме відеоконференції стали основним способом спілкування президентських радників.

Варто згадати про існування в західних країнах спеціальних служб для боротьби з комп'ютерним тероризмом у структурі правоохоронних органів, що говорить про дуже серйозні наміри держави стосовно Мережі. Сподіватися на те, що держава пустить на самоплив процеси у середовищі, що стає стрижнем нового світу, щонайменше наївно.

Треба зазначити, що й військові США активно працюють над підвищенням рівню своєї професійної підготовки. За повідомленням сайту Government Computer News, курсанти Військової академії США у Вест-Пойнті, Військово-морської академії в Анаполісі, Військово-повітряної академії у Колорадо-Спрінгс і Академії берегової охорони у Нью-Лондоні взяли участь у навчаннях по протидії кібератакам, де їх супротивниками були офіцери Агентства національної безпеки США.

У ході навчань команда кожної академії отримала у розпорядження мережу, що складалася із трьох підмереж та була обладнана брандмауером. Завдання курсантів полягало у забезпеченні безпеки та працездатності всіх без винятку мережевих служб. В цьому ім намагалися зашкодити представники так званої "червоної команди" АНБ. За кожне проникнення у мережу з академічних команд знімалися очки, а за усунення дір – нараховувались.

За підсумками вже других (!) навчань Cyber Defense Exercise, приз директора департаменту АНБ по захисту інформації знову вибороли курсанти Вест-Пойнту. Як представники АНБ, так й викладачі військових вузів відмітили, що рівень підготовки курсантів значно виріс у порівнянні із минулими на-

вчаннями.

Всі вищезгадані кроки досить добре вписуються у нову загальнонаціональну стратегію США в галузі кібербезпеки. Її можна описати словами конгресмена Ламара Смита: "у новому столітті ми повинні впритул зайнятися підготовкою нового покоління солдатів, основною зброєю яких стане не автомат, а переносний комп'ютер".

Таким чином, варто визнати, що світ входить у століття руйнівних війн в кіберпросторі зовсім непідготовленим. На сьогоднішній день цілком відсутня система міжнародної безпеки в Мережі, немає міжнародних угод чи структур, здатних якщо не зупинити мілітаризацію Інтернету, то хоча б не допустити масштабного використання військової сили у Всесвітній мережі. Можна констатувати, що Україна залишається абсолютно беззахисною перед можливою агресією із віртуального простору. А у контексті бурхливого розвитку інформаційних технологій у нашій країні (варто згадати лише наміри запровадження технології електронного урядування) ситуація може швидко набути рис, що становлять загрозу національній безпеці. Яскравим прикладом такої небезпеки є випадок у Воронежі, де відбувся суд над двома молодими людьми, які розіслали знайдений у Мережі вірус по 400 електронних адресах, включаючи обласну адміністрацію, **Нововоронезьку АЕС**, банк, лікарню і податкову поліцію. Обвинувачувані стверджують, що розіслали вірус жартома. Але, як вище вже було доведено, дуже часто подібні інтернет-атаки дуже ретельно плануються. Немає жодної гарантії, що будь-яке питання як міждержавного (територіальні, геополітичні, міжнаціональні проблеми), так й внутриполітичного рівня (відношення до НАТО, конфлікт з владними структурами) не може стати сигналом для окремої людини чи групи спеціалістів для здійснення відповідної кібератаки.

Отже, вже сьогодні Україні потрібний цілий комплекс законів та документів, що були б в змозі регулювати діяльність у національному сегменті Інтернету. Крім цього, країна потребує створення державних структур, які б були спроможні ефективно та швидко захистити у кіберпросторі національні інтереси та, по можливості, покарати порушника. Від вирішеня цих питань буде залежати розвиток інформаційних технологій та, певним чином, швидкість її інтеграції у глобальну економіку.

ДЖЕРЕЛА:

1. Поль Вирилио. Информационная бомба. Стратегия обмана. - М.: Фонд научных исследований «Прагматика культуры», 2002.
2. И. Кузнецов. Учебник по информационно-аналитической работе. М.: "Яуза", 2001.
3. С. Модестов, С. Сокут. Байты вместо пуль // Независимое военное обозрение № 13. – 9-15.04.1999
4. А. Леонов. Правительство on-line // ComputerWorld/Украина.- 07.11.2001

5. А. Леонов. Войны в Сети // ComputerWorld/Украина.- 05.09.2001
6. А. Леонов. Виртуальные тени реальных войн // ComputerWorld Украина. – 04.09.2002
7. О. Леонов. Інтернет як інструмент ведення кібернетичної війни // Стратегічна панорама. – 2002. - № 3

Лупаций В.С. ПОСТИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УСЛОВИЯХ ТОТАЛЬНОЙ И ГЛОБАЛЬНОЙ МАНИПУЛЯЦИИ *

При разговоре о манипулятивных технологиях, вспоминается эпитафия нашего великого соотечественника Г.С.Сковороды - "Світ ловив мене та не спіймав". Таким образом, проблема защиты от манипуляций и сохранение ясности и чистоты сознания возникла отнюдь не вчера. Однако сегодня манипулятивные технологии приобрели качественно иные характеристики.

Прежде всего, в современном мире пространство манипуляции стало тотальным и глобальным. Это связано с тем, что количественный и качественный рост интернета в комбинации с технологиями мультимедиа как бы "замыкают" манипулятивное пространство виртуальной реальности, которая начала выстраиваться с момента появления феномена СМИ и особенно телевидения.

Таким образом, виртуальная реальность становится тотальной и "захватывает" как индивида, так и социум. В следствии доминирования виртуальной реальности над социумом и индивидом возникает ряд побочных негативных эффектов. Прежде всего жизнь в условиях тотальной виртуальной реальности приводит к тому, что у индивида формируется набор алгоритмов, а не творческая интуиция. По мере нарастания коммулятивного эффекта происходит формирование нового антропологического типа с низким уровнем как интеллекта, так и нравственности.

Наиболее действенным противоядием от нарастания указанной социальной патологии может стать комплекс мер по "Восстановлению статуса полноценного мышления" (О.Г.Бахтияров). Решение указанной задачи предполагает переосмысление технологий психо-соматичного самосовершенствования, в том числе потенциал практик духовного роста, накопленных в мировых религиях. В целом усилия должны быть направлены на создание условий работающих на становление нового типа человека, сознание которого развито в четырех измерениях. Условно можно говорить о формировании типа личности, который не будет требовать руководства извне, то есть в виде закона, денег и т.п.

Во-вторых, следует учитывать, что сегодня мир впервые сталкивается с проблемами, которые превышают возможности как индивидуального созна-

* Манипулятивные стратегии в политике, экономике, бизнесе и методы противодействия. Материаллы конференции. – К., 2001

ния, так и компьютерных технологий. Фактически мир переживает крах "иллюзии информации". Новая информация теряет актуальность быстрее чем ее успевают эффективно использовать. Именно поэтому, речь должна идти о поиске альтернативы информации как базового управленческого ресурса, за счет которого воспроизводятся виртуальные реальности и технологии манипуляции. В этой связи, технологии формирования "целостного сознания" должны ориентироваться на разработку и создание методов, технологий и реальных объектов, которые уже принадлежат к пост-информационной реальности.

С организационной точки зрения, решение указанной задачи предполагает формирование спроса на внутреннем рынке, "организацию" в обществе социального заказа на весь комплекс психо-технических работ. Фактически должен быть поставлен вопрос о создании в Украине новой отрасли по разработке и применению пост-информационных технологий, за счет которых только и возможно преодолеть тиранию виртуальной реальности по отношению к индивиду и социуму.

В-третьих, с глобальными технологиями манипуляции тесно связаны современные целенаправленные попытки реинтерпритировать мировую историю, истории наций и этносов. Так, например, в России ведутся поиски русского пантеона православных святых, активно развивается евразийская концепция, посаженная усилиями А.Дугина на фундамент сакральной геополитики. В Чехии широкий социальный резонанс получило движение, продвигающее новую модель самоидентификации чехов. В социо-культурном плане в Чехии предпринимаются попытки идентифицировать себя не в качестве наследников империи западных славян, а цивилизации кельтов. Появляются заявки на реинтерпретацию истории Северной Америки и это только начало.

Как бы там ни было, но академические модели развития мировой истории, заложенные еще в 19-м веке стремительно делегитимизируются. В результате идет зачистка пространства открытого как для уточненных версий мировой и национальной истории, так и для глобальных манипуляций смыслом исторического бытия наций и народов, человеческой цивилизации в целом.

В Украине против профанации истории украинской государственности активно выступает журнал "Перехід-IV", в рамках которого развивается концепция "Индоевропейской мета-цивилизации". Однако очевидно, что "проект Украина" должен быть обращен в будущее. А интерес к истории должен стимулировать не усилия по "возрождению" ценностей "золотого века" (эпоха Казацкой державы), а на анализ феномена государственности на землях теперешней Украины в интервале от "послепотопных" времен и до наших дней. Такой подход позволит провести десакрализацию мировой и национальной истории, не скатываясь при этом к нигилизму и забытью истории и ее уроков.

Наконец не следует сбрасывать со счетов новые метатеории, задающие содержательные коридоры, в рамках которых разворачиваются глобальные технологии манипуляции.

Ярким примером является концепт, принадлежащий перу американского теоретика С.Хантингтона - "Война цивилизаций". Трудно переоценить манипулятивный потенциал концепции, которая в эпоху экономической глобализации и Интернета "прошивает" цивилизационные границы и "актуализирует" линии столкновений между цивилизациями. Фактически это руководство к действию, которое вполне может быть использовано США для нейтрализации геоэкономических конкурентов, "обремененных" своим происхождением и цивилизационным наследие. Концепция С.Хантингтона является далеко не абстрактной теорией. Так, например, Украина уже сегодня находится в эпицентре "столкновения цивилизаций".

Это проявляется:

- в реанимации, в связи з визитом в Украину Папы Римского, вражды и конфликта православных, ориентированных на УПЦ Московского патриархата и греко-католиков (униатов);
- в латентном напряжении, сохраняющемся между крымскими татарами (ислам) и русским большинством (православные коммунистической закалки);
- в сарказме и недоверии между членами возрождающихся иудейских общин в Украине и растущей массой маргинального населения, которое не лишено вируса бытового антисемитизма.

Таким образом, в Украине решение задачи по "дезактивации" манипулятивных технологий, которые спекулируют на религиозных чувствах людей следует вывести на уровень проблемы национальной безопасности.

В прикладном плане речь идет о стимулировании и культивировании процесса примирения между тремя мировыми религиями (христианство, ислам и иудаизм), что предполагает пересмотр целого ряда религиозных догматов, написанных не то Богом, не то от имени Бога. В III тысячелетии социальной нормой могла бы стать ситуация, при которой можно ходить в любую церковь, *духовно обогащаться и при этом никого не предавать.*

Минихэн К. А. ОБОРОНА СТРАНЫ ОТ КИБЕРНЕТИЧЕСКОЙ АТАКИ: ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СРЕДЕ*

"Нам грозит опасность. Жизнь в Америке во многом зависит от компьютеров. С помощью компьютеров осуществляется управление системами распределения электроэнергии, системами связи, средствами авиации и финансами. Компьютеры используются для хранения важнейшей информации, начиная с историй болезни и бизнес-планов и кончая сведениями о судимости. И хотя мы доверяем компьютерам, они подвержены риску как случайных

* Электронный журнал ЮСИА. – 1998. – т. 3. – № 4 (ноябрь) – http://usinfo.state.gov/journals/itps/1198/ijpr/pj48min.htm

сбоев в результате несовершенной конструкции или недостаточного контроля за качеством, так и — что более тревожно — риску умышленных посягательств. Вооружившись компьютером, современный вор может украсть больше, чем используя огнестрельное оружие. Завтрашний террорист сможет причинить более серьезный ущерб с помощью клавиатуры, чем с помощью бомбы".

"Компьютеры в опасности", Национальный исследовательский совет, 1991

Введение. Наверное, в приведенных выше словах самое примечательное то, что они были написаны еще на заре информационного века. До недавнего времени наша страна не придавала им большого значения. Соединенные Штаты и весь остальной мир по-прежнему не задумываясь используют достижения информационной революции, все глубже и глубже погружаясь в кибернетическое пространство. Информационные технологии продолжают быстро внедряться в жизнь и экономику нашей страны, которая является элементом глобального сообщества. "Информационная супермагистраль" в полном смысле стала неотъемлемым элементом экономики.

Соединенные Штаты ведут за собой мир в информационный век, но при этом сами они почти полностью зависят от информационных технологий — компьютеров и глобальных сетей, которые связывают эти компьютеры воедино. Эта зависимость превратилась в очевидную и непосредственную угрозу нашему экономическому благосостоянию, безопасности нашего общества и нашего государства.

Существующие в мире глобальные компьютерные сети, которые часто называют "кибернетическим пространством", не знают физических границ. Расширяя наши контакты с помощью кибернетического пространства, мы все больше подвергаем себя опасности посягательств со стороны старых и новых противников, число которых увеличивается. Террористы, радикально настроенные группы, наркодельцы, действующие лица в системе организованной преступности и враждебно настроенные к нам государства будут использовать многочисленные сложнейшие орудия информационной войны. Информационная война может дополнить или целиком заменить собой войну в привычном ее понимании, что в значительной степени усложняет и расширяет список угроз, которые необходимо предвидеть и предотвратить. Опасности подвергается не только информация, хранящаяся или передающаяся в кибернетическом пространстве, но и все компоненты нашей национальной инфраструктуры, зависящие от информационных технологий и от своевременного доступа к надежным данным. К этим компонентам относится сама телекоммуникационная инфраструктура, наши банковская и финансовая системы, система электроснабжения и другие энергетические системы, такие как нефте- и газопроводы, транспортные сети, системы водоснабжения, системы медицинских услуг и здравоохранения, полиция, пожарная и спасательная службы, а

также государственные органы и учреждения всех уровней. Все они необходимы для успешной экономической деятельности и обеспечения национальной безопасности.

Защита информационных систем — общенациональная задача. 22 мая 1998 г. Президент подписал директиву за номером 63 (ПДР-63) о мерах по защите важнейших объектов инфраструктуры. В этой директиве говорится: "Я намерен обеспечить принятие Соединенными Штатами всех необходимых мер для скорейшего устранения любых серьезных недостатков, делающих важнейшие объекты нашей инфраструктуры, и особенно наши компьютерные системы уязвимыми как к физическому, так и компьютерному нападению.

Общенациональная задача состоит в том, чтобы не позднее 2000 г. в Соединенных Штатах был разработан первоначальный комплекс мер в этой области, а не позднее, чем через пять лет были созданы средства и возможности для защиты важнейших объектов нашей инфраструктуры от умышленных акций, способных нанести существенный ущерб:

- Федеральному правительству в осуществлении важнейших задач в сфере национальной безопасности и обеспечения охраны здоровья и безопасности граждан;
- Правительствам штатов и местным органам власти в поддержании общественного порядка и предоставлении населению основных видов услуг;
- Частному сектору в обеспечении нормального функционирования экономики и работы важнейших телекоммуникационных, энергетических, финансовых и транспортных служб".

Реализация этой масштабной задачи потребует значительного напряжения сил и совместных усилий правительственных органов и частных компаний, отвечающих за работу важнейших объектов инфраструктуры. Согласно директиве Президента, федеральное правительство должно подать пример, обеспечив надежную работу федеральных систем. Но одновременно в президентской директиве указывается, что государство не сможет решить это проблему в одиночку. Работа каждого федерального ведомства и агентства в значительной степени зависит от услуг, предоставляемых частным сектором — речь идет об энергоснабжении, телекоммуникациях, транспорте и так далее. В связи с этим президентская директива предусматривает формирование партнерских отношений между государственным и частным сектором с целью разработки и реализации комплексного плана защиты национальной кибернетической инфраструктуры и борьбы с угрозой электронного терроризма. Сегодня встает непростая задача привлечения частного сектора к подобным мероприятиям в общенациональных масштабах. В настоящих условиях жесткой конкуренции в целях увеличения прибыли частные компании стремятся получить разного рода рыночные преимущества, включая

понижение производственных издержек. Усиленные меры защиты компьютерных систем потребуют как увеличения капиталовложений, так и определенного сотрудничества с конкурентами.

Важнейшие элементы. Любая стратегия, имеющая целью укрепление важнейших объектов нашей инфраструктуры, должна состоять из трех основных элементов: повышения степени защиты от посягательств на компьютерные системы, выявление подобных посягательств в тот момент, когда они происходят, противодействие им и/или восстановление инфраструктуры после нанесения ей ущерба.

Меры по усилению защиты от посягательств на компьютерные системы основаны на технологиях кодирования информации — включая опознавательные цифровые коды — обеспечивающих подтверждение личности пользователя, целостность информации, невозможность отрицать факт ее получения, а также конфиденциальность — то есть все, что необходимо для информационной защиты. Самым мощным средством защиты от посягательств на компьютерную информацию, вероятно, служит система опознавательных цифровых кодов. Встроенные опознавательные цифровые коды также обеспечивают целостность электронной информации и невозможность отрицать факт ее получения по системам компьютерной связи. Кодирование применяется в настольных компьютерах, файловых серверах и в компьютерных сетях для обеспечения конфиденциальности правительственной, деловой и личной информации, не подлежащей разглашению. Технологии кодирования, которые когда-то были исключительной прерогативой правительственных органов, сегодня широко применяются в коммерческой практике и представляют собой основное средство информационной защиты. 16 сентября 1998 г. вице-президент США объявил о крупных изменениях в мерах по контролю экспорта из США технологий кодирования, что подчеркивает важное значение таких технологий для защиты важнейших объектов инфраструктуры, глобальной электронной коммерции и экономического благополучия страны.

Поскольку технологии кодирования уже достигли необходимого уровня развития, встает задача последовательного и эффективного применения этих технологий во всех важнейших звеньях нашей инфраструктуры. Для этого потребуется создание рамочных условий, в которых услуги по кодированию информации могли бы комплексно предоставляться на всех уровнях. Необходимо также формирование особой вспомогательной инфраструктуры, то есть системы криптозащиты на основе публичного ключа, которая обеспечивала бы надежные и глобально распознаваемые цифровые подписи и сертификацию шифрующего ключа. По сути такая инфраструктура позволяла бы людям обладать уникальными "электронными удостоверениями личности", которые соответствовали бы всем требованиям информационного века. Услуги в этой области начинают появляться в частном секторе в связи со спросом на них со стороны глобальной

электронной коммерции. Но ими можно воспользоваться и при защите важнейших объектов инфраструктуры.

Сегодня не существует еще достаточно совершенных или эффективных технологий для того, чтобы прогнозировать, выявлять или реагировать на посягательства в отношении компьютерных систем. В настоящее время у Соединенных Штатов мало возможностей для выявления или распознавания посягательств на компьютерные системы правительственных или частных объектов инфраструктуры, и еще меньше возможностей для того, чтобы реагировать на такие посягательства. Способность идентифицировать посягательства на компьютерную систему одного или нескольких стратегических объектов инфраструктуры и соответствующим образом реагировать на такие посягательства безусловно представляет собой важнейшую задачу в сфере национальной безопасности. Дело осложняется еще и тем, что любое вторжение в компьютерные системы традиционно рассматривается как правонарушение и находится в компетенции правоохранительных органов. Когда происходит такое вторжение, *нарушителя выявляют (если это возможно), арестовывают и подвергают суду.* Но многие частные компании неохотно предоставляют информацию о вторжениях в их компьютерные системы, опасаясь негативного освещения в прессе (например, газетных заголовков типа: "В результате компьютерного вторжения банк потерял миллионы долларов", или "Компьютерные взломщики вывели из строя телефонную сеть"), а также негативной реакции со стороны общественности. Для того, чтобы построить эффективную национальную систему защиты компьютерных сетей, необходимо разработать новые "правила игры", создающие возможности для более открытого и динамичного сотрудничества между частным сектором, правоохранительными органами и службами национальной безопасности.

Новая роль Агентства национальной безопасности в деле защиты информации. В условиях информационного века традиционные задачи, которые выполняет Агентство национальной безопасности, такие, как электронная разведка и обеспечение безопасности информационных систем, эволюционируют в направлении обеспечения информационного превосходства Соединенных Штатов и их союзников. Главное в решении этой задачи — глубокое понимание глобальной информационной инфраструктуры и уязвимости информационных систем, объединенных в сети. АНБ уже предпринимает ряд мер по разработке технических основ защиты важнейших объектов нашей инфраструктуры.

Как уже упоминалось выше, технологии кодирования информации получили широкое распространение в коммерческой практике и служат основным средством защиты информационных систем от внешних посягательств. Плохо то, что многие продукты, которые уже существуют сегодня в этой сфере, не обеспечивают надежного взаимодействия друг с другом и имеют разную степень надежности, а, кроме того, существует

множество методов кодирования информации, которые часто не согласуются друг с другом. Так, например, существует кодирование электронной почты, кодирование файлов, кодирование вебсайтов, кодирование отсылок (линков) и кодирование виртуальных частных компьютерных сетей — и этот список можно продолжить. Чтобы поправить сложившееся положение, АНБ установило партнерские отношения с ведущими поставщиками технологий по защите информации с целью разработки общей основы кодирования информации, обеспечивая единообразие методов информационной защиты в рамках целого предприятия. Такая основа определяет пути согласованного применения технологий кодирования информации на предприятии, а также взаимодействия с другими обеспечивающими безопасность технологиями и продуктами, например, такими, как системы блокировки, серверы, маршрутизаторы, операционные системы, системы выявления вторжений, системы выявления преднамеренно дефектных кодов, средства проверки и инфраструктура публичных электронных ключей.

Другая сторона проблемы состоит в разной степени надежности разнообразных средств защиты, имеющихся на рынке. С целью решения этого вопроса АНБ установило партнерские отношения с Национальным институтом стандартов и технологий (НИСТ). В рамках этого партнерства АНБ и НИСТ будут осуществлять аттестацию коммерческих лабораторий, с тем, чтобы они могли проводить экспертизу средств защиты, подтверждая параметры защиты, о которых заявляет продавец, либо их соответствие критериям защиты, применяемым в конкретной компьютерной сети. Испытания продуктов будут проводится аттестованными лабораториями на платной основе; при этом лаборатория и фирма, реализующая продукт на рынке, будут договариваться о размерах оплаты и сроках.

Наконец, Агентство национальной безопасности считает, что в стране должен быть создан общий для всех набор средств защиты информации, имеющей важное значение с точки зрения национальной безопасности, и в связи с этим использует имеющийся у него уникальный опыт в разработке фундаментальных технологий для создания общенациональных возможностей по выявлению посягательств на компьютерные системы и реагированию на них. Эти технологии предусматривают интегрированное использование целого ряда датчиков, которые могут применяться на важнейших объектах инфраструктуры и в самой телекоммуникационной инфраструктуре, и которые обладают широким диапазоном аналитических возможностей для динамичного распознавания угроз, возникающих со стороны глобального кибернетического пространства в отношении важнейших объектов инфраструктуры. Эти технологии должны стать общими для органов национальной безопасности, федеральных учреждений, промышленных отраслей и региональных органов и должны обеспечивать одновременное выявление посягательств, защиту от них и восстановление работы важнейших служб и объектов инфраструктуры.

Заключение. Нынешний высокий уровень благосостояния нашей страны во многом опирается на достижения информационного века и на наше глобальное лидерство в области информационных технологий. Наше дальнейшее лидерство и процветание в системе глобальной экономики будут во многом зависеть от того, сумеет ли наша страна возглавить усилия в деле защиты информации в условиях глобальной информационной среды, которую мы сами помогали создавать. Издав Директиву-63, администрация США ясно дала понять, что настало время действовать, а со своей стороны Агентство национальной безопасности США готово откликнуться на этот призыв и предоставить имеющиеся у него технический опыт и знания. Информационное превосходство в информационный век — несомненно дело государственной важности.

Мюнклер Х. ТЕРРОРИЗМ КАК СТРАТЕГИЯ КОММУНИКАЦИИ. ПОСЛАНИЕ 11 СЕНТЯБРЯ.*

Аналитики, исследующие проблемы применения насилия, уже в семидесятые годы обратили внимание на то, что стратегия терроризма в меньшей степени нацелена на прямые физические последствия терактов, на наносимый ими материальный ущерб или количество погибших, на выведение из строя систем снабжения и т.д, а в значительно большей мере ориентирована на психологические эффекты, такие как страх и ужас, воодушевление и надежду (1).

В конце 60-х -начале 70-х годов современная стратегия терроризма развивалась как форма замещения партизанской борьбы или, соответственно, как некая предшествующая ей форма. Терроризм в виде рассчитанной на длительный период политико-военной стратегии существует не более тридцати лет. Даже если террористы долгое время использовали то же самое оружие, что и их предшественники, главным образом анархисты(2), все же фундаментальное отличие кроется в том, что они соединили это оружие с воздействием средств массовой информации. Это объединение представляет собой, так сказать, решающую инновацию в ходе использования террористами насилия.

Террористические стратегии не могут действовать без усиливающего эффекта публичности. В соответствии с этим в процессе интенсивного наращивания пробивной силы они следуют образцам медийных революций, в результате которых из локальной, в лучшем случае региональной общественности возникла мировая общественность, обслуживаемая в режиме реального времени. Решающими этапами этого процесса были возникновение массовой печати, распространение радио и, наконец, победное шествие телевидения по

Журнал «Международная политика» 2001 № 12 –
http://www.deutschebotschaft-moskau.ru/ru/bibliothek/internationale-politik/2001-12/article03_p.html

мере запуска на орбиту ретрансляционных спутников. При отсутствии этой мировой общественности террористические акты, осуществленные 11 сентября 2001 года, не возымели бы, несмотря на колоссальные разрушения и большое количество жертв, того воздействия, которое они оказали в кратко- и среднесрочной перспективе. Ни одна стратегия не способна использовать так называемый фактор CNN столь же эффективно и успешно, как террористическая стратегия.

В целом, терроризм можно определить как стратегию, которая при мобилизации незначительных собственных ресурсов позволяет террористам тягаться в насильственном конфликте с бесконечно превосходящими их по силе и возможностям державами. Эта способность обусловлена двумя особенностями, которые отличают террористическую стратегию от других форм вооруженного разрешения конфликтов. Это, во-первых, полное игнорирование всех и всяческих правил ведения войны, начиная от обозначения собственных бойцов с целью их отличия от не участвующих в борьбе людей, и до использования гражданского населения противника в качестве живого щита и заложников террористических групп; а во-вторых, безоглядное использование гражданских ресурсов атакованного противника в собственных военных целях.

Максимальные эффекты. К гражданским ресурсам атакованного противника, используемым террористами и обращаемым в качестве военных средств против него самого, относятся преимущественно транспортная и коммуникационная системы подвергающейся нападению стороны: от обычных курьерских служб и почты, которым можно всучить бомбы в виде пакетов и тому подобное - в последнее время это были письма со спорами сибирской язвы - до транспортных систем (преимущественно гражданской авиации) и систем высокоскоростной передачи данных, в которые можно запустить компьютерные вирусы, чтобы заблокировать или разрушить комплексную информационную структуру современных обществ. Но прежде всего к этим гражданским ресурсам относятся информационная и развлекательная системы, с помощью которых даже сравнительно небольшим акциям можно придать непропорционально большой резонанс.

Для этого, разумеется, необходимо планировать террористические акции таким образом, чтобы они достигали максимального эффекта с точки зрения коммуникационной стратегии. Одним из примеров этого служит захват израильских спортсменов группой палестинских террористов во время Олимпийских игр 1972 года в Мюнхене, другим - угон в июне 1985 года самолета авиакомпании ТВА, следовавшего рейсом 847, и семнадцатидневное удержание в заложниках в аэропорту Бейрута специально отобранных американских пассажиров. Этот инцидент необходимо выделить особо, поскольку последствием террористической акции стало ее самое интенсивное на тот момент освещение в средствах массовой информации (3). И наконец, еще одним примером является комбинированная террористическая акция 11 сентября - не

только потому, что она повлекла за собой наибольшее из имевшихся до сих пор при терактах количество жертв, но и прежде всего также по той причине, что поразила центры и символы глобального американского господства: Пентагон как командный центр, в который сходятся все нити управления американским военным аппаратом, и Всемирный торговый центр в его качестве одного из важнейших диспетчерских пунктов капиталистической экономики. Наряду с этим Пентагон слыл символом американской неуязвимости, а башни-близнецы Всемирного торгового центра символизировали доминирование американского капитала во всем мире.

Итак, это было (и остается) первым посланием от 11 сентября: картины сначала объятых пламенем, а затем обрушивающихся башен-близнецов представляют собой контр-символы к американскому доминированию, или также демонстративно инсценированную десимволизацию. Они показывают возможность нападения на США, демонстрируют уязвимость Америки, причем не только на периферии ее влияния - это подтвердили террористические акты против казармы морских пехотинцев в Бейруте и взрывы бомб у американских посольств в Найроби и Дар-эс-Саламе -, но также и непосредственно в центрах ее могущества: в Нью-Йорке и Вашингтоне. Ничто не могло бы запечатлеть это послание в сознание мировой общественности столь же убедительно и неизгладимо, как картины 11 сентября и следующих дней, когда сначала бесконечно крутили кадры любительской видеосъемки с врезающимися в башни-близнецы Всемирного торгового центра самолетами, которые сменились потом кадрами все еще дымящихся развалин на Ground Zero.

Вплоть до начала воздушных налетов на Афганистан борьба между стратегами террора и Соединенными Штатами Америки была в значительной мере войной телевизионных картинок, в которой США лишь медленно и постепенно смогли добиться паритета с напавшими на них террористами. Сначала вновь и вновь прокручивались кадры развертывания флота, которые служили сигналом того, что будет нанесен сокрушительный ответный удар, но на его подготовку потребуется еще несколько дней. К этому добавлялись картины патриотической решимости населения Нью-Йорка, хотя и казавшиеся подчас европейским зрителям несколько крикливыми, но выражавшие, что послание террористов не оказало на потерпевшую сторону ожидавшееся воздействие.

Эти адресованные мировой общественности ответные послания - демонстрация колоссальной военной машины, которая будет вскоре пущена в ход, и патриотическая решимость американского гражданского населения, не поставленного на колени брошенным террористами вызовом и готового взвалить на себя тяготы затяжной войны против международного терроризма, - дополняла и сплачивала воедино агрессивная военная риторика Джорджа В.Буша, функция которого вопреки спонтанно возникавшему впечатлению заключалась в значительной мере в том, чтобы выиграть время для Соединенных Штатов и идентифицировать нападавших, определенным образом ло-

кализовать их и, наконец, выработать приемлемую стратегию борьбы и победы над ними (4).

Третья сторона, которую "пытаются заинтересовать". До сих пор речь шла только об одной стороне послания, которое содержали в себе террористические акты 11 сентября: они адресовались атакованным американцам и должны были посеять страх и ужас. Однако, как правило, террористические акты представляют собой не только послание подвергшимся нападению, но и обращены к тем, кого в стратегии терроризма можно назвать потенциально заинтересованной третьей стороной. Речь при этом может идти, в зависимости от политико-идеологической направленности террористических групп, об этнических или религиозных меньшинствах в одном из государств, для которых необходимо отвоевать особые права или добиться также их политической независимости, об ущемленных в социальном плане, политически маргинальных слоях и классах. Террористы претендуют на стимулирование их революционной эмансипации. Далее речь может идти о группах, недавнему привилегированному положению которых угрожают общественные или политические преобразования. И в заключение, третьей стороной, способной проявить интерес, могут быть определяемые по религиозно-культурным признакам большие группы, которыми при осуществлении террористических актов 11 сентября являлись, по-видимому, широкие слои населения исламского мира.

Адресованное им и заключенное в террористических актах послание гласит, что сопротивление не только возможно, но и может вестись успешно. Все чаще встречаемые в новейших исследованиях терроризма различия между этно-националистическим, социально-революционным, направленным на проверку бдительности и религиозным терроризмом можно развивать как в плане соответствующего определения врагов, так и выявления потенциально заинтересованной третьей стороны. При этом послание, содержащееся в террористических актах, варьируется прежде всего в отношении третьей стороны, которую хотят заинтересовать.

Определение потенциально заинтересованной стороны в гораздо большей, чем соответствующее определение врага, мере имеет функцию регулирования выбора возможных целей и увеличения или ограничения количества жертв террористических актов и покушений. На протяжении многих десятилетий большинство исследователей терроризма склонялись к выводу о том, что усиление эффекта террористических актов путем их освещения средствами массовой информации вкупе с потребностью максимально точно и однозначно сформулировать послание к третье стороне, которую предполагается заинтересовать, будет способствовать тому, что террористы ни в коем случае не прибегнут к использованию оружия массового уничтожения, в особенности бактериологических и химических боевых веществ, поскольку при этом могли бы погибнуть или пострадать лица, относимые к потенциально заинтересованной третьей стороне, что представляло бы угрозу для собственных легитимационных ресурсов террористов.

Терроризм с религиозной мотивацией. Но это предположение было справедливо, очевидно, лишь по отношению к этно-националистическому и социально-революционному терроризму, при котором необходимо максимально точно очертить третью сторону, каковую собираются заинтересовать, а сами теракты необходимо убедительнейшим образом спланировать и осуществить как четко адресованные послания. Совершенно ясно, что в случае терроризма с религиозной мотивацией действие этого правила ослаблено: значительному расширению дефиниции врага, которая не подлежит более ограничению с точки зрения позиции или образа действия, соответствует расплывчатость образа третьей стороны, каковую предполагается заинтересовать. Вследствие этого нападения террористических групп, определявшиеся религиозно-культурной мотивацией, уже задолго до событий 11 сентября приводили к значительно большему количеству жертв, чем теракты групп с этно-националистическими или социально-революционными мотивами (5).

Применение ядовитого газа в Токийском метро, когда впервые прибегли к использованию оружия массового уничтожения, являло собой образец терроризма с религиозными мотивами. Первое нападение на Всемирный торговый центр в 1993 году - взрыв бомбы колоссальной мощности в подземном гараже под комплексом зданий, - который должен был обрушить обе башни, также на счету террористической группы, имеющей в широком смысле религиозно-культурную направленность (6). Объединение религиозных мотиваций и террористической стратегии привело к значительному ускорению раскручивания спирали эскалации и трагическому увеличению количества жертв(7). Это можно объяснить тем, что террористы с религиозными побуждениями не нуждаются в третьей стороне, которую предполагается заинтересовать, поскольку используют для легитимации своих действий апокалиптические представления или идеи тысячелетнего царства Христова.

Те, кому нет нужды при осуществлении своих акций обращать внимание на то, чтобы при этом не пострадали лица, причисляемые к третьей стороне, которую желательно заинтересовать, могут действовать почти без всяких ограничений. Именно террористы с религиозной мотивацией являются подлинными заказчиками того, что они называют тотальной войной. Это означает, их заказ является производным от них самих, и для легитимации им не нужны посторонние группы. Поэтому для террористов с религиозной мотивацией не имеют значения границы применения насилия, которые вынуждены устанавливать светские террористы, чтобы обратиться таким образом к своим сторонникам, не имеющим твердых убеждений и оказывающим им лишь ограниченную поддержку. Это отсутствие сторонников в том смысле, в котором имеют их светские террористы, ведет к разрешению применения почти ничем не ограниченного насилия против практически бесконечной категории целей, т.е. против любого, кто не исповедует данную религию или не является членом религиозной секты террористов" (8).

В соответствии с этим, послания, исходящие от террористических актов, осуществляемых группами с религиозной мотивацией, явным образом отличаются от аналогичных посланий террористов с социально-революционной и этно-националистической мотивацией. У подпитываемого религиозными идеями терроризма существует иная, нежели у светских террористических групп, коммуникация. Прежде всего напрашивается вывод о том, что движимые религиозными убеждениями террористы - независимо от того, исповедуют ли они исламский, иудейский или христианский фундаментализм, - отказываются брать на себя ответственность за содеянное, как это регулярно происходит в связи с террористическими актами, т.е. не делают заявлений, не разъясняют мотивы теракта вкупе с распространением оправданий и требований, а уповают исключительно на выразительность самих картин содеянного. В коммуникационной стратегии терроризма с религиозной мотивацией картины отделились от текста. Так, и послание от 11 сентября также было сделано в форме картин в полном отрыве от текста.

А вот последствия того, что послания становятся полисемическими: они могут означать очень многое, и для пущей надежности в них вкладывается сразу несколько сообщений. Но в картинах терактов невозможно рассмотреть, как они соотносятся друг с другом по степени важности, ведь картины распространяются без авторизованного террористами субтекста. Подобная неопределенность в случае с религиозно мотивированным терроризмом не является тактическим недостатком, как это было бы, пожалуй, при деяниях террористов с этно-националистическими или социально-революционными побудительными причинами, а представляет собой главную составную часть стратегии: подвергшейся нападению стороне загадывают загадку и оставляют ее в неведении относительно того, достижением каких политических целей могли бы удовлетвориться нападающие.

Теракты 11 сентября не имеют однозначной политической мотивации. Связаны ли они с палестинским конфликтом и в особенности с последними осложнениями, или речь идет о физическом присутствии нескольких тысяч американцев на территории Саудовской Аравии? Или дело в принципиальном конфликте ценностей между западными жизненными нормами и законами ислама или, соответственно, его произвольными толкованиями, осуществляемыми террористами?

На поверку это оказалось проблемой не нападавших, а подвергшихся нападению, и связано с дополнительной кодировкой способа осуществления террористического акта: это сознательный отказ террористов от возможных путей отхода и спасения, чтобы миновать таким образом подготовленной для других катастрофы.

Помимо того, что самоубийство террористов при атаках 11 сентября было предпосылкой успешного проведения этой операции, оно еще и подает весть друзьям и врагам, сигнализируя о безоговорочной решимости вести эту борьбу как сражение без возможности достичь компромисса или пойти на ми-

ровую. Таким образом, тот факт, что как раз при осуществлении религиозно мотивированных терактов наблюдается появление все большего числа террористов-самоубийц, имеет наряду с инструментальной сильную символическую составляющую. И, наконец, своим деянием террорист-камикадзе вызывает "непревосходимый эффект публичности" (9).

Повышенное воздействие терактов в демократических государствах. Разумеется, обращает на себя внимание то обстоятельство, что террористическая стратегия, основные черты которой были описаны выше, может, в принципе, проявить свою действенность только в демократических государствах, в то время как в условиях диктатуры и тоталитарных режимов она остается относительно неэффективной и не достигает поставленных целей. В одном репрезентативном исследовании анализировалась связь действий террористических групп после 1945 года с политическими системами, против которых они были направлены. При этом выяснилось, что террористические группы заявляли о себе в демократических государствах в три с половиной раза чаще, чем в странах с авторитарными режимами (10). Очевидно, принципы устройства демократии и связанные с нею, как правило, социальные структуры являются для террористов функциональным эквивалентом того, чем для партизан служат болота и недоступные горные районы (11).

Перво-наперво это более высокая плотность коммуникации в демократических государствах, представляющая собой фундаментальную предпосылку для проявления действенности стратегии терроризма. В странах, где эта коммуникационная плотность недостаточна, общественность вообще не узнала бы о многих террористических актах, а там, где просачивание информации подавляется с помощью государственных средств, как это делается в условиях диктатуры, террористы лишены решающего оружия для ведения своей борьбы. Говоря другими словами, там, где очень плотная коммуникация, существует, соответственно, и повышенная вероятность террористических атак, что необходимо принимать во внимание. Эксперты даже полагают, что тот факт, что в последние тридцать лет американские граждане намного чаще становились жертвами нападений террористов, чем граждане какой-либо другой страны, в решающей степени связан "с несравнимо более высокими шансами на публичность и самопрезентацию террористов во всем мире". Когда они нападали на американских граждан, это становилось новостью, подававшейся на первых местах в информационных передачах американских средств массовой информации, которые принимаются во всем мире (12).

Типичная для демократических государств плотность коммуникации, позволяющая достичь психологические эффекты при осуществлении терактов, характерна, конечно, и для инфраструктуры современных обществ в целом, что открывает перед террористами целый ряд привлекательных целей, по которым можно сравнительно легко нанести удары. Они простираются от транспорта до коммуникационной системы. Чем плотнее и интенсивнее ве-

дутся внутренние и внешние обмены в обществах, чем выше скорость этих обменов, тем уязвимее сами общества для террористических атак.

Сюда добавляется, наконец, то обстоятельство, что общества, где аграрный сектор играет незначительную роль, все сильнее проявляют качества, которые можно, обобщая, назвать "постгероизмом". Героические жесты, свойственные террористическим группам в целом, и в особой мере присущие тем из них, в рядах которых находится большое количество смертников, вызывают в таких обществах особенно сильный резонанс.

Помимо того, что люди, готовые принести себя в жертву, вырабатывают особенно сильное презрение к формам жизни постгероических обществ, в расчетах стратегов террора, по-видимому, играет свою роль и упование на то, что такие общества обладают ярко выраженной ментальностью отступления и капитуляции и быстро проявят готовность откупиться от смертельной опасности, предложив деньги или пойдя также на политические уступки. Повторяющиеся вновь и вновь успешные попытки добиться освобождения находящихся в заключении соратников с помощью захвата заложников и угрозы их убийства убедительно подтвердили это базовое предположение террористических деятелей. В странах с авторитарными или тоталитарными режимами, в которых жизнь отдельно взятого человека не имеет такого большого значения, где невозможно также использовать общественность в качестве инструмента для нагнетания ситуации, эти тактические приемы никогда не смогут набрать сравнимую пробивную силу.

Таким образом, каждый террористический акт, совершаемый в демократических государствах или вообще направленный против них, содержит в себе стереотипное послание. Оно гласит, что нападающие в высшей степени презирают подвергшихся нападению и их формы жизни. В терактах 11 сентября это презрение выражено особенно сильно. И поэтому эти теракты, даже если никто и не взял на себя ответственность за их исполнение, можно понимать как посягательство на западную демократическую форму жизни в целом.

Примечания

1. Образцовое исследование Д.Фромкина. David Fromkin Die Strategie des Terrorismus; in: M.Funke (Hrsg.) Terrorismus. Untersuchungen zur Strategie und Struktur revolutiondrer Gewaltpolitik, Bonn 1977 (Schriftenreihe der Bundeszentrale fьr politische Bildung, Bd. 123), S.83-99, insbes. S.93 ff.; vgl. zusammenfassend Mьnkler Guerillakrieg und Terrorismus; in:Neue politische Literatur, XXV. Jg. 1980, Heft 3, S.299-326 [Стратегия терроризма. В: М.Функе (изд.) Терроризм. Исследования стратегии и структуры политики насилия революционеров. Бонн 1977 (серия публикаций Федерального центра политического просвещения). т.123, С.83-99, в особенности с.93. Ср.: Х.Мюнклер Партизанская война и терроризм. В: Новая политическая литература, XXV, 1980 г., №3, С.229-326].

2. Обстоятельно на эту тему см. Walter Laqueur, Terrorismus, Kronberg/Ts. 1977, S.22-77 Вальтер Лакер. Терроризм. Кронберг/Тс., 1977, с.22-77.
3. Bruce Hoffman Terrorismus - der unerkldrte Krieg. Neue Gefahren politischer Gewalt, Frankfurt/M. 1999, S.174f [Брюс Хоффман Терроризм-необъявленная война. Новые угрозы политического насилия. Франкфурт-на-Майне, 1999, С. 174].
4. Многочисленные европейские наблюдатели и комментаторы явно превратно истолковывали воинственную риторику американского президента, поскольку они интерпретировали ее, обращая внимание на соответствующее намерение, а не на функцию выигрывания времени при создании так называемой антитеррористической коалиции. Впрочем, я не хочу утверждать тем самым, что президент Джордж В.Буш сам намеревался достичь эти функциональные эффекты. В отличие от этого они были явно запланированы в сценариях штабов и советников, которые разработали политику борьбы с международным терроризмом повсюду в мире.
5. Ср. Peter Waldmann Terrorismus. Provokation der Macht, Mьnchen 1998, S 23 f [Петер Вальдманн Провокация силы. Мюнхен, 1998, С. 23].
6. Ср. Russ Baker Vorbote des Unheils. Der Mann, der das erste Attentat auf das World Trade Center verьbte; FAZ, 11.11.2001, S.8[Р.Бейкер Предвестник несчастья. Человек, осуществивший первый теракт против ВТО. ФАЦ 11.11.2001, С.8.
7. Ср. Laqueur Die globale Bedrohung. Neue Gefahren des Terrorismus, Berlin 1998, S.315 ff.[В.Лакер. Глобальная угроза. Новые опасности терроризма. Берлин, 1998, С. 315.
8. Брюс Хоффман, см. выше, С. 122 .
9. Ср. Петер Вальдманн, см. выше, С. 108.
10. Ср.W. Lee Eubank and Leonard Weinberg. Does Democracy Encourage Terrorism?, in: Terrorism and Political Violence, Bd. 6, №4, (зима 1994), С. 417-443.
11. При партизанской войне можно обойтись и без ее освещения в средствах массовой информации, однако для городского терроризма публичность имеет жизненно важное значение. Чем меньше террористическая группа, тем больше она зависит от публичности. Так считает Вальтер Лакер (см. выше).
12. Брюс Хоффман, см. выше, С. 180.

Най Дж., Оуэнс У. ГЛАВНАЯ СИЛА АМЕРИКИ – ЕЕ ИНФОРМАЦИОННЫЕ ВОЗМОЖНОСТИ *

Силы и ресурсы будущего. Сегодня в большей степени чем раньше знания – сила. Та страна, которая возглавит информационную революцию, и будет обладать большей силой по сравнению с другими странами. В обозримом будущем такой страной, очевидно, останутся Соединенные Штаты. Америка обладает явной военной и экономической мощью. Между тем, ее менее очевидное преимущество перед другими странами состоит в способности собирать, обрабатывать, использовать и распространять информацию – преимущество, которое почти наверняка будет увеличиваться в течение следующего десятилетия. Это преимущество появилось в результате усилий, предпринятых в годы холодной войны, и существования в Америке открытого общества, благодаря чему Америка играет доминирующую роль в использовании важнейших средств связи и информационных технологий, таких как спутниковое наблюдение, прямое вещание, высокоскоростные компьютеры, а также обладает непревзойденными возможностями в интегрировании сложных информационных систем.

Это информационное преимущество способно помочь в сдерживании или нейтрализации традиционных военных угроз при сравнительно низких затратах. В мире, где изменился смысл понятий сдерживания, ядерного зонтика и неядерного устрашения, наличие информационного преимущества способно укрепить интеллектуальную связь между внешней политикой США и их военной мощью и вызвать появление новых способов сохранения лидерства в альянсах и временных коалициях.

Информационное лидерство имеет не менее важное значение в качестве средства, усиливающего эффект американской дипломатии, в том числе в качестве инструмента "мягкой силы" – использования привлекательности американской демократии и свободного рынка. Соединенные Штаты могут использовать свои информационные ресурсы для вовлечения Китая, России и других крупных государств в диалог по вопросам безопасности и тем самым не дать им занять враждебную позицию. В то же время имеющееся у Америки информационное преимущество способно помешать уже занимающим враждебную позицию государствам, таким как Иран и Ирак, наращивать свою мощь. Более того, Америка способна помогать в развитии новых демократий и вступать в прямые контакты с теми, кто живет в условиях недемократических режимов. Это преимущество также важно с точки зрения усилий по предотвращению и разрешению региональных конфликтов, а также по решению проблем, связанных с крупными угрозами, который возникли после окончания холодной войны, такими как международная преступность, терроризм, распространение оружия массового уничтожения и глобальная экологическая деградация.

Электронный журнал ЮСИА. – 1996. – т. 1. – № 12 (сентябрь) – http://usinfo.state.gov/journals/itgic/0996/ijgr/gjcom6.htm

Между тем, существуют две концептуальные проблемы, которые мешают Соединенным Штатам реализовать свой потенциал. Первая состоит в том, что старое мышление не позволяет полностью оценить роль информации как силы. Традиционные мерки, такие как военная мощь, валовой национальный продукт, численность населения, энергетические ресурсы, размеры территории и наличие полезных ископаемых, по-прежнему доминируют в дискуссиях о балансе сил...

Вторая концептуальная проблема заключается в непонимании природы информации. Легко проследить и предсказать развитие возможностей по переработке и обмену информацией. Так, например, информационная революция явно находится на стадии развития, однако можно предвидеть, что уже на следующем этапе произойдет слияние ключевых технологий, таких как цифровая обработка данных, компьютеры, телефоны, телевидение и прецизионное глобальное позиционирование. Гораздо труднее понять последствия роста информационных возможностей, особенно последствия взаимодействий между ними. Информационное могущество трудно поддается определению, поскольку оно имеет отношение ко всем другим военным, экономическим, социальным и политическим возможностям, составляющим мощь государства и общества — иногда уменьшая эту мощь, а иногда многократно усиливая ее...

Военная сила и информация. Характер вооруженных сил США меняется, и, возможно, эти изменения происходят гораздо быстрее, чем думают многие, поскольку информационная революция влечет за собой революцию в военном деле. Источником этой революции, во главе которой стоит Америка, является развитие ряда технологий и — что еще более важно — способность сочетать все эти достижения и строить доктрины, стратегии и тактические варианты, основанные на их техническом потенциале.

Применяемое в вооруженных силах США сокращение ISR означает систему сбора разведывательных данных, наблюдения и разведки. Понятие C4I означает комплекс технологий и систем, обеспечивающих командование, управление, связь и компьютерную обработку данных. Наверное, наибольшую известность приобрели в этом смысле средства прецизионного ведения огня — благодаря видеосъемкам действия прецизионных боеприпасов в ходе операции "Буря в пустыне". Последние представляют собой более широкое понятие, чем думают многие, поскольку они являются элементом общей способности наносить поражающие удары с большой скоростью, на большом расстоянии и с предельной точностью.

Отчасти благодаря прошлым усилиям, отчасти в силу своей прозорливости, Соединенные Штаты являются лидером в этих областях по сравнению с другими странами, и ближайшее десятилетие будет двигаться вперед беспрецедентными темпами...

Вышеназванные технологии дают возможность собирать, сортировать, обрабатывать, передавать и демонстрировать информацию о самых сложных событиях, происходящих в крупных географических районах. Между тем, эта

возможность имеет важное значение не только для ведения войн. В быстро меняющемся мире информация о том, что происходит в этом мире, становится главным товаром в международных отношениях, подобно тому, как угроза применения и применение военной силы в свое время рассматривались как главный ресурс военной мощи в рамках международной системы, над которой как облако нависала потенциальная угроза столкновения между сверхдержавами.

Развитие информации носит взрывной характер. Между тем, определенные виды информации – точной, своевременной и понятной – ценится больше, чем другие. Выразительные видеокадры, показывающие руандийских беженцев, бегущих от ужасов межплеменной ненависти, могут вызвать сочувствие во всем мире и призывы к действиям. Однако, точное знание числа таких беженцев, а также того, куда, как и при в каких условиях они перемещаются, имеет критически важное значение для оказания им эффективной помощи.

Информация военного характера о дислокации, действиях и возможностях вооруженных сил по-прежнему имеет важное значение, поскольку вооруженные силы, как и прежде, рассматриваются в качестве окончательного арбитра при решении разного рода споров и разногласий. Более того, поведение государств по-прежнему в значительной степени определяется страхом перед применением к ним военной силы.

Растущая взаимозависимость мирового сообщества не обязательно ведет к развитию гармоничных отношений между его членами. Эта тенденция, однако, заставляет мировую общественность проявлять интерес к вооруженным силам конкретных стран. Прямое использование военной силы уже не вызывает призрак глобального ядерного Холокоста, однако, оно по-прежнему является дорогостоящим и опасным делом...

Концепция сдерживания, которая составляет основу нарождающейся американской "системы систем", предусматривает наличие вооруженных сил, обладающих достаточной мощью для того, чтобы нейтрализовать любые военные действия со стороны иностранного государства или государств и не идти при этом на соизмеримый военный риск или затраты. Те силы, которые подумывают о военном конфликте с Соединенными Штатами, должны будут отдавать себе отчет в том, что США обладают способностью остановить и обратить вспять любые враждебные действия с минимальной угрозой для собственных вооруженных сил...

Информационный зонтик. Информационные технологии, являющиеся движущей силой нарождающихся военных возможностей Америки, способны изменить классическую теорию сдерживания. Угроза применения военной силы не используется американцами автоматически или с готовностью, поскольку это всегда было сопряжено с нежелательными побочными эффектами. В эпоху, когда "мягкая сила" оказывает растущее влияние на международные дела, угрозы и имидж высокомерия и воинственности, который всегда

сопровождает их, наносят ущерб имиджу государства, строящего свою политику на принципах разумности, демократии и открытого диалога.

Нарождающиеся военные возможности Америки — в особенности те из них, которые обеспечивают гораздо более глубокий уровень понимания того, что происходит в крупном географическом районе в режиме реального времени — способны лишить это противоречие его прежней остроты. Эти возможности, например, обеспечивают гораздо большую степень транспарентности в преддверии кризиса. Если Соединенные Штаты хотят, чтобы эта транспарентность стала достоянием и других государств, им лучше иметь возможность создавать оппозиционные коалиции еще до того, как произойдет агрессия. Последствия этого могут носить более общий характер, поскольку все государства мирового сообщества сегодня действуют в неоднозначном мире, то есть в контексте не всегда благоприятной или спокойной обстановки.

На этом фоне нарождающиеся военные возможности Америки предполагают привлечение дружественных государств к тому, что в свое время обеспечивалось политикой расширенного ядерного сдерживания. Тогда ядерный зонтик предоставлял структуру для сотрудничества, связывая Соединенные Штаты на взаимовыгодной основе с широким кругом дружественных, союзнических и нейтральных государств. Это был логический ответ на центральную проблему международных отношений — угрозу советской агрессии. Сегодня же центральная проблема состоит в неоднозначности категорий и степени угроз, а основой сотрудничества является способность прояснять и устранять такую неоднозначность.

Набор неопределенных установок и интерпретаций, существовавших в годы холодной войны, сменился еще большей неоднозначностью отношения к международным событиям. Поскольку почти все государства рассматривали международную систему через призму холодной войны, они более или менее однозначно относились к происходящему в мире. Характер и сложность гражданской войны на Балканах имел бы гораздо меньшее значение для всех стран мирового сообщества, чем сам факт военного поворота событий в этом районе, поскольку такой поворот мог бы повлечь за собой военную конфронтацию между НАТО и Варшавским Договором. Подробности столкновений между китайскими и советскими пограничниками на самом деле не имели особого значения; главное состояло в том, что в одной из крупнейших коалиций мира наметилась трещина. Сегодня же как раз подробности происходящих событий приобретают решающее значение. В отсутствие организующих структур времен холодной войны, последствия становится все труднее классифицировать, при этом все страны хотят получать больше информации о том, что происходит в районе конфликта, стремясь понять, почему они должны помогать одной из противоборствующих сторон, какое это будет иметь для них значение и что они должны делать. Лидерство в коалициях в обозримом будущем будет основываться в меньшей степени на военных возможностях по уничтожению сил противника и в большей степени на способ-

ности оперативно прояснять неоднозначность ситуаций, связанных с насилием, гибко реагировать и при необходимости применять силу — точно и аккуратно.

Основа таких возможностей — наличие наиболее полной информации о происходящем в конкретной ситуации — не является чем-то неделимым. Соединенные Штаты могут передавать всю имеющуюся у них информацию или ее часть тем, кому они пожелают ее передать. Полученная таким способом информация даст возможность государству-реципиенту принимать более совершенное решение в этом несовершенном мире, и если это государство решит вступать в военные действия, оно будет способно достичь того же военного превосходства, что и Соединенные Штаты.

Таким образом, эти возможности влекут за собой появление того, что можно назвать информационным зонтиком. Подобно расширенному ядерному сдерживанию, они могут составить фундамент взаимовыгодных отношений. Соединенные Штаты будут предоставлять информацию о том, что происходит в конкретной ситуации, в частности, по вопросам, представляющим военный интерес для других стран. Другие страны более охотно будут идти на сотрудничество с Соединенными Штатами, поскольку могут получить от них информацию о конкретных событиях или кризисе.

Начало таким взаимоотношениям было положено в ходе фолклендского конфликта, и сегодня эти взаимоотношения развиваются на Балканах. В настоящее время Соединенные Штаты предоставляют основную массу данных, касающихся развития ситуации, силам по выполнению мирных соглашений, силам ООН по охране, государствам-членам НАТО и другим странам, которые непосредственно участвуют в разрешении этого конфликта или проявляют интерес к его разрешению. Вполне возможно, что подобным же образом центральная информационная роль будет принадлежать Соединенным Штатам и в других кризисах или при появлении угроз потенциальной конфронтации — примером может служить работа по выяснению обстановки на островах Спратли, или распутывание неразберихи в связи с гуманитарными операциями в Камбодже и Руанде. Получение точной информации о происходящем в режиме реального времени является ключевым моментом в достижении соглашений в рамках коалиций по вопросу о том, что именно должна делать та или иная коалиция, и имеет важнейшее значение с точки зрения применения вооруженных сил, вне зависимости от того, какая роль им отводится и какая миссия им поручается...

Все это касается предоставления США на выборочной основе другим странам имеющихся у них возможностей по сбору данных о боевой обстановке, комплекса данных, получаемых в результате применения так называемого комплекса C4I, и возможностей для нанесения прецизионных ударов. Люди со старым мышлением, наверное, содрогнулись бы от такой перспективы, и им пришлось бы преодолевать укоренившееся предубеждение против открытости и щедрости в предоставлении другим того, что в широком смысле мож-

но называть информацией разведывательного характера. В прошлом это предубеждение основывалось на двух соображениях: во-первых, тогда полагали, что предоставление слишком больших объемов разведданных ставит под угрозу распознавания и, возможно, даже утраты источников и методов получения таких данных, и во-вторых, что предоставление информации такого характера может выявить те сферы, о которых у Соединенных Штатов нет сведений, а это нанесет удар по репутации США как сверхдержавы.

Эти соображения сегодня вызывают еще больше вопросов, чем в прошлом. Соединенные Штаты уже не играют ва-банк, когда любое раскрытие возможностей становится потенциальным проигрышем для них и выигрышем для неумолимого противника. Характер этих постоянно совершенствующихся возможностей сегодня уже другой. Во-первых, Соединенные Штаты намного перегнали другие страны. Усилия, предпринимаемые США в области сбора разведданных, наблюдения и разведки – в частности, по линии космических систем – предпринимаются гораздо в большем объеме, чем всеми другими странами вместе взятыми, при этом Америка намного обгоняет другие страны с точки зрения C4I и возможностей по нанесению прецизионных ударов...

Некоторые страны способны догнать Соединенные Штаты на этом пути, однако, это произойдет не скоро. Эта революция происходит на основе технологий, которые являются достоянием всего мира. Переход на цифровые технологии, компьютерная обработка данных, прецизионное глобальное позиционирование и интеграция различных систем, то есть, технологическая база, на которой строятся все новые возможности, доступны любой стране, у которой есть деньги на эти цели и стремление к системному применению этих технологий в целях совершенствования военных возможностей. Работа с этими технологиями может быть связана с большими денежными затратами. Но что еще более важно, у всех этих стран нет конкретного стимула для построения систем, аналогичных той, которую строят для себя Соединенные Штаты – конечно, если эти страны не считают, что Соединенные Штаты представляют для них угрозу. Таким образом, имеются признаки грядущего симбиоза между государствами – вступление любого государства в гонку, связанную с информационной революцией, зависит от того, каким образом США используют свою лидирующую позицию. Если Америка не будет делиться с другими странами накопленным опытом и знаниями, то у этих стран появится стимул догонять Америку. Следовательно, выборочное предоставление другим государствам таких возможностей является для США не только способом утверждения себя в роли лидера в рамках различных коалиций, но и ключевым условием сохранения своего военного превосходства.

"Мягкая составляющая" информационной мощи. Один из иронических аспектов истории 20-го века состоит в том, что теоретики марксизма, а также его критики типа Джорджа Оруэлла, правильно заметили, что научно-

технический прогресс способен производить глубокие изменения в общественном и государственном строе, однако, и те, и другие имели неправильное представление о том, как именно это будет происходить. Оказалось, что технологические и экономические изменения в основном множат силы, способствующие формированию свободных рынков, а не репрессивные силы, способствующие укреплению централизованной власти.

Один из факторов, обусловивших огромные перемены в жизни Советского Союза состоял в том, что Михаил Горбачев и другие советские руководители понимали, что советская экономика не может перейти с экстенсивного или индустриального пути развития на интенсивную или постиндустриальную стадию развития, если не будут ослаблены ограничения на все технологии, начиная с компьютеров и кончая копировальными машинами типа "Ксерокс", которые могут применяться для распространения отличающихся друг от друга политических взглядов. Китай попытался воспротивиться этому веянию и запретил было использование аппаратов факсимильной связи, однако, эта попытка не увенчалась успехом. Сегодня в Китае полно не только факсов, но и тарелок спутниковой связи...

Этот новый политический и технологический ландшафт готов к тому, чтобы Соединенные Штаты с выгодой для себя использовали имеющиеся у них мощные инструменты так называемой "мягкой силы", то есть, более широко продемонстрировали другим странам привлекательность своих идеалов, идеологии, культуры, экономической модели, а также социальных и политических институтов, и обратит в свою пользу имеющиеся у них структуры для ведения международного бизнеса и телекоммуникационные сети...

В условиях нынешнего информационного разнообразия, те, кто отвечает за решение четырех важнейших задач, могут воспользоваться сравнительными преимуществами, которыми обладает Америка в области информации и ресурсов так называемой мягкой силы. Эти задачи состоят в следующем: оказание помощи оставшимся коммунистическим и авторитарным государствам в переходе к демократическому строю; предотвращение поворота назад в странах с молодой и хрупкой демократией; предупреждение и разрешение региональных конфликтов; противодействие угрозам, которые представляют собой терроризм, международная преступность, распространение оружия массового уничтожения и экологическая деградация в глобальном масштабе. Каждая из этих задач требует тесной координации между военным и дипломатическим компонентами американской внешней политики.

Контакты с недемократическими государствами и содействие в переходе к демократии. Холодную войну пережили многие недемократические режимы, в число которых входят не только коммунистические государства, такие как Китай и Куба, но и целый ряд стран, правительства которых не избирались, а формировались авторитарными или доминирующими социальными, этническими, религиозными или семейными кланами. Правительства некоторых таких стран предпринимают зловещие попытки заполучить ядерное

оружие, например, правительства Ливии, Ирана, Ирака и Северной Кореи. Политика США в отношении этих государств проводится в соответствии с конкретными обстоятельствами, в которых находятся эти страны, и их международным поведением. Соединенным Штатам следует и впредь на выборочной основе устанавливать и поддерживать контакты с такими странами, например, с Китаем, которые склонны к вступлению в международное сообщество, и одновременно предпринимать усилия для сдерживания режимов, таких как иракский, которые с этой точки зрения являются безнадежными. В попытках установить контакты с недемократическими режимами или изолировать их, Соединенные Штаты должны общаться с народами этих стран, информировать их о событиях, происходящих в мире, и помогать им готовиться к построению демократического рыночного общества, когда для этого возникнут условия.

Такие организации, как Информационное Агентство США, играют важнейшую роль, помогая другим государствам в переходе к демократическому строю. В этом смысле Китай являет собой наглядный пример. Радиостанция "Голос Америки", являющаяся рупором международного вещания ЮСИА, за последние несколько лет стала важнейшим источником новостей для 60 процентов образованных китайцев...

Защита новых демократий. Демократические государства возникли из коммунистического советского блока и авторитарных режимов в других регионах, таких как Латинская Америка, где впервые в истории во всех странах, кроме Кубы, действуют правительства, пришедшие к власти в результате выборов. Главная задача, которую ставят перед собой Соединенные Штаты, состоит в том, чтобы помешать возврату этих стран к принципам авторитаризма...

Важной программой в данной сфере является международная программа обучения и подготовки военнослужащих (ИМЕТ). В рамках ИМЕТ, созданной в 1950-х годах, свыше полумиллиона высших офицеров иностранных государств прошли военное обучение по американской методике и курс отношений между гражданскими и военными структурами в демократическом обществе. После окончания холодной войны эта программа была расширена, и в нее были включены вопросы, связанные с потребностями новых демократий, и сделан упор на подготовку гражданских служащих, на которых возлагается надзор за военными организациями и бюджетами.

Предупреждение и разрешение региональных конфликтов. Общинные конфликты или конфликты по поводу этнического, религиозного или национального суверенитета часто идут по пути эскалации в результате пропагандистских кампаний, проводимых демагогически настроенными лидерами, а особенно теми, кто стремится отвлечь внимание от собственных промахов и неудач, установить свой авторитет или захватить власть. Между тем, в развивающихся странах быстро развиваются телефонная связь, телевидение и

другие формы телекоммуникаций, давая возможность ЮСИА и другим агентствам проникать в информационное пространство этих стран и подрывать искусственную атмосферу непримиримости и единства, создаваемую этно-националистической пропагандой. Время от времени могут применяться военные технологии США для подавления или глушения радио- и телепередач, взывающих к насилию, а между тем, ЮСИА может обеспечивать беспристрастное освещение событий и выявлять ложную информацию и сообщения...

Заключение осенью прошлого года в Дейтоне, штат Огайо, мирного соглашения по Боснии стало иллюстрацией дипломатического измерения информационной силы. Соединенным Штатам удалось добиться соглашения, которого в течение нескольких лет не могли добиться на других переговорах, отчасти потому, что США обладают информационным превосходством. Способность наблюдать за действиями всех сторон в условиях конфликта помогла добиться уверенности в том, что соглашение будет поддаваться проверке, а подробные карты территории Боснии позволили уменьшить возможные разногласия.

Преступность, терроризм, распространение оружия массового уничтожения и Экология. Четвертая задача состоит в том, чтобы сфокусировать имеющиеся у США информационные технологии на проблемах международного терроризма, международной преступности, наркобизнеса, распространения оружия массового уничтожения и глобальных экологических проблемах. Директор ЦРУ Джон М. Дойч концентрирует усилия руководимого им ведомства на первых четырех из вышеперечисленных задач, в то время как новое управление глобальных проблем при Госдепартаменте берет на себя ведущую роль в изучении глобальных вопросов охраны окружающей среды. Информация всегда была лучшим средством предотвращения и предупреждения террористических актов; Соединенные Штаты могут использовать аналогичные возможности по изучению и обработке информации за границей, которые ФБР применяло внутри страны для поимки террористов, совершивших взрыв во Всемирном торговом центре.

Соединенные Штаты использовали свои информационные ресурсы для выявления программы по разработке ядерного оружия в Корее и для заключения подробного соглашения о ее ликвидации; для оперативного выявления и пресечения сотрудничества России и Китая с Ираном в ядерной области; для усиления возможностей ООН по инспектированию иракских ядерных объектов, а также для содействия в безопасном хранении запасов обогащенного урана на территории бывшего Советского Союза. Растущее число свидетельств экологических опасностей, таких как глобальное потепление и истощение озонового слоя, большая часть которых была добыта и распространена американскими учеными и государственными учреждениями США, помогает другим странам осознавать серьезность этих проблем и дает им возможность уже сегодня изыскивать экономически оправданные методы решения этих проблем...

Ожеван М.А.

ДВОГОСТРА ЗБРОЯ *

Мас-медіа часто називають сторожем демократії, Однак в епоху глобалізації інформаційні системи перетворюються ще й на небезпечну зброю, яку можна використовувати і з метою творення, і з метою руйнування

* За умов теперішньої розвиненості масових комунікацій у світі, що невпинно рухається до глобалізації, мас-медіа з їхніми можливостями впливу на масову ментальність і архетипи колективного несвідомого - це грізна зброя, яку можна обернути й на користь антитерористичним операціям.

Зловісна гра мас-медіа. Але з таким самим успіхом цю зброю можуть використати й терористи. Орієнтуючись на низькопробні смаки, мас-медіа, зазвичай, схильні не лише до всілякої "полуничкі", але й до демонстрації сцен терору з метою збільшення чисельності своєї аудиторії. Адже відповідно зростають і доходи від реклами. Один із західних фахівців з проблем медіа-тероризму, Тед Коппел, що представляє американську телекомпанію ABC, свого часу слушно зауважив: "Мас-медіа - особливо телебачення - й терористи, вступаючи у відносини спеціальної залежності, потребують один одного, між ними виникають відносини симбіозу. Без телебачення терорист уподібнився б до філософа, закинутого у лісові нетрі, до голосу якого ніхто не дослухається й докази якого ніким не почуті. Але й телебачення без показу актів терору...втратило б значною мірою інтерес аудиторії".

Реальність поза грою. Без сумніву, тут створюється певне замкнене коло, адже, демонструючи сцени ігрового чи реального терору, мас-медіа продукують "терористичну свідомість" з усіма наслідками так званого "секондного тероризму". Ця закономірність добре відома західним фахівцям зі спецслужб. Отже, виникає цілковито обґрунтована підозра, що саме ці фахівці часто-густо й диригують масовими кампаніями на захист "свободи мас-медіа у нових незалежних державах" від будь-яких спроб державного регулювання. Але чи усвідомлюють вони те, що, таким чином, свідомо сприяють деградації масової свідомості у "нових демократіях", це вже інше питання.

Тим часом, за умов низької платоспроможності населення та майже повної економічної залежності нових "демократичних мас-медіа" від іноземного й вітчизняного капіталу термін "свобода слова" звучить майже так само як "гарячий лід" (філологи називають такі словосполучення оксюморонами). Кампанії на захист "свободи мас-медіа" активно підтримують місцеві медіа-магнати, зацікавлені у зростанні доходів від реклами.

Засоби, перевірені кров'ю і часом. Особливим різновидом медіа-тероризму є відверта пропаганда. Ще в 1938 році у США вийшла друком серія книг, присвячена розвінчуванню прийомів політичної пропаганди. В одній з них було названо сім типових пропагандистських прийомів:

- називання речей "своїми іменами" (Name-Calling),

Журнал "Підприємництво в Україні". – 2001. – № 8 –
http://www.niisp.gov.ua/publication.php?razdel=info&doc=ozhevan2

- "блискучі узагальнення" (Glittering Generality),
- звертання до "заповітів предків" (Testimonial),
- звертання до "простих людей" (Plain Folks),
- "підвищування ставок" (Card Stacking),
- передача "важливих повідомлень" (Transfer),
- "гуркотливий віз" (Band Wagon).

До речі, це слово у вітчизняній літературі іноді звучить у позитивному сенсі, хоча у західній має однозначно негативне забарвлення й означає використовувати різні засоби впливу на масову свідомість з метою формування "фальшивих цінностей" (аттитюдів). З початком інформаційної революції можливості терористичних груп для пропагування своїх поглядів і маніпулювання масовою свідомістю значно зросли. У випадку медіа-інформаційного тероризму (МІТ) йдеться про різновид інформаційного тероризму (ІТ), що є "зловживанням інформаційними системами, мережами та їхніми компонентами для здійснення терористичних дій та акцій". ІТ характеризується як множина інформаційних війн та спецоперацій, пов'язаних з національними або транснаціональними кримінальними структурами й спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує ризики ІТ. Відповідно, що більш інформатизованим є суспільство, то воно є більш вразливіше до ризиків ІТ. Для України, де інформаційна діяльність поки що не набула належного розвитку, головні загрози у сфері ІТ є не внутрішніми, а зовнішніми. їх переважно створюють іноземні держави, міжнародні терористичні та інші злочинні угруповання й організації, які користуються нерозвиненістю й слабкістю відповідних державних структур.

Непрозорість або напівпрозорість -це так само зброя. Особливістю негативних інформаційних впливів разом з актами інформаційного терору є їхня непрозорість або напівпрозорість. Отже, вони можуть бути виявлені лише в результаті спеціальної експертизи. Щодо технологічного виміру ІТ, то він пов'язаний з хакерством та іншими видами "кіберзлочинності". Високий ступінь залежності України від імпортних комп'ютерів та інших інформаційних систем (з програмним забезпеченням включно) вже сьогодні створює додаткові ризики організованих хакерських атак, здатних, якщо не паралізувати, то, принаймні, серйозно пошкодити урядові, банківські, енергетичні, транспортні та інші інформаційно-комунікаційні мережі.

Медіа-тероризм або "медіа-кілерство" є особливим різновидом інформаційно-психологічного терору, що належить до так званого "інфраструктурного терору" й полягає у спробах шляхом організації спеціальних медіа-кампаній дестабілізувати суспільство, створити у ньому атмосферу громадянської непокори, недовіри суспільства до дій та намірів влади й особливо - її силових структур, покликаних захищати суспільний порядок. Для цього використовуються не лише друковані ЗМІ та мережі ефірних й кабельних мас-медіа, але й Інтернет, електронна пошта, різноманітні електронні іграшки, компакт-диски, аудіокасети тощо.

Україна як медіа-терористичний полігон. Організовуються й спеціальні деструктивні медіа-кампанії та спецоперації, спрямовані на поширення в "нових демократіях" дезінформації та дифамації, насаджування духу *ненависті та нетерпимості щодо певних суспільних груп* (етнічних, класових, конфесійних тощо). Досвід сусідніх країн свідчить про те, що такі кампанії разом з актами психологічного терору проти "чужинців" передували громадянським конфліктам та війнам. У 2000 році спроба організувати таку кампанію на тлі подій, пов'язаних з трагічною смертю композитора І.Білозіра, була здійснена у Львові.

Йдеться також про відверту медіа-пропаганду діяльності терористичних груп та політичних або релігійних екстремістів, які видають себе за "захисників свободи та незалежності", "справжніх патріотів", "невинних правдолюбців та шукачів істини" тощо. Японія, зокрема, стикнулася свого часу з такою пропагандою діяльності деструктивних культів типу "Аум сінрікьо". В Україні свого часу так само безкарно пропагувалося "Велике Біле Братство".

З виявами медіа-терору Україна стикнулася також під час так званого "касетного скандалу". І лише нестача медіа-ресурсів та відсутність в Україні "медіа-кілерів" високої кваліфікації (типу Сергія Доренка) завадила організаторам цієї акції досягти своєї мети - ліквідувати інститут президентства.

Мас-медіа використовуються, насамперед, з метою психологічної обробки масової свідомості для ліквідації "імунних бар'єрів" самозбереження та самозахисту, ігнорування елементарними правилами особистої та громадської безпеки, насаджування відчуття приреченості тощо. Для цього використовуються прийоми зняття природжених табу та естетизація психопатичної поведінки та різноманітних збочень включно із вбивствами та фізичним і психологічним насильством (після того як в американських школах почастішали акти насильства і вбивств спеціальною комісією Конгресу США було проведено експертизу різноманітних "трилерів", яка виявила, що серед героїв цих фільмів приблизно однакова кількість "хороших" й "поганих" хлопців, так само як і сцен психологічного терору й фізичного терору), героїзація криміналітету й, навпаки, - дегероїзація працівників спецслужб, правоохоронних органів, ветеранів війн та праці тощо. У цьому розумінні медіа-тероризм часто передує актам "матеріального" тероризму.

Гротескно-спотворений імідж України. Особливу увагу слід звернути на формування позитивного "антитерористичного" іміджу України як суспільства і держави у західних мас-медіа, оскільки останнім часом вони систематично насаджують гротескно-спотворений імідж України як країни, що нібито надає притулок терористичним групам, продає зброю "проблемним" країнам, які підтримують тероризм.

Україну постійно й на всіх рівнях репрезентують як наскрізь корумповану й криміналізовану державу, в якій масово поширюються ВІЛ-інфекція та наркоманія тощо. При чому, більшість негативних сюжетів західних мас-медіа з "мазохістською завзятістю" підхоплюють вітчизняні медіа. Часто вони й

самі "підкидають" такі сюжети Заходові. ГПрикладом цього є дезінформація напередодні "атак на Америку" (отримана буцімто каналами СБУ й згодом спростована СБУ) щодо діяльності в Україні близько десяти іноземних терористичних центрів. Що ж до системи контр-пропаганди, то вона, попри усі розмови про її необхідність, в Україні фактично відсутня.

Держкомтелерадіо України та відповідний парламентський комітет обмежуються переважно розмовами про "свободу слова" замість того, щоб вжити заходів щодо активного державно-правового регулювання інформаційними процесами й відвернення інформаційних загроз, приведення національного інформаційного законодавства у відповідність з нормами міжнародного права за умов одночасного захисту національних інтересів в інформаційній сфері.

Довгі язики кораблі топлять. Після терористичних атак на Америку офіційні особи дедалі частіше накладають обмеження на діяльність не-залежних мас-медіа та аналітичних центрів, що намагаються виступати з критикою діяльності уряду та спецслужб. Такі публікації розглядають як "непатріотичні" й загрозливі для національної безпеки. В одному з офіційних виступів критиці було піддано журналістів, які надто прискіпливо з'ясовували маршрути пересування Президента й віце-президента трагічного дня 11 вересня. В іншому, - те, що журналісти почали писати про нібито неактуальну сьогодні для США загрозу "біологічного тероризму", підсилюючи, таким чином, настрої розгубленості й непевності.

Як визнав 18 вересня один з оглядачів американської телекомпанії MBC, старший віце-президент цієї компанії Білл Уітлі (Bill Wheatley) розіслав усім журналістам цієї компанії з відділу новин попередження часів Пірл-Харбору про те, що "довгі язики топлять кораблі" (Loose lips sink ships"), майже аналогічне вітчизняному крилатому вислову часів тієї ж II Світової війни - "базіка — знахідка для шпигуна". При цьому у листі зазначалося: "На цей момент ми маємо бути дуже обережними з тим, про що повідомляємо. Майте на увазі, що поширювана нами інформація може бути використана як тими зловмисниками, які розробляють плани нападів на наших співвітчизників, так і нашими урядовцями й нашими військовими. Тому будьте обережними, повідомляючи про маршрути пересування Президента або розпорядження щодо заходів безпеки, таємні військові плани, маневри військ тощо". Керівник американської телекомпанії зазначав при цьому, що розуміє, наскільки важко дотримуватися цих обмежень, але висловив сподівання, що журналісти не допустяться помилок і "не опиняться на боці загроз" (should "егг оп the side of caution").

По суті все це є закликом до самоцензури. Але, не має жодного сумніву, стосовно "нерозуміючих" журналістів діятиме й "зовнішня цензура". Принаймні, це стає зрозумілим кожному відвідувачу американських сайтів, найбільш цікавих з точки зору отримання "стратегічної інформації". На час підготовки "антитерористичної операції" вони раптом без будь-якої на те при-

чини перестали "завантажуватися". А в публікаціях американських масових газет побільшало "води" і поменшало гострих оцінок, коментарів тощо. Натомість зустрічаються майже тотожні метафори й психосемантичні звороти і навіть одні й ті ж самі фотографії, покликані пробуджувати "національний дух" та почуття солідарності.

Не варто поспішати з осудом подібної цензури як "наступу на свободу слова". Адже не таємниця, що зовнішньо-політичні акції і внутрішня ситуація в країні - це речі тісно взаємопов'язані. Терористи завжди належать до певної спільноти й насамперед - етнічної. Отже, ненависть до них, посіяна мас-медіа, буде неодмінно переноситися на всіх без винятку представників цієї спільноти. Не випадково у США (не без впливу мас-медіа) після атак 11 вересня слово "араб" у масовій свідомості почало сприйматися майже тотожним до слова "терорист", що стало причиною нападів на безневинних людей.

Негативні конотації не поліпшать ситуації. Нібито й не погоджуючись з ототожненням усіх "арабів" з "терористами", популярний польський тижневик "Впрост" розвивав в одній із публікацій ксенофобні за своїм спрямуванням ідеї, відштовхуючись від історії ісламських завоювань у Європі, які нібито остаточно зупинив польський король Ян Собеський. Крім того, автор публікації підкреслював, що супроти арабських терористів усі інші - все одно, що "коти проти тигра". До речі, на долю "котів з ЕТА", які розпочали свої терористичні акції з 1968 року, припадає 800 невинних жертв.

На час "кризового менеджменту", коли вступає в дію старе правило про те, що "слово - не горобець", потрібні не лише цензурні обмеження щодо мас-медіа. Такі ж самі обмеження досвідчені журналісти мали б накладати на метафори й словосполучення, які потрапляють до офіційних документів та промов офіційних осіб. Адже хто, як не журналісти та фахівці з медіа-політики, знають про психосемантичний вплив на масову свідомість різних словосполучень і термінів. Йдеться, передовсім про представників таких професій, яких на Заході називають "спічрайтерами" та "споуксменами (споуксвуменами)". Зокрема, у США після 11 вересня неадекватну лексику стали застосовувати не лише мас-медіа, але й Президент та інші представники Білого Дому, що вживали спочатку не зовсім вдалу термінологію для означення джерел тероризму та мети антитерористичної операції. Ще тоді, коли невидимого ворога виразно й реалістично не було ідентифіковано, розпочалися заклики до "аморфного" "хрестового походу" (crusade).

Зокрема, репутацію "яструба" не-безпідставно заслужив заступник міністра оборони США Пол Вольфовіц, який у перші ж години після терористичної атаки на США вдався до дипломатичного методу, що зветься "розвідкою боєм" ("cautious approach"). Він закликав тоді відразу вдарити по усіх "країнах, які надають притулок терористам" ("states that harbour terrorist networks"), хоча й обмовився при цьому, що не має на увазі самі лише військові дії. У його виступах згадувалося майже 60 країн. Таким же невдалим виявився в устах секретаря Держдепартаменту Коліна Пауелла термін "теро-

ристичні держави" ("terror states). У свою чергу, в лексиконі і Президента США, і інших високоповажних урядовців переважали фрази типу "глобальне зло тероризму" тощо. Коли йдеться про таке безлике зло і "хрестовий похід", то виникають, звичайно, негативні історичні конотації стосовно ісламського світу загалом.

Хоча такі терміни були "емоційно задовільними", але вони порушили правило об'єктивності та більшість фундаментальних правил зовнішньої політики. Якщо держсекретаря США розуміти буквально, то може здатися, що США негайно оголосять війну, принаймні, семи державам, які ще в квітні 2001 року потрапили до офіційного списку Державного департаменту як "terror states" (Куба, Іран, Ірак, Сирія, Північна Корея, Лівія і Судан). Але зрозуміло, що навіть США не під силу воювати з усіма цими країнами водночас і, що це було б початком III Світової війни. Не випадково після таких заяв, багаторазово підсилених мас-медіа, у США розпочалася легка паніка й люди стали скуповувати харчі й товари першої необхідності.

До того ж, цей список Держдепартаменту був далеко неповним і навіть курйозним. До нього, зокрема, не потрапив Афганістан, оскільки США не встановили дипломатичних відносин з режимом талібів і для них такої держави як Афганістан нібито взагалі не існує. Не потрапили до цього "чорного списку" й інші країни, які, хоча й надають притулок терористам, але офіційно вважаються "друзями Америки" - Саудівська Аравія, Пакистан, Колумбія тощо.

Крім того, якщо вже бути логічним, то список Держдепартаменту слід було б поповнити усіма країнами, де діють терористичні організації. І тоді до нього потраплять Ірландія, Іспанія, Шрі Ланка і т. д. (тобто виявиться, що "вороги Америки" є всюди). Але, якщо називати речі "своїми іменами", то виявиться, що офіційні діячі з Вашингтону, що нібито намагаються побороти "глобальне зло тероризму", насправді мають на увазі лише "ісламський тероризм". Але і в цьому разі, за законами кризового менеджменту слід виставляти певні "рамкові умови" й переконувати чисельні ісламські держави й організації, що "священна війна" ("holy war"), не спрямована проти них. Отже, і мас-медіа, і урядовцям слід відкинути зайву риторику й сфокусувати зусилля на реальних речах.

Коли Америка вступила у другу світову війну, вона оголосила її двом конкретним країнам - Японії і Німеччині, а не "диктаторам усього світу". Америка не декларувала тоді війну "фашизму", не воювала з іспанцем Франсіско Франко або аргентинцем Хуаном Пероном тощо. Що ж до СРСР, то "неакуратна лексика" радянських діячів та підконтрольних їм мас-медіа призвела, як відомо, до того, що навіть невгодний Йосифу Сталіну югославський лідер Йосип Броз Тіто на якийсь час отримав титул "фашиста". Звичайно, баланс порозуміння між представниками владних структур та мас-медіа завжди є досить хистким і тут доводиться постійно вибирати між правом громадськості на поінформованість та інтересами національної безпеки

("Security vs. need-to-know"). На час військових дій і терористичних атак цей баланс стає ще більш непевним. Особливо, коли йдеться про невизначені фронти терористичних загроз, яких невідомо звідки й від кого чекати. Тобто позиції урядовців і представників спецслужб зрозуміти не так вже й важко. Але й вони мусять зрозуміти, що без мас-медіа громадськість нічого не знатиме про характер загроз, запобіжні заходи, першочергові дії в екстремальних ситуаціях тощо.

Журналістська виваженість як індикатор здорового суспільства. Зрештою, традиційну роль "сторожової собаки" ("watchdog") журналістика покликана виконувати за будь-яких умов, якщо суспільство визнає себе демократичним.

Однак слід визнати також і ті обмеження, які необхідні в екстремальних умовах. Якщо інформаційні продукти ЗМІ поділити на журналістику "фактів" і оцінок", то очевидно "фактів" за умов загрозливої ситуації має побільшати, а "оцінок" поменшати. Тобто, суб'єктивні оцінки журналіста мають "ховатися у тінь" офіційних оцінок ситуації. Інакше, на суспільну свідомість чекає майже цілковита дезорієнтація. Не кажу вже про те, що частина журналістів замість виваженості даватиме суто емоційні оцінки, сіючи, таким чином, зерна страху, розгубленості й паніки. А це якраз те, чого добиваються будь-які терористи і чого організоване суспільство, готове дати рішучу відсіч терористичним атакам, аж ніяк не може собі дозволити. Звідси - необхідність цензури й самоцензури, які мас-медіа, на жаль, сприймають дуже болісно.

Ожеван М.А.

ФРОНТИ Й ТИЛИ ВЕЛИКИХ ІНФОРМАЦІЙНИХ ВІЙН *

У недорозвиненості інформаційної сфери криється вкрай серйозна небезпека підриву національної безпеки нашої країни. І перестануть журналістські пера бути іграшкою для маніпуляцій та розпалювання інформаційних війн?!

Інформаційне суспільство, до якого, принаймні, декларативно, але так палко прагне увійти Україна, має глобальний характер. І він полягає насамперед у просуванні до глобальної "інтелектуальної економіки", в системі якої нівелюватимуться всі географічні межі ринків збуту. Натомість з'являтимуться розподілені мережеві трудові ресурси, кардинально зблизяться виробництво й споживання, зростатимуть роль та значимість транснаціональних компаній, загостриться боротьба за обмежені сировинні ресурси і за такий специфічний ресурс, як людські мізки або людський капітал.

Вторинний ринок інформації: велетень на карликових ногах. На Заході з'явився новий фах - "хіт-хантер" ("мисливець за людьми"). Йдеться про активне імпортування з-за кордону спеціалістів з програмування. Розви-

Журнал "Підприємництво в Україні". – 2001. – № 4-5. – http://www.niisp.gov.ua/publication.php?razdel=info&doc=ozhevan1

вається й ринок так званого офшорного програмування, на якому минулого року Індія, до речі, заробила 4 млрд. доларів.

В інформаційному суспільстві неодмінно з'являтимуться нові нетрадиційні ринки інтелектуального споживання. А це означає, що більша частина "доданої вартості" концентруватиметься саме у сфері "м'яких технологій". Звісно, це призведе до докорінних зрушень у суспільному житті. Адже, щоб забезпечити лише 1% економічного зростання, Україні вже сьогодні потрібно на 3% зміцнити свою індустрію телекомунікацій. Отже, у розвиток цієї галузі упродовж найближчих п'яти років слід буде вкласти щонайменше 5-7 млрд. доларів.

Не розв'язавши цих інфаструктурних проблем, годі сподіватися на стійке економічне зростання. Тим часом, покладатися в цьому, очевидно, можна лише на іноземного інвестора, бо кошти, які вкладає держава, просто неспівмірні з необхідними потребами. Упродовж 1998-99 років було повністю відсутнє бюджетне фінансування Національної програми інформатизації. Упродовж 2000 р. на це було виділено 5 млн. грн., а у 2001 р. - 8 млн. грн. Тобто ми вкладаємо на державному рівні в інформаційну сферу лише одну тисячну частину від належного.

Як відомо, українські мас-медіа використовують переважно інформацію не оригінального походження, а запозичену з іноземних, переважно російських джерел. Замість того, щоб пропонувати ближнім і далеким сусідам свою власну. Тут не обійтися лише нарощенням кількості інформаційних агенцій та їхніх представництв у різних куточках світу. Слід навчитися працювати за законами світового ринку інформації:

- інформація мусить бути вірогідною, оригінальною, ексклюзивною;
- її слід "запакувати" за звичними для зарубіжного споживача стандартами і подати в технологічно придатному вигляді;
- вона має бути адекватно і якісно перекладена іноземними мовами;
- іноземний споживач має довіряти українським Інформаційним джерелам і на основі такої інформації приймати свої рішення.

На жаль, цього ще й досі немає. І це вкрай негативно впливає на міжнародний імідж України, яку на Заході за інерцією все ще сприймають як "ту ж саму Росію, але більш зіпсовану". Так званий касетний скандал, до речі, ще більше посилив цю хибну переконаність західної громадськості. Що й казати, навіть на внутрішньому інформаційному ринку ми часто віддаємо перевагу інформації, здобутій із зовнішніх джерел, адже свої внутрішні підкидають нам не стільки інформацію, скільки дезінформацію. Тож доводиться постійно витрачати енергію на те, щоб відокремлювати зерно від полови. Але природа інформаційного простору така, що він ніколи не буває порожнім. Там, де не дотягують національні виробники інформаційного продукту, замість них допрацьовують іноземні. І було б наївно гадати, що вони завжди працюють лише на користь наших національних інтересів.

Суб'єкти інформаційного простору: засилля інформації ненаціонального походження. Державні ЗМІ через низьку якість пропонованого ними про-

дукту дедалі більше втрачають свою популярність. Тож близько 80% ефірного часу телерадіотрансляцій вже заповнено продуктом неукраїнського походження. Кабельними мережами поширюються сигнали провідних російських телекомпаній (ОРТ, РТР, НТВ), програми яких часто-густо мають виразно антиукраїнську (в ліпшому разі - неукраїнську) спрямованість.

За соціологічними даними, серед українських телеканалів кияни віддають перевагу "Інтеру" (82%) й "1+1" (77%). Високим є також рейтинг "Нового каналу" (49%), що навіть перевищує рейтинги російських РТР та НТВ. З програм новин популярними є "Подробности-Время" на "Інтері" і ТСН на каналі "1+1". А от респондентів, які віддавали перевагу "Вікнам" на СТБ, виявилося стільки, скільки й прихильників "Сегодня" на НТВ або "Вестей" на РТР. Найнижчі за рейтингом позиції офіційного каналу УТ-1 (40%) та каналу ТЕТ (26%). Ті самі канали мають і найнижчі рівні довіри. Зменшилася популярність державних радіостанцій за винятком офіційної першої програми українського радіо, яка збирає більшу аудиторію, ніж інші довгохвильові радіостанції. Їхній невисокий рейтинг коливається в межах 1-3%. Головна причина такого стану - застаріла концепція радіоканалів, які не витримують конкуренції з комерційними FM- станціями музичних форматів. При цьому не слід забувати, що для FM-аудиторії, переважну частину якої складає молодь, інформаційні блоки цих станцій є головним джерелом новин.

Російські бізнес-структури активно скуповують акції провідних українських телеканалів: 82% акцій СТБ контролюється "Лукойлом", 30% "Інтеру" належить ОРТ. Російськими власниками контролюється телекомпанія "НАРТ". Значна частина власності "Нового каналу" належить російській "Альфа-групі". "1+1" контролюється американською фірмою СМЕ (Р.Лаудер). Іноземні компанії контролюють близько 80% рекламного ринку в інформаційному просторі України. До того ж, український медіапростір активно "обстрілюється" як з територій суміжних держав, так і з використанням супутникового мовлення. У західному регіоні України активно діють польські ("TV-Polonia", RFM тощо), угорські (Duna-TV) телерадіокомпанії. На території України здійснюють своє мовлення "Радіо Свобода" (США), ВВС (Великобританія), DW (ФРН).

Активну діяльність розгорнула фірма "Гарант", яка, надаючи документи на ексклюзивні права щодо розповсюдження в Україні програм російського каналу "НТВ", прагне підпорядкувати собі компанії кабельного телебачення. Водночас Всесвітня служба радіомовлення України здійснює трансляцію програм лише трьома іноземними мовами - англійською, німецькою та румунською. Через постійну нестачу фінансування зменшуються обсяги мовлення. Більше того, через вимкнення передавачів Львівського ОРТПЦ та дворічного простою Миколаївського РПЦ зупинено трансляцію програм на Північну й Південну Америку, Австралію.

Великі інформаційні війни: коли гуркотять гармати, пера притуплюються. В Україні простежується тенденція до концентрації та монополізації

ЗМІ. Формуються потужні холдинги, які стають для фінансово-політичних угруповань специфічними інструментами політичного впливу. Простежуються тенденції відтворення на нашому грунті російської моделі медіа-холдингів, функціонування яких призвело до формування джерела політичної нестабільності внаслідок постійних "інформаційних війн". Подібним структурам властиве нехтування національними інтересами на користь власних корисливих інтересів, ледь завуальованих ідеалами боротьби за свободу слова. Все це складає постійну загрозу національній безпеці.

З одного боку, часто наражаються на невдачу спроби журналістів отримати більш-менш об'єктивну інформацію про перебіг соціально-політичних процесів в Україні, намірів та дій влади. І причина тут, звісно, не в журналістах, а в самих державних "достойниках", яким слід, нарешті, визначитися, хто і що вповноважений компетентно стверджувати у кожному конкретному випадку. Необхідно сформувати певні ієрархічні правила й поінформувати про них ЗМІ, що дасть змогу зняти, якщо не всі, то більшість проблем довкола забезпечення свободи слова в Україні.

З іншого боку, самим журналістам слід опрацювати і включити до свого морально-етичного професійного кодексу певні правила висвітлення діяльності владних органів. Критикувати певні персоналії, звичайно, можна і потрібно. Але справою вкрай негідною і, врешті-решт, непрофесійною є спроби атакувати цілі державні інституції лише тому, що їх представляють не ті люди, яких хотілось б бачити на відповідних посадах авторам так званих компроматних інформаційних матеріалів та замовникам цих матеріалів. Тут існує та морально-етична межа, яку за жодних умов не варто переходити журналісту, що справді поважає свою професію. І чим швидше це зрозуміють окремі журналісти і цілі журналістські колективи, тим конструктивніше у них складатимуться стосунки не лише з владою, але й з власними читачами, глядачами та слухачами. Тим вищим буде ступінь довіри до мас-медіа.

Кадри і зарплата: закон тотожності. Загалом, вкрай актуальною є проблема підготовки журналістських кадрів, переважна більшість яких працює на досить низькому професійному й творчому рівні. Так само актуальною є проблема й підготовки кадрів для пресових та PR-служб, які могли би компетентно представляти органи державної влади і державу в цілому. До внутрішніх проблем журналістського середовища слід віднести також небажання журналістів займатися досудовим, корпоративним розглядом конфліктів на "судах журналістської честі".

Суттєвою є також проблема підготовки кадрів технічних фахівців на рівні сучасних інформаційних технологій, адже поки що немає достатнього бюджетного фінансування цього освітнього процесу. Розвиток відповідних технологій та технологічне оновлення основних фондів державних каналів радіо та телебачення, на жаль, входять до тих питань, які не мають належного відображення в бюджеті 2001 р. До того ж однією з найболючіших проблем є перетікання за кордон кваліфікованих кадрів, оскільки умови оплати праці

за кордоном і в самій Україні поки що несумірні. Ця проблема стосується, серед іншого, й представництва органів державної влади в Інтернеті. Адже, щоб виготовити професійний сайт та підтримувати його на належному рівні необхідні фахові системні адміністратори, web-дизайнери, залучати яких за теперішнього низького рівня зарплати в державно-бюджетній сфері вкрай проблемно. Більше того, значна кількість комп'ютерних спеціалізацій й досі не входять до загальнодержавного реєстру професій.

Надзвичайно гострими є бюджетні проблеми державного концерну РРТ. Низькі ставки посадових окладів працівників державних радіо-телеканалів - як технічних, так і творчих, - низькі доходи районних та міських газет ставлять, у свою чергу, під загрозу нормальне пенсійне забезпечення журналістів.

Виходом з цієї ситуації може стати укладання державних угод між замовником та видавцем з виплатою замовником стартової суми, що забезпечить гарантований доход даного виду ЗМІ. Існує також проблема державного замовлення для ЗМІ та чіткого термінологічного визначення цього поняття. Внаслідок недостатньої уваги до кадрів творчих та технічних працівників та їх матеріального забезпечення досить низьким є загальноестетичний, творчий та інтелектуальний рівень газетних статей, радіо- і телепередач.

Загальні інформаційні потреби та інтереси. До цього ж долучаються також постійні порушення ЗМІ взятих на себе нормативно-правових зобов'язань. Лише одиниці з тих близько 900 телерадіоорганізацій, які отримали ліцензії, дотримуються своїх ліцензійних програмних зобов'язань. Через це ефір переповнюється зразками примітивної зарубіжної масової культури. Так само відбувається суто стихійний, без належного нормативно-правового регулювання, розвиток кабельного телебачення та сучасних цифрових технологій мовлення. На тлі занепаду електронної промисловості (зокрема, зі створенням сучасних цифрових приймачів) та відсутності науково-дослідницької підтримки телерадіоінформаційної галузі теперішня ситуація є досить тривожною і складає безпосередню загрозу інформаційній безпеці України.

Якщо абстрагуватися від приватних інтересів окремих державних службовців та публічних політиків і зосередитися на загальнодержавних інформаційних потребах та інтересах, то вони зводяться, власне, до чотирьох позицій, які і стають предметом постійного діалогу влади через мас-медіа з громадськістю:

- отримання вірогідної, оперативної та якісної інформації, придатної для підготовки та прийняття керівних і управлінських рішень;
- проведення масштабних обговорень в мас-медіа досить дискусійних неоднозначних державних рішень;
- оперативне донесення інформації про прийняті рішення до об'єктів керування й управління;
- проведення масштабних медіа-кампаній з метою мобілізації як вітчизняної, так і міжнародної громадської думки з метою реалізації прийнятих рішень.

Власне, до зазначених позицій і лежать ключові питання забезпечення ефективної державної медіа-політики та ефективного медіа-супроводу загальнодержавних акцій.

Влада і мас-медіа: тернистий шлях до діалогу. Особливо актуальною є проблема діалогу влади зі ЗМІ під час спілкування журналістів з регіональними органами державної влади. Склалося так, що для представників ЗМІ значно складніше отримати інформацію від губернатора чи його заступників, аніж від міністра чи іншого представника центральних органів влади. Інакшими словами, влада на місцях, зазвичай, не звикла рахуватися з "четвертою владою", є менш демократичною, значно закритішою і менш налаштованою на зворотні зв'язки за посередництвом ЗМІ з громадянами. Є навіть приклади відвертої грубості, яку дозволяють собі деякі можновладці на місцях.

Певна опозиційність засобів масової інформації до чинної влади є явищем нормальним і притаманним усім демократичним країнам. Але, щоб конструктивно опонувати владним структурам, ЗМІ мають бути економічно самодостатніми і в цьому розумінні незалежними й автономними. Нині ж вони зазвичай залежні від певних олігархічних кланів, що зловживають свободою слова і часто використовують її для ведення інформаційних війн проти своїх конкурентів, викиду компромату тощо.

В свою чергу, для вирішення економічних проблем мас-медіа потрібні:

- суттєве зростання платоспроможного попиту населення на інформаційний продукт і зниження собівартості самого інформаційного продукту;
- формування інформаційних потреб та запитів, а на засадах їх розширення і якісного оновлення - інформаційного ринку та його невід'ємної складової - рекламного ринку. Певною загрозою для інформаційної безпеки України є інтенсивне проникнення на внутрішній інформаційний ринок іноземного інформаційного продукту, що ставить вітчизняного виробника цього продукту в нерівні умови конкуренції, а українське суспільство в умови постійної інформаційної, духовної та культурної залежності. В українських виробників інформації зникають стимули для створення власного інформаційного продукту.

Сюди ж слід віднести й проблеми поширення як в Україні, так і за її межами тиражованої в Україні так званої піратської продукції. Виникла цілком реальна і вкрай небезпечна в епоху інформаційної революції загроза втрати вже в найближчій перспективі творчих людей, здатних до виготовлення національного інтелектуального продукту. Адже пригодований інформаційним "секендом", наш споживач масової інформації може взагалі знехтувати інформаційним продуктом, маркованим позначкою "Мейд ін Юкрейн".

Попри певні позитивні зрушення в розвитку національного інформаційного простору та нормативно-правового забезпечення інформаційних відносин, загальна ситуація поки що не від-повідає сучасним вимогам, інтересам суспільства і держави. А головні загрози національній безпеці України в

інформаційній сфері загалом залишаються неподоланими. Про це, зокрема, свідчать технічне і технологічне відставання електронних ЗМІ, кризовий стан (фізична зношеність і моральна застарілість) інфраструктури вітчизняного телерадіомовлення, діючих мереж і парку технічних засобів, які практично не оновлювались ще від 80-х років.

Водночас, чимало норм, закладених в українському законодавстві щодо ЗМІ, наприклад, та, що обмежує іноземні інвестиції у статутний фонд телерадіокомпаній та друкованих ЗМІ лише 30 відсотками, виглядають, принаймні, наївними, якщо не шкідливими. Адже за фактичної відсутності внутрішніх інвестицій обмежувати приплив інвестицій зовнішніх вкрай нерозумно.

Україна має навчитися своєчасно реагувати на виклики інформаційної революції, зважаючи також на національні інтереси й проблеми власної національної безпеки. Наша країна поки що не втратила шанс, сконцентрувавши державну та недержавну політику на ключових галузях інформаційних технологій, скоротити відставання від розвинених країн. Але для цього слід активно прискорити випуск та споживання такого специфічного національного продукту як інформація.

Панарин И.Н.
КОНДОЛИЗА РАЙС: ДИПЛОМАТИЯ ИНФОРМАЦИОННОЙ ЭКСПАНСИИ*

Кондолиза Райс утверждена на должность главы внешнеполитического ведомства страны. В структуре власти США госсекретарь занимает ключевую позицию. Это серьезный игрок, к мнению которого зачастую прислушиваются больше, нежели к мнению президента.

26 января все узнали результаты многочасового обсуждения достоинств бывшего советника президента по национальной безопасности. 85-13 - таков итог голосования. При всей внешней внушительности этой победы стоит учесть, что только у одного госсекретаря США рейтинг сенатского одобрения был еще ниже: в 1825 году против кандидатуры Генри Клея высказалось 14 заседателей верхней палаты Конгресса.

Она стала первой афроамериканкой, занявшей пост госсекретаря США. В половой категории ее обошла чешская еврейка Мадлен Олбрайт. Достижение, тем не менее, значительное, если вспомнить, что детство госпожи Райс, прошедшее на родине Форреста Гампа, в Алабаме, где для граждан США ее расы были специальные магазины и посадочные места в автобусах, явно не сулило ей таких умопомрачительных перспектив.

Что касается прогнозов о деятельности нового госсекретаря, то ответ здесь очевиден и отчасти содержится в речи самой Райс, которую она произ-

несла перед утомленными дебатами сенаторами. Будучи всегда последовательным сторонником "силовой " политики экспансии Буша, она останется им и впредь. Даже после того, как США и мировым сообществом было официально признано, что в Ираке не было оружия массового поражения, а значит и не было никакого повода для оккупации государства –члена ООН, Райс не нашла в себе силы признать неверность своих оценок. То есть она не хочет и не будет признавать ни своих ошибок, ни ошибок во внешнеполитической стратегии США.

Весь мир вскоре станет свидетелем появления нового вида дипломатии – дипломатии информационной экспансии, в интересах мирового экспорта свободы по-американски. Эта дипломатия будет бескомпромиссной, в стиле идей И.Сталина, высказанных Дж.Бушем в сентябре 2001 года – "Кто не с нами, тот против нас".

Новый Государственный секретарь Кондолиза Райс заявила 27 января 2005 года сотрудникам Госдепартамента о своем намерении энергично осуществлять намеченную Президентом Бушем новую Доктрину –доктрину экспансии свободы по-американски.

Некоторые выдержки ее выступления.

- Дипломатия будет столь важна для упрочения завоеваний последних четырех лет и для энергичного осуществления повестки дня более свободного и благополучного мира.
- Не могу себе представить лучший призыв, чем сказать, что Америка будет отстаивать свободу, что Америка будет поддерживать тех, кто хочет осуществить свое стремление к свободе. И я, и Президент будем рассчитывать на то, что Государственный департамент возглавит эту работу. Нам надо не просто проводить политику, нам понадобятся идеи, интеллектуальный капитал.
- Поймите, что сейчас такое время, когда нас призывает история. И я рассчитываю работать с каждым из вас для достижения этой цели.
- Хочу, чтобы вы также знали: я буду твердо настроена добиваться того, чтобы у нас были инструменты, необходимые нам для осуществления этой повестки дня. Я верю в обучение и верю в образование, непрерывное образование в дипломатическом корпусе.
- Знаю, кое-кто сомневается, может ли демократия закрепиться на каменистой почве Западного берега, или в Ираке, или в Афганистане. Я считаю, что мы, как американцы, знающие, как труден путь к демократии, должны в это верить. И мы должны сделать так, чтобы мы работали с теми, кто хочет реализовать эти устремления.

Каковы же "инструменты", необходимые для осуществления новой Доктрины Буша?

США намерены активизировать работу в области "публичной дипломатии" и информационной деятельности за рубежом. Об этом заявила Кондоли-

за Райс в сенатском комитете по иностранным делам на слушаниях по утверждению ее кандидатуры на пост госсекретаря США. Предполагается увеличить финансовые расходы на внешнеполитическую пропаганду на 20%.

К.Райс определила и главные объекты массированного информационно-психологического воздействия. Это страны СНГ и Ближнего Востока.

Она подчеркнула, что в качестве главы американского внешнеполитического ведомства намерена тесно взаимодействовать с входящим в структуру правительства США.

Советом по иновещанию, отвечающим за радио и телевизионное вещание на зарубежные страны. А на просторах СНГ вслед за Грузией и Украиной готовятся новые "разноцветные демократические" революции. Сначала Киргизия и Молдавия, затем Казахстан, а потом и Россия. Таким образом, информационная экспансия США на Россию будет усиливаться в ближайшие годы.

"Если мы хотим победить в "войне идей", нам придется вести соревнование на игровой площадке намного более успешнее, чем мы это делаем в настоящее время", - подчеркнула Райс. Таким образом, новая Администрация США провозглашает курс на активизацию ведения информационной войны.

Интересно, что Райс не выдвигает ничего нового, а лишь повторяет мысли американского президента Р.Рейгана.

После прихода к власти он особо акцентировал растущее значение СМИ на международной арене. Р. Рейган в своей речи в британском парламенте 8 июня 1981года заметил, что "исход борьбы, развернувшейся в мире, будет зависеть не от числа бомб и ракет, а от победы или поражения стремлений и идей".

Если попытаться объективно проанализировать политические причины поражения СССР в "холодной войне", то на наш взгляд, наряду с объективными (экономическими, идеологическими и т.д.), существовали и субъективные (недооценка военно-политическим руководством СССР роли и значения информационных факторов, неспособность советской политической элиты вести активное информационное противоборство и др.).

Ведь в начале 80-х годов роль информационно-психологического воздействия, психологических операций в системе обеспечения национальной безопасности США резко возросла.

Сразу же после прихода в Белый дом президент Р.Рейган выдвинул свою стратегию национальной безопасности, состоящую из четырех компонентов: дипломатического, экономического, военного и информационного. Упор на информационный компонент был сохранен и в последующих мероприятиях по вопросам национальной безопасности.

В 1981 году в США был разработан проект "Истина", который предусматривал организацию пропаганды против СССР, путем быстрого информационного реагирования, а также пропаганды привлекательности США.

В 1983 году появился проект "Демократия", в рамках которого был создан штаб при СНБ по психологическому воздействию на СССР (через эми-

грантские центры, организацию прямого ТВ-вещания из США через спутник на посольства США в соцстранах, поддержку оппозиционных партий, профсоюзов).

В январе 1983 года Р.Рейган подписал директиву № 77 озаглавленную "Руководством общественной дипломатией, связанной с целями национальной безопасности". Эта директива давала более широкое определение государственной дипломатии, утверждая, что она "включает также мероприятия правительства США, направленные на обеспечение поддержки нашей политики национальной безопасности". Также определение подразумевало организацию и проведение широкого круга информационно-культурных мероприятий. Эта директива обеспечивала выработку механизма планирования и координации общественной, информационной, политической деятельности администрации США, а также вопросов, связанных с теле- и радиовещанием.

По мнению автора, с приходом Рейгана к власти, информационное воздействие стал принципиально иным. Началась эра глобальной борьбы за общественное сознание народов с использованием новейших информационных технологий на основе координации деятельности всех государственных, коммерческих структур и спецслужб США.

В США был реально образован союз спецслужб и крупного капитала. Этот союз создал мощные структуры анализа и ведения информационной войны против СССР.

При Р.Рейгане конституционные и государственные органы стали в возрастающей степени использоваться в качестве координационных и направляющих центров информационно-психологического воздействия. Центральную роль в процессе стратегического анализа и координации деятельности информационно-психологических структур США при Р.Рейгане стал занимать Совет национальной безопасности (СНБ).

Безусловно, скоординированная деятельность информационно-психологических структур принесла свои плоды – СССР перестал существовать.

Новая Доктрина Буша определяет Госдепартамент главным координационным и направляющим центром информационной экспансии США вместо Совета национальной безопасности. Поэтому и произошли кадровые перестановки в Вашингтоне.

24 февраля 2005 года состоится встреча президентов России и США в Братиславе.

Но антироссийские информационные операции, в духе реализации новой Доктрины Буша, уже начались. Их основная цель – информационно создать условия, при которых президент России пошел бы на стратегические уступки США.

27 января 2005 года влиятельная газета "The Washington Post", близкая к Администрации США (как газета "Правда" в СССР) печатает статью "Украинский урок Путину. Грозит ли российскому лидеру такое же испытание?".

Лишь одна цитата из этой статьи.

"Коррумпированная система власти Украины рухнула в результате восстания 'миллионеров против миллиардеров', которое также помогло Виктору Ющенко стать президентом. Перспектива восстания, возможно, маячит и перед президентом России Владимиром Путиным".

А 29 января 2005 года стало известно о том, что в комитете сената США по иностранным делам назначены слушания на тему "Отступление демократии в России" которые состоятся 17 февраля (ровно за неделю до встречи Буша и Путина) и будут проходить под председательством главы этого комитета сенатора-республиканца Ричарда Лугара.

Одним из главных выступающих будет председатель правления "ЮКОСа" Стивен Тиди. С оценкой "дела ЮКОСа" перед сенаторами выступит также один из самых известных американских юристов, член руководства адвокатской конторы "Williams & Connolly" Грегори Крэйг, специализирующийся на особо "громких" судебных делах.

Ранее он занимал пост помощника госсекретаря США Мадлен Олбрайт, отличающейся негативным отношением к России.

На предстоящих сенатских слушаниях выступят также директор программы по России и Евразии Фонда Карнеги экономист Андерс Аслунд, которых за последние несколько месяцев опубликовал более десяти антипутинских и антироссийских публикаций в ведущих западных СМИ.

Таким образом, реализация информационных антироссийских акций уже началась. Новая Доктрина Буша уже начинает действовать. У американцев слова не расходятся с делами.

Панарин И.Н.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В СОВРЕМЕННЫХ УСЛОВИЯХ *

Смену мировоззрения, произошедшую на рубеже третьего тысячелетия, предопределила революция в области коммуникаций и информации. Массовая компьютеризация, внедрение и развитие новейших информационных технологий привели к впечатляющему рывку вперед в сферах образования, бизнеса, промышленного производства и научных исследований.

До недавнего времени и в теории, и на практике в области обеспечения безопасности государств основное внимание уделялось ее военной составляющей. Сегодня уже стала очевидной ограниченность данного подхода, так как научно-техническая революция привела к созданию информационного обще-

* Информационные войны. Хрестоматия /Составители: Скиба Н.Е., Малыгин А.В., Бондаренко Е.И.. Учебное пособие для студентов высших учебных заведений, обучающихся по специальностям и направлениям «Международные отношения». – Хмельницкий. – 2003

ства, в котором информация является главным фактором управления современным миром и основным инструментом власти.

Глобальные социальные изменения, произошедшие в мире в конце XX в., требуют объективного анализа информационной среды мирового сообщества. Следует отметить, что ранее проблема обеспечения информационной безопасности в нашей стране не только не рассматривалась, но и фактически игнорировалась. При этом считалось возможным ее решение путем введения тотальной секретности и различных ограничений. И только в последние годы в России была осознана вся важность данного вопроса: в составе Совета безопасности РФ создана Межведомственная комиссия по информационной безопасности. Разработан проект ее доктрины, в которой отражены методы и средства защиты жизненно важных интересов личности, общества, государства в мировом информационном пространстве.

Современная геополитическая ситуация требует принципиально иного подхода к проблеме обеспечения национальной безопасности России, анализа содержания и эволюции всего спектра геополитических факторов, важнейшим из которых является информационный. Сегодня правомерно утверждать, что при прочих равных условиях достижение государством стратегических преимуществ зависит от имеющихся у него информационных возможностей. Об этом свидетельствуют итоги "холодной войны", которая велась прежде всего информационными средствами. Достигнув паритета с США в военной сфере, СССР потерпел поражение в информационном противоборстве.

В этом контексте становится понятной оценка американским военно-политическим руководством роли информации и объяснимы причины постоянного увеличения ассигнований на развитие и совершенствование информационных технологий. Так, если в 1980 г. на приобретение информтехнологий тратилось около 8 млрд. долл., то в 1994 г. – уже свыше 25 млрд.

Если попытаться объективно проанализировать политические причины поражения СССР в "холодной войне", то следует отметить, что наряду с объективными (экономическими, идеологическими и т.д.) существовали и субъективные (недооценка военно-политическим руководством СССР роли и значения информационных факторов, отсутствие эффективных технологий ведения информационного противоборства и др.). При этом в начале 80-х гг. роль информационнопсихологического воздействия, психологических операций в системе обеспечения национальной безопасности США резко возросла. Сразу же после своего избрания президент Р.Рейган выдвинул стратегию национальной безопасности, состоявшую из четырех компонентов: дипломатического, экономического, военного и информационного.

Акцент на информационном компоненте был сохранен и в последующих документах по вопросам национальной безопасности. В январе 1983 г. Р.Рейган подписал директиву "Руководство государственной дипломатией, связанной с целями национальной безопасности". Директива давала более широкое определение государственной дипломатической деятельности, утверждая, что

она "включает также мероприятия правительства США, направленные на обеспечение поддержки нашей политики национальной безопасности". Такая трактовка подразумевала организацию и проведение широкого круга информационно-культурных мероприятий. Более того, данная директива обеспечивала выработку механизма планирования и координации общественной, информационной, политической деятельности администрации США, а также вопросов, связанных с теле- и радиовещанием. В 1987 г. Дж.Сорос предпринял первую попытку внедриться в информационное пространство СССР в целях реализации рейгановской программы борьбы с "империей зла" и информационного компонента американской доктрины национальной безопасности.

Впервые Сорос получил мировую известность в 1992 г., когда после предпринятых им финансовых операций произошло катастрофическое падение курса фунта стерлингов. Он заработал на этом кризисе около 2 млрд. долл. Именно эти деньги стали использоваться для создания Фондов Сороса в постсоциалистических странах Восточной Европы (в настоящее время такие фонды функционируют в 30 странах, только в Белоруссии удалось юридически прекратить деятельность Фонда, через который осуществлялось финансирование деятельности антипрезидентской оппозиции), в том числе и в России.

Одновременно с приходом в США к власти администрации Р.Рейгана произошли кардинальные изменения в теории и практике информационного воздействия. Началась эра глобальной борьбы за общественное сознание народов с использованием новейших информационных технологий на основе координации деятельности всех государственных структур и транснациональных корпораций.

При Р.Рейгане государственные органы стали в возрастающей степени использоваться в качестве координационных и направляющих центров информационно-психологического воздействия. Центральную роль в процессе координации деятельности информационно-психологических структур США стал играть Совет национальной безопасности (СНБ). В доктрине "Психологическая пропаганда и национальная безопасность" СНБ квалифицируется как центральное звено в системе психологических операций наряду с госдепартаментом, МО, ЦРУ, а также Информационным агенством США (ЮСИА). Появился механизм глобального скоординированного информационно-психологического воздействия на мировое сообщество, состоящий из следующих звеньев: президент США - СНБ - министерства (ведомства) и организации США.

Безусловно, скоординированная деятельность информационно-психологических структур (государственных, общественных и коммерческих организаций) принесла свои плоды: сейчас США доминируют в мировом информационном пространстве. А с помощью развития сети Интернет США стремятся установить свое стратегическое лидерство в глобальном информационном пространстве и в XXI в. Пересмотр приоритетов и акцентов в интерпре-

тации проблем национальной безопасности поставили науку и практику перед необходимостью разработки совершенно нового аспекта этой проблемы – безопасности психологической.

В настоящее время в РФ существует система обеспечения необходимого уровня защищенности объектов безопасности (личность, общество, государство), созданная на основе закона "О безопасности".

Вместе с тем понятие "психологическая безопасность" не включено в этот закон и другие нормативные акты, касающиеся национальной безопасности России. Ускорившийся в последнее время процесс фундаментальных перемен в мире настоятельным образом требует решения информационно-психологических проблем обеспечения национальной безопасности России, защиты психики населения и военнослужащих от негативных информационно-психологических воздействий.

В настоящее время создано много новых средств воздействия на психику людей и управления их поведением. В прессе периодически появляется информация об американских программах "МК-ультра", АРТИШОК, а также аналогичных программах, разрабатываемых во Франции, Германии, Израиле, Японии и других странах.

В последние десятилетия возможности воздействия на психику человека резко возросли. Одной из главных причин этого являются значительные успехи, достигнутые в области психотроники, парапсихологии, биоэнергетики, других психофизиологических феноменов.

Поиск новых форм и методов воздействия на психику человека, больших масс людей развернут в большинстве ведущих стран мира. Лидером в этом деле; являются США, которые располагают наиболее разветвленной сетью институтов, центров, лабораторий, обществ для проведения теоретических исследований и решения задач военноприкладного характера. Большой интерес к подобным разработкам проявляют военные ведомства США.

Технически уже возможно и воздействие на психику человека с помощью спутников. В этой связи вызывает определенное опасение развертывание спутниковой системы ТЕЛЕДЕСИК, которое хочет осуществить с помощью российских ракет СС-18 (РС-20) американский миллиардер Б.Гейтс. Стоимость проекта составляет около 5 млрд. долл.3 Эта система может использоваться и в военных целях, а также для ведения информационного противоборства. Большое количество спутников (более 300) обеспечит возможность облучения любой точки Земли одновременно как минимум с двух спутников. Учитывая то, что американцы имеют сейчас на орбите 420 спутников, а Россия -160, в начале XXI в. США будут абсолютно доминировать в информационном пространстве планеты.

Таким образом, для защиты социальных объектов (личности, общества, государства) от опасных информационных воздействий необходимо создание системы информационно-психологического обеспечения как составной части системы национальной безопасности.

Информационно-психологическое обеспечение национальной безопасности России (ИПО НБ) представляет собой часть (подсистему) системы обеспечения национальной безопасности, позволяющую организовать скоординированную деятельность министерств (ведомств), предприятий, организаций, воинских частей, органов государственного и военного управления, общественных объединений, политических партий и граждан по обеспечению безопасности информационно-психологической среды общества, психологической безопасности населения и военнослужащих России.

Объектами ИПО НБ являются: а) информационно-психологическая среда общества (ИПСО), которая является частью информационной среды мирового сообщества и связана с использованием информации, информационных ресурсов, информационной инфраструктуры для оказания воздействия (влияния) на психику и поведение людей; б) информационные ресурсы (о духовных, культурных, исторических, национальных ценностях, традициях и т.д.); в) система формирования общественного сознания (мировоззрение, политические взгляды, духовные ценности); г) система формирования общественного мнения; д) система принятия политических решений; е) психика и поведение человека.

ИПО НБ имеет следующие цели: защита психики населения, социальных групп, военнослужащих, граждан от деструктивных информационно-психологических воздействий ИПСО; противодействие попыткам манипулирования процессами восприятия информации населением и военнослужащими со стороны враждебных Российскому государству политических сил, проводимым с целью ослабления его обороноспособности; отстаивание национальных интересов, целей и ценностей России в информационном пространстве (глобальном, региональном, субрегиональном, стран СНГ, национальном); постоянный мониторинг отношения российского общества к важнейшим проблемам национальной безопасности (диагностика общественного мнения), психического состояния российского народа, военнослужащих; противодействие информационной экспансии США в духовнонравственной сфере.

В последние годы на Западе искусственно создается негативный образ России. В СМИ распространяются слухи о "русской мафии", дискредитируются ведущие российские банки и компании. Голливуд резко увеличил выпуск кинофильмов, в которых русские представляются в качестве террористов, насильников. В этом контексте характерен эпизод с контрактом на 2 млрд. долл., который заключил "Газпром" с иранской фирмой НИОС в сентябре 1997 г. о разработке газового месторождения Южный Парс (совместно с компаниями Франции и Малайзии). Данная сделка сразу же вызвала возмущение конгресса США, который усмотрел в ней поддержку международного терроризма. Более того, 15 октября 1997 г. посол США в РФ Дж.Коллинз неожиданно посетил председателя правления РАО "Газпром" Р.Вяхирева и заявил, что активность "Газпрома" в Иране может стать основанием для применения санкций против этой российской компании.

Кроме того, на руководство РФ со стороны США было оказано значительное политическое давление в связи с принятием в сентябре 1997 г. Закона "О свободе совести и религиозных объединениях", который ограничивает деятельность тоталитарных сект и иностранных проповедников на территории России.

Госсекретарь США М.Олбрайт незадолго до принятия этого закона посетила Москву. На встрече с патриархом Алексием II, она обратилась к нему с просьбой не противодействовать активной деятельности западных религиозных сект на территории России. По мнению госпожи Олбрайт, это явилось бы наглядным подтверждением приверженности России идеалам свободы и демократии. Реакция патриарха была отрицательной. В одном из своих интервью он, например, заявил: "В России сегодня действует огромное количество зарубежных церквей, приходов и сект, деятельность многих из которых носит тоталитарный и деструктивный характер. Они применяют методики зомбирования и гипноза. Прибегают к помощи психотропных средств. Таким образом подавляется личность".

Информация на всех этапах исторического развития являлась объектом борьбы. Информационное противоборство велось практически во всех войнах. Его основное содержание долгое время составляли действия противостоящих сторон по ведению разведки и противодействию ей. Заметные количественные и качественные изменения информационное противоборство стало претерпевать по мере того, как началось создание единого мирового информационного пространства.

Современная научно-техническая революция произвела подлинный переворот в информационном обеспечении человеческой деятельности. Появилась массовая информация - предназначенные для неограниченного круга лиц печатные, аудио, видео и другие сообщения. Были созданы средства их быстрого распространения.

Следует различать информационное противоборство в широком и узком смысле слова (в военной или оборонной сфере). Так, в широком смысле информационное противоборство - это форма борьбы, представляющая собой использование специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Информационное противоборство в военной сфере представляет собой комплекс мероприятий информационного обеспечения, информационного воздействия и информационной защиты, проводимых по единому замыслу и плану в целях захвата и удержания информационного превосходства над противником при подготовке и в ходе военных (боевых) действий, доминирования в информационном пространстве (мировом, региональном, субрегиональном, национальном).

Следует также выделить два вида информационного противоборства в военной сфере: информационно-техническое и информационно-психологиче-

ское. При ведении информационно-технического противоборства главными объектами воздействия и защиты являются информационно-технические системы (системы связи, телекоммуникационные системы, радиоэлектронные средства и т.д.). Главными объектами воздействия и защиты в информационно-психологическом противоборстве являются психика личного состава вооруженных сил, спецслужб и населения противостоящих сторон; системы формирования общественного сознания, мнения и принятия решений.

Информационное противоборство в военной сфере включает три составные части. Первая - комплекс мероприятий по добыванию информации о противнике и условиях информационного противоборства; сбору информации о своих войсках; обработке информации и обмену ею между органами (пунктами) управления в целях организации и ведения боевых действий. Информация должна быть достоверной, точной и полной, а информирование - избирательным и своевременным. Решение перечисленных задач логично назвать информационным обеспечением управления войсками и оружием. Вторая - информационное воздействие. Оно включает мероприятия по блокированию добывания, обработки и обмена информацией, внедрению дезинформации. Третья - мероприятия информационной защиты, включающие действия по деблокированию информации, необходимой для решения задач управления, и блокированию дезинформации, распространяемой и внедряемой в систему управления.

Разрабатывая теорию информационного противоборства, следует учитывать, что оно ведется на стратегическом, оперативном и тактическом уровнях. В основном на стратегическом уровне должны действовать высшие органы государственной власти России, а спецслужбы и армейские подразделения - на оперативном и тактическом уровнях.

Понятия "информационное противоборство" и "информационная война" не идентичны. Информационное противоборство представляет собой комплексное совместное применение сил и средств информационного противоборства и вооруженной борьбы. Информационная борьба, в отличие от вооруженной борьбы, ведется как в мирное, так и в военное время.

Роль и место информационного противоборства в системе обеспечения национальной безопасности любого государства постепенно возрастает. Ведущие страны мира в настоящее время располагают мощным информационным потенциалом (прежде всего США, Япония, Франция, Германия), который может обеспечить им достижение политических целей, тем более, что отсутствуют международные юридические нормы ведения информационного противоборства.

Для защиты социальных объектов от негативных воздействий в ходе глобального информационного противоборства необходимо создание системы информационно-психологического обеспечения как составной части национальной безопасности России. Данная система должна обеспечить защиту психики гражданского населения и военнослужащих России от негативно-

го информационно-психологического воздействия. Ее основная задача —обеспечение психологической безопасности личности, общества, государства.

Информационно-психологическое воздействие представляет собой целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние (положительное или отрицательное) на функционирование и развитие информационно-психологической среды общества, психику и поведение населения, военнослужащих. Разновидностями информационнопсихологического воздействия являются психологическое и пропагандистское воздействие.

В связи с появлением и ускоренным развитием электронных СМИ резко усилилась роль общественного мнения, которое стало оказывать большое влияние на общественно-политические процессы, особенности функционирования информационно-психологической среды общества, психическое состояние военнослужащих в ходе войн и вооруженных конфликтов. Поэтому система формирования общественного мнения также является одним из основных объектов информационно-психологического обеспечения. Следовательно, необходимо изучение особенностей формирования и функционирования общественного мнения во время вооруженных конфликтов, на основе которого следует выработать практические пути обеспечения психологической безопасности военнослужащих.

Широкая информатизация вооруженных сил создала качественно новую ситуацию в развитии военного дела. Наглядной иллюстрацией этого служат вооруженные конфликты и войны последних десятилетий XX в. Их анализ со всей очевидностью свидетельствует о том, что ход и исход боевых действий любого масштаба в современном мире во многом определяются искусством ведения информационного противоборства.

Изучение вооруженных конфликтов второй половины XX в. показывает, что произошел перенос усилий в применении сил и средств информационно-психологического воздействия на более ранний период (от одного-двух месяцев до нескольких лет перед началом боевых действий), появились новые средства и способы информационно-психологического воздействия (информационное оружие).

Информационное оружие - это устройства и средства, предназначенные для нанесения противоборствующей стороне максимального урона в ходе информационного противоборства путем опасных информационных воздействий. Объектами воздействия информационного оружия могут являться: информационно-технические системы; информационно-аналитические системы; информационно-технические системы, включающие человека; информационно-аналитические системы, включающие человека; информационные ресурсы; системы формирования общественного сознания и мнения, базирующиеся на средствах массовой информации и пропаганды; психика человека. В тех случаях, когда информационное оружие прямо или опосредованно ис-

пользуется против психики человека (или социальной группы), то речь должна идти об информационно-психологическом воздействии.

Существующая в современной России система взглядов на информационно-психологическое обеспечение национальной безопасности на практике оказалась малоэффективной. Необходимы срочные меры по организации и проведению научно-исследовательских работ и научно-практических конференций с целью создания эффективных технологий обеспечения информационной безопасности России в условиях ведения глобального информационно-психологического противоборства.

Панарин И.Н.

СЛУХИ КАК ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ ВОЙНЫ*

Использование данной технологии имеет смысл выделить отдельно так, так, как она реализуется в результате применения комплекса различных приемов. Существует также ряд предпосылок социально-психологического характера, которые способствуют возникновению и распространению слухов среди людей. Психологические механизмы возникновения и распространения слухов давно привлекают внимание исследователей. Как правило эффект от использования ложной информации носит кратковременный характер, в основном в тот период, пока пропагандистское воздействие осуществляется в условиях дефицита информации.

Живучесть и восприимчивость к слухам, в значительной степени определяется тем, что они является легко доступным способом удовлетворения информационных потребностей человека, т.е. потребностей в информации, необходимой для социальной ориентации и организации своего поведения. Эмоционально негативные переживания сопровождают человека если у него нет информации о происходящих событиях, т.е. когда он находится в состоянии своеобразной "информационной неопределенности", "информационного дефицита". Вот этот информационный дефицит и помогают нейтрализовать слухи. Таким образом, человек субъективно ощущает себя информированным, но в то же время его поведение объективно начинает попадать в определенной степени в зависимость от конкретных слухов. Психологической основой для возникновения слухов является, в частности, искажение информации при устной передаче ее людьми друг другу. Причем, чем длиннее "цепочка", чем большее количество людей участвует в передаче сведений не подкрепленных достоверными данными официальных источников информации, тем значительнее искажаются эти сведения.

Проведенные специалистами эксперименты показали, что характер этих искажений непосредственно связан с имеющимися у людей социальными установками, так называемыми предиспозиционными факторами - чело-

век подсознательно настроен воспринимать в первую очередь именно то, что он ожидает. Кроме этого искажение также определяется особенностями и механизмами человеческого восприятия и отношений между людьми в процессе общения.

К другим причинам объективного характера, способствующим возникновению и распространению слухов, относятся следующие психологические факторы, способствующие искажению информации при ее передаче "из уст в уста":

- ограничение оперативной памяти человека, не позволяющее удержать большое количество информации; трудность в подборе точных семантических эквивалентов обозначения предметов и событий, о которых идет речь, а потому происходит постепенная подмена смысла;
- "домысливание" фрагментов отсутствующей информации, когда для придания ей стройности и достоверности приходиться додумывать недостающие детали; отсутствие критичности, что приводит к одностороннему восприятию без уточняющих вопросов в сомнительных деталях получаемой информации.

Среди социальных причин, порождающих, слухи в первую очередь необходимо выделить отсутствие или дефицит информации по волнующим людей проблемам или событиям, а также недостаточную оперативность, запаздывание в подаче информации.

Содержанием слухов чаще становится информация, удовлетворяющая потребности людей, которые неудовлетворены иными способами. Неудовлетворенность и ожидание удовлетворения выступают в качестве основных мотивов для восприятия и передачи воспринятой информации. По происхождению или источнику возникновения слухи могут быть стихийными или умышленно фабрикуемыми и целенаправленно распространяемыми.

Система слухов предназначена для распространения информации любого толка и создание определенного настроения среди населения. Посредством слухов возможно отыгрывать клеветнические материалы или самим распространять "темы" снижающие рейтинг оппонента. Через сеть "слухи" задаются информационные поводы, которые в дальнейшем отыгрываются в СМИ. Пример – "Население говорит что, а правда ли это?" Существуют и другие формы, но все зависит от слуха и что конкретно преследовалось создавая и распространяя слух.

Все слухи обсуждаются и получают четкую территориальную привязку по распространению и идеологическую направленность. Система слухов работает как в обычных условиях, так и в ходе выборов.

Основные направления

- Создание благоприятных условий для ведения пропаганды и агитации в пользу кандидата.
- Повышение рейтинга кандидата.
- Своевременная отработка информационных поводов.

- Привлечение внимания к нашим изданиям.
- Создание условий для опровержения клеветнических нападок со стороны оппонентов.
- Искусственное создание информационных поводов как для защиты так и для нападения.
- Посредством слуха возможно введение населения в заблуждение.
- Дискредитация наших противников.

Распространение слухов

- Непосредственные места работы.
- Садовые участки, дачи если есть.
- Соседи по дому, знакомые.
- Любые мероприятия посещаемые "Слухачами".
- В сети "Интернет" - специальные сайты.

Принцип работы

- Задается тема "слух".
- Прописывается сценарий.
- Инструктор и сценарист прорабатывают возможные варианты подачи слуха.
- Выезд на территории и сбор людей для проведения занятий по обучению методикам подачи слуха.
- Инструктаж по порядку работы с заданным слухом.
- Определяется время действия слуха.
- Проводится практическое занятие.

Формы распространения

- Рассказ, одного другому о том, что он где-то слышал или читал (в случае "читал" по заданию указывается издание).
- Обмен мнением о прочитанном "материале" в удобной для нас форме
- (по необходимости указывают издание).
- Рассказ что я слышал от своего знакомого о...ТЕМА. (Форма рассказа по секрету. Я первый узнал из достоверных источников, это точно проверено.)
- Доверительная беседа с друзьями и знакомыми и перевод разговора на заданную тему с высказыванием НАШЕГО МНЕНИЯ, НАШЕЙ ИНФОРМАЦИИ.
- В беседе с домашними и близкими родственниками. Я ехал и слышал в транспорте, что спорили или говорили о... ТЕМА.

Одна из задач распространителей слухов, выявить наших активных сторонников и привлечь их в наши ряды для дальнейшей работы.

Дополнительно под каждый слух прописывается сценарии и формы распространения.

За основу типологии слухов берутся следующие две характеристики: информационная и экспрессивная. Первая характеристика, определяет собой объективную степень достоверности, а вторая - общий тип эмоциональной реакции, на которую рассчитан и которую вызывает слух при его восприятии людьми, - желание, страх или враждебность.

В соответствии с информационной характеристикой слухи подразделяются на четыре основных типа:

- абсолютно недостоверные слухи;
- недостоверные слухи с элементами правдоподобия;
- правдоподобные слухи;
- достоверные слухи с элементами неправдоподобия.

Используя экспрессивную характеристику и вызываемую общую моциональную реакцию слухи, слухи подразделяются на следующие типы:

- слухи-желания, когда распространяемая информация имеет целью или объективно приводит к разочарованию по поводу несбывшихся в последующем ожиданий и вызывает соответствующую деморализацию людей;
- слухи-пугала, распространение которых наиболее эффективно и имеет благоприятную психологическую основу в среде с преобладающими настроениями тревоги, неуверенности и страха и обычно существенно деморализует людей, блокирует реализацию ими своих социальных обязанностей и дезорганизует целесообразную деятельность;
- разобщающие агрессивные слухи, вносящие разлад во взаимоотношения людей, нарушающие привычные социальные связи и организационно-структурные образования подозрительностью и взаимным недоверием, неприязнью и ненавистью к отдельным лицам или группам людей.

По степени влияния на психику людей слухи также подразделяются на:

- будоражащие общественное мнение определенных групп людей, но не вызывающие явно выраженных форм асоциального поведения;
- вызывающие антиобщественное поведение некоторой части определенных социальных групп;
- разрушающие социальные связи и организационно-управленческие отношения между людьми и выливающиеся в массовые беспорядки, панику и т.п.

Вывод - слухи являются эффективным средством ведения информационной войны во всех сферах (политической, дипломатической, финансово-экономической, военной).

Пахомов Ю.

МАНИПУЛИТИВНЫЕ ТЕХНОЛОГИИ В РЫНОЧНО-РЕФОРМАТОРСКОМ КОНТЕКСТЕ *

Сейчас уже признано, что Украина, наряду с Россией, больше других стран пострадала от глобальной реформаторской модели, – модели МВФ. Но почему, – возникает тогда вопрос, – протесты против глобализации и МВФ прошли не у нас, а в преуспевающих странах? То же относится и к массовым протестам на 1 мая сего года. Далее, – с чем связан наш, украинский парадокс, проявившийся в том, что модель, обрушивающая один мир, и создавшая другой, была сразу же принята буквально на веру: без осмысливания последствий, без выстраивания алгоритма? Кто-то скажет, – тогда не знали о губительных последствиях... Отвечу: во-первых, – это не аргумент; надо было узнавать. Во-вторых, – узнавать было легко: ведь были уже предостережения в адрес власти и реформаторской элиты со стороны ученых (российских и наших), уже тогда имевших представления о последствиях. К тому же на лицо был крайне негативный латиноамериканский опыт 80-ых годов; опыт получивший название "потерянное десятилетие". Наконец, – в третьих, - власть была уже в начале оповещена, что предлагаемая нам модель не годится для индустриальных стран, что она расчитана на слаборазвитые (лишенные тяжелой индустрии, науки, развитой социальной сферы) страны-должники с целью выкачки долгов и расчистки рынков для ТНК.

Возвращаясь к вопросу, – почему мы были так неосмотрительны, – важно сказать о подкупе элиты; ведь кредиты МВФ, превратившиеся затем в долги (значит, долговую зависимость) откровенно разворовывались.

Да, это был довольно мощный рычаг совращения новой элиты, в том числе и собственно реформаторов. Однако одного этого было мало. Ведь народ тогда (начало 90-ых годов) еще не был в состоянии нищенства и безысходности, – а значит он мог что-то узнавать и сопротивляться. К тому же энергия и дерзновенное желание новой жизни были тогда (в отличие от нынешних времен) на подъёме. А значит, – могли быть протесты, – причем тогда ещё, – не в виде наёмной (купленной) демократии, а подлинные.

Как видим, обстановка с принятием грабительской модели могла быть не так уж однозначной. Поэтому в дополнение к подкупу и развязанной (сверху-снизу) коррупции, важно было запустить тяжелую артиллерию иного рода, – артиллерию манипулирования общественным сознанием с целью психологического зомбирования и порабощения.

Возникает все же вопрос, – почему со стороны Запада, и, в частности, США (ведь МВФ подконтролен США) нам не была рекомендована модель созидательная, вроде тех, которые использовались в Испании, Турции, Египте, Японии, странах Юго-Восточной Азии, а также в странах послевоенной Европы? Ведь некоторые из этих моделей были адекватны именно нашей си-

* Манипулятивные стратегии в политике, экономике, бизнесе и методы противодействия. Материаллы конференции. – К., 2001

туации, – причем среди них и те, которые дали эффект "экономического чуда".

Объяснение тут имеется. Во-первых, Россия и Украина обладали мощным военно-промышленным комплексом, а разрушение его было возможно лишь в ходе общего развала экономики. Во-вторых, - и это обстоятельство более общее, – на годы развала СССР и нашего рыночного реформирования приходится бум глобализации, набиравший силу с 70-ых, и позволявший высокоразвитым странам облегченно присваивать доходы других стран на неэквивалентной основе. Новые информационные технологии, составляющие технологическую основу глобализации, давали огромные экономические преимущества технически передовому Западу. Причем именно на мирохозяйственной арене.

Для главных глобальных игроков открывалась возможность быстрее, весомее и проще обогащаться за счет участия в глобальном бизнесе, сравнительно с возможностями бизнеса внутреннего. Быстрее потому, что мгновенный маневр денежными потоками в масштабах планеты отныне позволял избегать длительных ожиданий финансовой отдачи. Основные доходы можно было получить за счет спекулятивных акций сразу же вслед за вложением т.н. портфельных инвестиций. Весомее, – потому что невиданное ранее ажиотажное перетекание капитала на глобальную арену вызвало к жизни гигантские ТНК, часто превосходящие своим могуществом (каждая в отдельности) довольно развитые страны. Проще, – потому, что главным источником обогощения стало не созидание (т.е. не прямое инвестирование), а финансовое изъятие дохода в режиме невиданно разросшейся неэквивалентности.

Итогом реализации глобальными игроками своих новых конкурентных преимуществ стало стремительное, катастрофическое отставание стран третьего мира от высокоразвитых стран. Так, диспаритет (по показателю ВВП на душу населения) 20% стран сильных и 20% стран слабых в разные годы соотносился: в 1960 г. как 30:1; в 1990 г. – 60:1; в 1999 г. – 90:1.

В такой ситуации естественной реакцией стран третьего мира, а равно и стран с переходными экономиками было выстраивание защитных мер, что требовало определенной (выборочной) закрытости и укрепления защитных функций государства. Важно было также брать на вооружение такую реформаторскую модель, которая бы обеспечивала созидание и ограждала от экспансии.

Глобальным игрокам как раз и понадобилась концепция и модель, нейтрализующие защитные меры, обеспечивавшие легкое взламывание экономических границ и обессиливание государства, облегчающие изъятие национального богатства за счет использования изощрённых финансовых инструментов.

Такой концепцией оказался опробованый в странах Латинской Америки монетаризм, такой моделью – модель (и рецептура) Международного валютного фонда. Однако шансы, что страны добровольно примут такую модель

были малы, да к тому же и элиты не везде настолько продажны, чтобы запросто продать страну.

Вот тут и понадобилось планетарного масштаба зомбирование, благо именно новейшие информационные технологии были для этого как нельзя лучше пригодны. Тем более, должна была сработать новейшая максима: "тот, кто владеет информацией, владеет миром."

Технологии, расчитанные на внедрение в сознание штампов монетарного реформаторства, разрабатывались с большой тщательностью, включая не только идеологические, но и организационные аспекты. Знаковым было само возложение задач планетарного реформирования на т.н. Вашингтонский консенсус. Это была своего рода разовая сходка представителей наиболее продвинутых стран и полностью подвластных США институтов, таких как МВФ, Всемирный банк и другие. Сошлись, приняли решение и разъехались, – конкретно не отвечает никто: ни США, ни МВФ, ни ВТО... При этом сразу же проявился двойной стандарт: одни (государственнические) модели – для себя; другие – прямо противоположные, – для зомбируемых стран-клиентов. Как писал по этому поводу Первый вице-президент Всемирного банка Дж.Стиглиц: "Ирония положения МВФ в том, что пока администрация Клинтона занималась продвижением принципов пути у себя дома, – посредством повышения роли государства в экономическом росте, – в действиях США (через МВФ) на международной арене господствовал рыночный фундаментализм, т.е. идеи, которые были опровергнуты в самой Америке."

Сам процесс навязывания модели МВФ сопровождался невиданной по масштабам информационной атакой и промыванием мозгов насчет спасительной роли монетаризма. Странам и народам через могущественные СМИ внушалость, что модель МВФ единственна и безальтернативна, что всё остальное – от лукавого. И это притом, что в мире именно успешными странами применялись десятки достойных внимания моделей, с рекомендациями прямо противоположными рецептуре МВФ. Адепты МВФ не останавливались перед подлогом и лжерекламой. Чего стоит, например, награждение Китая, отвергнувшего рецепты МВФ как вредоносные, премией за якобы реализацию эмвээфовских рекомендаций.

Но подлинное информационное передергивание в целях зомбирования осуществлялось по ходу реализации в стране-клиенте отдельных рецептов. Практически не было ни одной экономической истины, внедряемой в общественное сознание, которая не была бы извращена в интересах глобальной монетаристской экспансии. Народам внушалось, что государство должно сойти с экономической арены, что рынок сам все расставит. И это в тот период, когда Запад у себя дома усиливал роль, и усложнял функции, повышал расходы государства. К тому же сам либерализм, исповедуемый Западом, предполагал наиболее существенное повышение роли государства именно на этапе реформирования. Далее, подопечным странам, ввязавшимся в игры с МВФ, навязывались, как спасительные, идеи внезапной внешнеэкономической откры-

тости и внутренней взрывной либерализации, что сразу обрекало страны, лишенные на старте конкурентоспособности, на разорение индустриального потенциала, крушение науки, и сдачу рыночных позиций глобальным игрокам.

Мощнейшие информационные акции навязывания псевдореформаторских штампов и психологического манипулирования проводились в каждой "податливой" стране и в связи с решением задач захвата рынка импортом, внедрения рецептов сжатия денежной массы, обесточивания социальной сферы, выведения финансовых потоков из страны на тот же Запад.

Все, что делалось по линии рецептуры МВФ по всем каналам СМИ объявлялось единственно правильным. А возражать было не только сложно (ведь СМИ – в руках манипуляторов), но и психологически невыносимо. На каждого, кто выступал против рецептов МВФ наклеивались позорящие ярлыки "противников реформ", "зовущих в позорное прошлое", "красно-коричневых" и просто глупых. "Готовые на все" СМИ, воители рассеянных по стране и хорошо подкармливаемых Западом фондов и "независимых" экспертов неправительсвенных организаций, и просто одураченные шквалом пропаганды волонтеры-активисты, – практически лишали общество способности взлянуть на происходящее непредвзятым взглядом. Причем на каждый оппозиционный аргумент были заранее продуманные заготовки. Так, неудачи объяснялись отсутствием решительности и непоследовательным проведением безупречных реформаторских замыслов; ограбление народа трактовалось как плата за советское прошлое; накопление новыми богатыми несметных богатств, – неизбежностью этапа первоначального ("дикого") капиталистического накопления. При этом наших и заезжих реформаторов не смущало, что в той же успешной Польше или Венгрии от рецептов МВФ оставляли "рожки да ножки", что многое, притом, – главное делалось с точностью до наоборот. Что ни в Китае, ни во Вьетнаме, ни в Чехии, Польше и Венгрии не было ничего похожего на наше "неизбежное" и сказочное обогащение новоявленной элиты.

Нужно отдать манипуляциям от МВФ, а с ними и нашим подпевалам, должное. Их хватка и квалификация не уступала в эффективности высокому исскуству наиболее изощрённых режимов тоталитаризма. Они усвоили, да и знали по прошлому, что говорить с массами надо на языке чувств и верований, а не разумных доводов, доказательств и знания. Умело эксплуатировали они и то обстоятельство, что душа народа в высшей степени проста и цельна, что она не признает никакой половинчатости, что для нее существует только любовь и ненависть, правда и ложь. Учтено было в ходе проведенных в Украине реформ и то, весьма немаловажное для манипулирования обстоятельство, что с человеком голодным, да ещё и дрожащим от холода и безысходности, можно делать что угодно, причем безнаказанно.

Значение фактора манипулирования общественным сознанием концентрировано выявляется в том, что именно манипулятивные информационные технологии обеспечивают на мировой арене наибольшую прибыль. И если вернуться к вопросу о стремительно растущем разрыве в доходах богатых и

бедных стран, если упомянуть такое новое явление как "конченные страны", то все эти явления, таящие угрозу самому существованию человечества обусловлены в наибольшей степени фактором психологического порабощения. Кстати, именно на украинском и российском примерах это очевидно. Ведь именно вследствие психологического навязывания нашим двум странам реформаторской модели, расчитанной на разгром экономики, из Росии выведено в западные банки и оффшоры от 300 до 800 млрд. долларов США, а из Украины - более 40 млрд., что более чем десятикратно превышает украинский бюджет.

И не случайно зомбирующие технологии (особенно т.н. "метатехнологии") никогда и никому не продаются, и держатся под строжайшим секретом. Они ведь по большему счету не только сверхвыгодны, но и преступны.

Задумаемся: почему наши два народа, буквально в штыки встречавшие ещё в конце 80-ых годов любое посягательство на их доход (вспомним реакцию на маневр премьера СССР В.Павлова с пятидесятирублевыми купюрами), - в годы 90-ые безропотно позволили перетекать своим сбережениям в карманы богачей!? - да потому, что видимость была такая, вроде сбережения исчезли по воле рока, а не по злому умыслу. А ведь взрывная гиперинфляция - это был именно умысел, преследующий цели мгновенного создания на пустом месте класса богачей, тех богачей, которые вследствии своей преступности и искусственно создаваемой нестабильности переведут капиталы на Запад. И операция эта имела в тайниках у реформаторов (западных и наших) даже свое название: "ликвидация навеса в виде сбережений".

Прозрение наступило лишь тогда, когда страна вплотную подошла к пропасти, — да и то, — с помощью разоблачений и разгрома руководства МВФ (а с ними и идей Вашингтонского консенсуса), осуществленных под влиянием мировой общественности на Востоке и на Западе.

Даже Комиссия Когресса США признала, что "курс МВФ привел к сокрушительному провалу и отбросил Россию и другие бывшие республики СССР на задворки мирового сообщества".

Мир, как видим, стряхнул с себя зловещий навес в виде глобальных психологических манипуляций от МВФ. Мы же вылазим из-под могильного камня эмвээфовских реформ, — увы, — не по своей инициативе, и не по причине преодоления внедренных в наше сознание штампов, а по причине внешней, от нас не зависящей. И вовсе не ясно, обрели ли мы достаточный иммунитет против психологического манипулирования и зомбирования. А ведь именно от этого зависит, какое нас ожидает будущее.

Важно нам задуматься и над тем, почему под власть общепланетарного психологического манипулироания не попали такие страны как Венгрия, Чехия, Польша; почему модель МВФ была категорически отвергнута большинством азиатских и ближневосточных стран.

Видимо, во многих случаях дает себя знать "броня" в виде чувства собственного достоинства, а также и системы цивилизационных ценностей. Ус-

пех, как показывает мировой опыт, достигнут лишь теми странами, которые сами выстраивали и концепции, и модели своих реформ, которые весьма избирательно - очень недоверчиво, осваивали лучший (а не худший) мировой опыт. А мы ведь даже гордились, что не будем изобретать свой "велосипед", что будем "как все". И было нам почему-то невдомек, что "все", кто удачливы, трансформируют свою экономику по-разному — синтезируя разное лучшее, и адаптируя это лучшее к себе, к своей экономической, социальной и (что немаловажно) ментальной специфике.

Печоров С.

ДЕЗИНФОРМАЦИЯ КАК МЕТОД ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ *
(По итогам конфликта в Персидском заливе)

Вооруженный конфликт в зоне Персидского залива, завершившийся фактически поражением Ирака, имел ряд особенностей с точки зрения методов, масштабов и достигнутых результатов психологической войны, которая была развернута задолго до начала боевых действий. Необходимо отметить, что главная роль отводилась обширному комплексу дезинформационных мероприятий, применявшихся противоборствующими сторонами для обеспечения военных в политических акций оперативного и стратегического характера. Особенность этих мероприятий во многом определялась задачами, которые решали участники конфликта на каждом из четырех этапов его развития.

Первый этап (до 2 августа 1990 года) - непосредственная подготовка к вторжению иракских войск в Кувейт. Командование армии Ирака постаралось обеспечить всестороннюю внезапность нападения на Кувейт. С этой целью Багдад предпринял ряд шагов, усыпивших бдительность кувейтского руководства и навязавших специальным службам Кувейта и союзных ему государств заведомо ложное представление о своих намерениях. Саддаму Хусейну, давно снискавшему себе репутацию «постоянного нарушителя спокойствия» в регионе, не удовлетворенному неуступчивостью Кувейта по отношению к его требованиям, связанным с квотами на нефть и притязаниями на кувейтские месторождения этого стратегического сырья, путем постепенного нагнетания антикувейтской истерии в национальных средствах массовой информации удалось создать впечатление, будто его угрозы Кувейту представляют собой не что иное, как очередной «иракский шантаж».

Весьма примечательно, что на эту уловку, видимо, попались и американцы. Согласно сообщениям западной прессы, еще 25 июля 1990 года ЦРУ передало в Белый дом полученные с помощью космических средств фотоснимки, подтверждавшие, что иракские войска продолжают концентрироваться на границе с Кувейтом. 30 июля американская разведка информировала руководителей ряда арабских государств, что численность группировки в

* Информационные войны. Хрестоматия /Составители: Скиба Н.Е., Малыгин А.В., Бондаренко Е.И.. Учебное пособие для студентов высших учебных заведений, обучающихся по специальностям и направлениям «Международные отношения». – Хмельницкий. – 2003

данном районе достигла 100 тыс. человек. Однако акция С. Хусейна расценивалась руководством США всего лишь как «игра мускулами». 1 августа, когда Багдад уже принял решение о вторжении, иракские и кувейтские представители все еще вели переговоры по мирному урегулированию конфликта. Несмотря на то что к концу указанного дня американская и израильская разведки выразили сомнение относительно истинности намерений Ирака, «слишком прямолинейный», но «не выходящий за рамки обычного» тон угроз не внушал серьезных опасений. Если предположить (а для этого имеются все основания), что США, преследуя свои цели, умышленно подыгрывали Багдаду, настраивая кувейтцев на «безмятежный лад», то и в таком случае можно констатировать: дезинформация, на сей раз осуществленная американцами, увенчалась успехом. Так или иначе, но ночное вторжение иракцев на территорию Кувейта явилось «полной неожиданностью» для руководства этого государства.

Второй этап, связанный с проведением сторонами комплекса мер по обоюдной дезинформации, охватывает период со 2 августа 1990 года по 17 января 1991-го (операция «Щит пустыни»). Инициатива в проведении дезинформационных мероприятий на данном этапе конфликта в Персидском заливе принадлежала американцам. С начала осуществления операции «Щит пустыни», имевшей целью обеспечить всестороннюю подготовку к войне с Ираком, в том числе переброску в регион к развертывание значительного количества войск и военной техники, командование вооруженных сил США во взаимодействии прежде всего с руководством вооруженных сил Великобритании, Франции, принимавших активное участие в военной кампании, разработало и четко провело в жизнь комплекс мер по психологической обработке и дезинформации противника.

По данным иностранной печати, в период с августа по декабрь 1990 года президент Дж. Буш подписал три секретные директивы, санкционировавшие осуществление «самых разнообразных мероприятий по специальным программам», в том числе и дезинформационным. Они проводились совместно специальными службами военных ведомств США и союзных стран с целью введения в заблуждение не только вооруженных сил и населения Ирака, но и народов своих государств, международной общественности. При этом особая роль отводилась средствам массовой информации, чья работа строилась на основе специальных инструкций и наставлений Пентагона для корреспондентского корпуса, реализация которых фактически превратила конфликт в Персидском заливе, по выражению французской газеты «Юманите», «в самый закрытый в нынешнем столетии».

Американские, британские и французские корреспонденты, включенные в состав аккредитованных при МНС журналистских пулов, в письменной форме обязались строго соблюдать жесткие нормы в отношении характера и содержания передаваемых сообщений, установленные военными властями. Практически все сведения из районов конфликта строго дозировалась воен-

ной цензурой. Теле- и радиоком-пании могли интервьюировать только специально отобранных для общения с репортерами военнослужащих. Соответствующие военные органы предоставляли в распоряжение телекомпаний специально снятые видеоклипы, изображавшие в нужном для командования союзников свете ход подготовки к ведению боевых действий. Весьма характерно, что в рекомендации радио- и телекомпании Би-би-си, специально составленной для освещения конфликта, также подчеркивалась необходимость сведения к минимуму публичного показа снятых крупным планом раненых или трупов погибших британских военнослужащих, а также ограничения эфирного времени, предоставляемого противникам войны.

Основным объектом психологического давления и дезинформации, естественно, были вооруженные силы Ирака и население этой страны. Мощной кампанией, развернутой средствами массовой информации, главным образом через радиовещание, американцы и их союзники преследовали цель подорвать доверие иракцев к президенту С. Хусейну, убедить в бесперспективности сопротивления военной машине США, дискредитировать и принизить качество состоявшего на вооружении иракской армии оружия и военной техники, а также дезинформировать иракского лидера и командование вооруженных сил Ирака о планах подготовки к боевым действиям американских войск и их союзников в целом. В рамках этой кампании самолеты ВВС США сбрасывали над районами дислокации частей иракской армии миллионы листовок, призывавших солдат не оказывать сопротивления и переходить на сторону коалиции, возглавляемой Соединенными Штатами. Вместе с листовками разбрасывались и малогабаритные радиоприемники, позволявшие прослушивать на фиксированных частотах передачи специальных «антииракских радиопередатчиков».

Одновременно с этими мероприятиями предпринимались шаги и в противоположном направлеиии. Подыгрывая иракским средствам массовой информации, которые изо дня в день внушали своим гражданам, что их армия, «закаленная в многолетних боях» с Ираком, имеет «всесторонний, богатый опыт», президент «обладает полководческим талантом», американские официальные представители умышленно искажали данные своей разведки, сознательно недооценивая в публичных выступлениях, такие казавшиеся в итоге решающими факторы, как недостаточные профессионализм и морально-волевые качества иракских военнослужащих. Этому в известной степени способствовали и появившиеся в западной печати прогнозы потерь многонациональных сил в случае начала боевых действий, исчислявшихся десятками тысяч. В частности, выделялся факт прибытия из США в Саудовскую Аравию 55 тыс. пластиковых мешков-гробов, а также огромных плавучих госпиталей «Мерси» (США) и «Ла-Ранс» (Франция), каждый из которых способен круглосуточно принимать до 200 раненых. Эти два, казалось бы, взаимоисключающих направления психологической обработки в действительности дополняли друг друга, обеспечивая полное перекрытие воспринимаемого иракцами

информационного потока. Причем наибольшего эффекта достигли в тот период как раз те сообщения, передача которых преследовала цель «расслабить» иракцев, стимулировала у командования вооруженных сил страны чрезмерную самоуверенность и непогрешимость в своих действиях.

Пытаясь оправдать свое намерение во что бы то ни стало разрешить возникший кризис военным путем, американские представители на самом высоком уровне постоянно дезинформировали мировое общественное мнение относительно степени угрозы вторжения Ирака в Саудовскую Аравию, ОАЭ, а также высадки десанта в Бахрейне.

Столь же преувеличенными были заявления представителей администрации США о ядерном потенциале Ирака. В то же время, нагнетая в средствах массовой информации психоз относительно большой вероятности использования Ираком химического оружия, американцы и их союзники явно переусердствовали, спровоцировав в свою очередь иракскую кампанию по запугиванию противников возможностью применения этого оружия. Так, печатный орган иракского военного ведомства «Аль-Кадисия» констатировал: любая атака на Ирак будет отбита с использованием химического оружия. Между тем, как свидетельствовала западная печать, в ходе операции по освобождению Кувейта так и не удалось обнаружить ни одного химического снаряда.

Отсутствовали средства химической защиты и у большинства попавших в плен иракских военнослужащих, Эта хорошо скоординированная «информационная агрессия» достигла своей цели, по крайней мере. в отношении населения США. Если к концу сентября 1990 года лишь каждый десятый американец выступал в поддержку войны, то к началу ее развязывания (середина января 1991 года), согласно данным опросов, уже свыше 80 проц. граждан США поддерживали действия своего президента относительно урегулирования кризиса силой.

Что касается иракских мероприятий по дезинформации противника в тот период, то, по мнению западных аналитиков, они не принесли сколько-нибудь ощутимых результатов. Прежде всего это относится к воздействию иракской машины психологической войны на американцев и западно-европейцев. Специалисты в этой области из стран Запада однозначно оценили мероприятия Ирака по дезинформации как «неуклюжие». Примерами могут служить распространявшиеся в тот период иракскими органами массовой информации (но тут же легко опровергаемые) слухи о якобы имевших место казнях в вооруженных силах Саудовской Аравии «за отказ воевать со своими иракскими братьями», а также сообщения о якобы тайных переговорах между Ираком и Кувейтом с целью разрешения кризиса на приемлемых для обеих сторон условиях.

Следует подчеркнуть, что за несколько недель до начала боевых действий в средствах массовой информации Запада появились сообщения о «действенности экономических санкций», введенных решением СБ ООН. Так, в

ряде публичных выступлений директор ЦРУ США У. Уэбстер подчеркивал, что «санкции оказались более эффективными, чем ожидалось», что они «подорвали экономику Ирака и ослабили его армию», следовательно, мол, нет необходимости в ведении боевых действий: Ирак через некоторое время и так будет «положен на лопатки».

Накануне нападения в содержании ориентированной на Багдад дезинформации появились новые акценты. Теперь уже официальные представитель министерства обороны США, не отрицая возможности развязывания военных действий, вводили иракцев в заблуждение относительно того, что МНС будут готовы к ночному наступлению лишь к началу марта, а к дневному - в лучшем случае к середине февраля.

Это «подтверждалось» многочисленными комментариями в различных печатных изданиях, в программах радио и телевидения. Так, буквально за несколько часов до начала воздушной кампании представитель Эй-би-си, комментируя экстренное совещание совета национальной безопасности США, подчеркнул: «Истечение срока вывода иракских войск из Кувейта (15 января) не означает автоматического вступления США в войну». Одновременно агентство АП со ссылкой на «секретные источники» в Вашингтоне уточнило, что президент Буш «еще не принял решение о войне с Ираком» и «каждый новый день предоставляет Багдаду возможность избежать войны и выбрать тропу мира».

Все это в значительной мере дезориентировало иракское руководство и настолько притупило его бдительность, что даже неоднократные предупреждения в советской прессе о серьезности намерений США не возымели действия. Получив за несколько дней до начала воздушной кампании предложение президента Буша обменяться визитами министров иностранных дел, С. Хусейн заявил в своем окружении: «Я же говорил вам, что Советский Союз запугивает нас неизбежностью удара, а события идут по другому сценарию».

В зарубежной печати особо выделялась роль американских спецслужб в распространении различного рода ложных, дезинформирующих сообщений на всем протяжении конфликта с целью представить в невыгодном свете Советский Союз. Нельзя расценить иначе, как провокационное, появившееся 14 ноября 1990 года на страницах «Вашингтон тайме» и подхваченное другими изданиями со ссылкой на источники в разведслужбах США сообщение о якобы продолжавшихся поставках советских ракет СС-12 в Ирак, хотя к этому времени Советский Союз уже определил свое отношение к агрессии Ирака против Кувейта и добивался ее прекращения политическими средствами.

В феврале 1991 года, тогда военные действия союзников против Ирака были в полном разгаре, средства массовой информации Запада передали целую подборку материалов, в которых со ссылкой на анонимные источники из ЦРУ и представителей радиоразведки Саудовской Аравии, сообщалось о якобы перехваченных радиопереговорах какого-то советского офицера, руководившего действиями иракского батальона, о советских военных советниках и

специалистах, помогавших иракцам обслуживать и наводить на цели ракеты «Скад», о неопознанном советском судне с военным грузом для Ирака, о целых транспортных колоннах, направлявшихся из южной части СССР через Иран в Ирак и т. п.

Организаторы этой антисоветской кампании в средствах массовой информации США пытались ввести в заблуждение мировую общественность относительно искренности позиции СССР в отношении конфликта, вызвать недоверие к предпринимавшимся дипломатическим шагам Москвы для мирного решения проблемы. В подобных действиях усматривалось одно намерение: отстранить Советский Союз от участия в дальнейшем урегулировании обстановки на Ближнем Востоке в целом.

Третий этап дезинформационных мероприятий — это время с начала воздушной кампании до непосредственной подготовки к проведению воздушно-наземной операции.

Еще накануне нападения на Ирак в средствах массовой информации стран Запада развернулось широкое обсуждение возможного характера предстоящих военных действий. Направление этой дискуссии задал государственный секретарь США Дж. Бейкер, который в своем официальном выступлении 28 ноября 1990 года подчеркнул, что Соединенные Штаты нанесут внезапный массированный и решающий удар всеми тремя видами вооруженных сил. «Мы хотим дать противнику возможность выбрать один из многих способов погибнуть», — заявил высокопоставленный сотрудник Пентагона: комментируя выступление главы дипломатического ведомства США в сенатском комитет, по иностранным делам. За два месяца до начала боевых действий министр обороны Р. Чейни отстранил от должности начальника штаба ВВС М. Дугана, который в интервью газете «Вашингтон пост» «чересчур откровенно» высказался о решающей роли, отводившейся в грядущей войне авиации союзников. Судя по официальным комментариям в связи с этим смещением, заявление американского генерала явно противоречит принятой в армии США концепции «воздушно-наземная операция (сражение)». И даже тот факт, что массированным авиационным ударом практически без участия наземных войск американцы в точности повторили вариант боевых действий, отрабатывавшийся ими во время учений на континентальной части, говорит об успехе дезинформационных мероприятий союзников, заставивших иракское командование допустить существенный просчет в оценке форм и способов предстоящих боевых действий.

Первые комментарии в западной прессе по поводу результатов воздушной наступательной операции, в ходе которой выполнялось до 1,5 - 2 тыс. самолето-вылетов в сутки, отличались беспрецедентным психологическим делением на иракцев, создававшим впечатление полного разгрома их вооруженных сил. Однако, несмотря на подавляющее преимущество многонациональных сил в воздухе, решительного успех в первые дни ведения военных действий добиться не удалось. Чтобы не подорвать свой авторитет и, что еще

более важно, не дать повода иракцам свести на нет последующие усилия союзников в области дезинформации, представители вооруженных сил антииракской коалиции и средств массовой информации Запада пошли даже на такой шаг, как официальное дезавуирование первых победных реляций. В частности, как были вынуждены признать иностранные специалисты, вопреки первым сообщениям систему ПВО Ирака полностью уничтожить не удалось.

Продуманно и эффективно, с учетом опыта восьмилетней войны с Ираном, в Ираке была осуществлена оперативная маскировка, создано значительное число ложных аэродромов и стартовых (огневых) позиций. По сообщениям западной прессы, особенно удачно использовалось несколько тысяч макетов танков и самолетов, а также и ракет для дезориентации летчиков авиации МНС. Благодаря ложным радиосетям удалось обеспечить живучесть войск в ходе первых массированных налетов авиации противника Целенаправленно было проведено инженерное оборудование местности. Еще до начала конфликта Ирак приобрел десятки гектаров маскировочных сетей, позволившие скрыть от наблюдения противника скопления боевой техники. Следует подчеркнуть, что искусная маскировка, осуществленная иракцами, при всей ограниченной маскировочной емкости театра даже заслужила похвалу председателя комитета начальников штабов США генерала К. Пауэлла.

Эффективно, с прицелом на мировое общественное мнение иракцы использовали некоторые телепередачи с мест разрушений в результате бомбардировок и обстрелов крылатыми ракетами «Томахок». Несмотря на опровержения западными специалистами видеоклипа о «разрушении находившейся вблизи Багдада фабрики молочных смесей для грудных детей» (под тем предлогом, что это якобы было предприятие по производству биологического оружия), данный телесюжет вызвал бурное негодование во всем мире и инициировал кампанию за немедленное прекращение боевых действий.

Четвертый этап дезинформационных мероприятий был связан с непосредственной подготовкой МИС к проведению наземной операции по освобождению Кувейта и разгрому группировки иракских войск.

Через неделю после начала массированных налетов авиации МНС, когда разрушительные последствия бомбардировок стали очевидны, в средствах массовой информации стран Запада появились первые заявление представителей высшего командования США и пространные комментарии, в которых ставилась под сомнение необходимость проведения операции сухопутными войсками. Приблизительно через три недели массированных налетов акцент был резко смещен.

Теперь уже не отрицалась необходимость ведения замены, но все еще высказывались предположения о целесообразности продолжения бомбардировки и обстрела крылатыми ракетами. Так, за десять дней до начала операции сухопутных войск израильское радио информировало о том, что командующий группировкой МНС в зоне Персидского залива генерал Н. Шварцкопф рекомендовал министру обороны США Р. Чейни продолжать еще в течении

месяца налеты на иракские позиции, а уже потом приступить к боевым действиям на суше. В это же время американские средства массовой информации со ссылкой на анонимные военные источники сообщили о намерении руководителей операции «Буря в пустыне» продлить бомбардировки еще на 30 суток. Одновременно в интересах дезинформации иракцев о направлении предполагаемого главного удара вблизи кувейтско-саудовской границы проводилась имитация переброс войск.

Весьма искусно американцы и их союзники вводили в заблуждение иракское командование относительно своего мнимого намерения высадить морской десант на побережье оккупированного Кувейта.

Так, в западных средствах массовой информации появились сообщения о том, что «наземной кампании против Ирака обязательно будет предшествовать высадка крупных сил десанта, в частности морской пехоты». Эта версия, активно обсуждавшаяся в прессе, а также проведенные американским амфибийно-десантным соединением в водах Персидского залива демонстративные действия и мероприятия по уничтожению рифов, песчаных отмелей и других естественных препятствий, подавление некоторых целей на берегу вынудили Ирак стянуть в противодесантную оборону до пяти дивизий. На самом деле высадки не произошло, а значительная часть иракских войск была практически выключена из боевых действий, что облегчило наступление 1-й и 2-й экспедиционных дивизий морской пехоты США на приморском направлении.

Все это наряду с продолжавшимися более месяца воздушными налетами, приведшими к огромным человеческим жертвам и разрушениям, окончательно сломило боевой дух иракских военнослужащих. В результате начавшееся 24 февраля наступление многонациональных сил завершилось уже к исходу пятых суток вытеснением иракской группировки из Кувейта и освобождением этой страны.

Весьма характерным представляется использование США и их союзниками «фактора ООН» для развязывания себе рук в ходе развития событий в зоне Персидского залива. По мере того как бомбардировки населенных пунктов Ирака становились все более интенсивными, средства массовой информации Запада все чаще характеризовали явно выходящие за рамки «достаточности» массированные налеты как «войну, ведущуюся ООН». Однако сам генеральный секретарь этой организации Перес де Куэльяр в то же время подчеркивал: «Необходимо прежде всего уточнить одну вещь, которая остается пока неясной. Нынешний конфликт - это не война ООН. Это - война, санкционированная Советом Безопасности».

В заключение следует отметить тот факт, что на протяжении всего конфликта, особенно его «боевой стадии», средства массовой информации Запада безудержно восхваляли, а также явно преувеличивали достоинства оружия и военной техники, состоящих на вооружении многонациональных сил, и прежде всего США. Необходимо признать умелое использование американским военно-промышленного комплексом для проталкивания через конгресс

новых заказов на вооружения. Бывший директор Агентства по контролю за вооружением и разоружение П. Уернке был даже вынужден предостеречь законодателей от «быстрой и чрезмерной реакции» на давление лоббистов из военно-промышленных концернов и обслуживающей Пентагон прессы. В частности, выразив сомнение относительно появившихся в средствах массовой информации данных об успешных пусках ракет "Патриот", (в действительности они были строго засекречены), он высказал предположение, что сторонники «звездных войн» наверняка воспользуются этим для увеличения закупок не только ракет данного класса, но и сокращенные в последние годы расходов на СОИ. Не прошло и нескольких недель после окончаний военных действий, как оно сбылось: в конгресс поступил запрос о выделений дополнительных средств на приобретение 500 ракет «Патриот», хотя в Заливе их было использовано менее 200. Министр обороны Р. Чейни выступил с предложением увеличить в следующем финансовом году на 60 проц. (до 4,6 млрд. долларов) расходы по программе СОИ.

Не остались в стороне от этой кампании и западноевропейцы. Так, известный французский специалист в области вооружений П. Лелюш в целой серии статей обосновал необходимость немедленного отказа от намеченного было сокращения военного бюджета Франции под предлогом, «чтобы безнадежно не отстать от США в военных технологиях».

Таким образом, подготовка и ведение военных действий в зоне Персидского залива подтвердили значение методов психологического давления, и особенно дезинформационных мероприятий как их важнейшей части, продемонстрировали необходимость тесного взаимодействия всех видов и способов введения в заблуждение на стратегическом и оперативно-тактическом уровнях, наглядно показали ту роль, которую могут играть средства массовой информации в сохранении в тайне планов, введении в заблуждение противника, навязывании ему своей воли и дезориентации мировой общественности.

Почепцов Г.Г.
ИНФОРМАЦИОННЫЕ ДЕЙСТВИЯ И ПРОТИВОДЕЙСТВИЯ: ОСНОВНЫЕ ХАРАКТЕРИСТИКИ*

Современный мир вступил в совершенно новый тип жизни, в котором качественно иную роль играет информация и строящаяся на ней экономика. Информационные процессы, став главным нервом современного общества, сделали это общество не только сильнее, но и гораздо уязвимее. Украинский пример с «кассетным скандалом» демонстрирует эту новую роль информации. Российский пример с раскруткой гибели «Курска» и сменой владельцев НТВ также показывает этот новый тип влияния на общества, когда медиакризис может быть сильнее реального кризиса. Смена владельца акций НТВ

* Манипулятивные стратегии в политике, экономике, бизнесе и методы противодействия. *Материаллы конференции.* – К., 2001

стала кризисом, порожденным медиа-структурой, при этом речь идет только о том, что Е. Киселев не может претендовать на роль гендиректора, а только на роль главного редактора. Но всю страну лихорадит, поскольку информационная инфраструктура стала сегодня одним из важнейших нервов общества. Наш «кассетный скандал» также является медиа-кризисом, раскрученность которого привела к политическим последствиям и резкой поляризации общества, когда все ходят обвешанные ярлыками (пропрезидентскими или антипрезидентскими).

«Информация редко бывает нейтральной или объективной», —отмечают современные британский исследователи (Sherman B., Judkins P. Virtual reality and its implications. - London, 1992. - P. 231). Именно эта ее характеристика ставит информацию в центр современной политики и бизнеса.

Информация также стала серьезным инструментарием, позволяющим изменять сложившиеся ситуации в политике и бизнесе. Приведем лишь некоторые примеры использования информационного инструментария для резкого изменения политической ситуации в стране.

В конце пятидесятых британский МИД выделял деньги на издание в Иране в переводе на фарси романа Бориса Пастернака «Доктор Живаго», чтобы рассказ об ужасах гражданской войны и большевизма спас шаха, заставив иранцев отвернуться от революционеров («Книжное обозрение», 2001, 6 авг.). То есть текст, созданный совершенно в иных условиях, запускается в новую страну, чтобы получить совершенно конкретные планируемые результаты. По сути делается попытка изменить виртуальную реальность, чтобы в результате изменить подлинную реальность.

Рой Медведев связывает ГКЧП с публикацией в «Московских новостях» последнего варианта Союзного договора (Медведев Р. За кулисами августа. К 10-й годовщине ГКЧП // «Столичные новости" 2001, 14-20 авг.). Документ продемонстрироваол, что будет иметь место фактический распад СССР. М. Горбачев был разгневан публикацией и требовал обнаружить виновников «утечки», но на следующий день все центральные газеты обнародовали этот документ. В результате будущее ГКЧП как бы получило идеологическую поддержку, обосновывающую приостановление процесса распада. Здесь также изменения в виртуальной реальности вызвали изменения в подлинной реальности (ГКЧП), которые привели к изменениям.

Великобритания. В 1972 г. была проведена информационная операция, призванная привязать Советский Союз к событиям в Северной Ирландии, создавая из нее «британскую Кубу» (Lashmar P., Oliver J. Britain's secret propaganda war. - Phoenix Mill, 1998). Журналисты рассказали о высадке с советской подводной лодки обученных КГБ спецов в области подрывных операций. Для достоверности были даже распространены сфальцифицированные фотографии. Здесь мы тоже видим перехода к виртуальной реальности, чтобы получить результирующие изменения в подлинной реальности.

Это получает подтверждение в мифологической картинке, привычно

рисующей СССР как «империю зла». Как видим, придумывается событие, которое соответствует не реальности, а мифологии. Псевдособытие «вытекает» из модели мира, а не наоборот – модель мира формируется событиями.

Во всех этих случаях информация в сочетании с имеющимся на данный момент контекстом призвана вывести индивидуальное/массовое сознание на определенные действия:

ИНФОРМАЦИЯ + КОНТЕКСТ = ДЕЙСТВИЕ

Планировщики такого события имеют в наличии контекст и четкое представление о желаемом действии, поэтому они имеют возможность подобрать именно ту информацию, которая и сработает в роли определенного «триггера». И таких псевдотекстов в современной истории достаточно. Это, к примеру, «Протоколы сионских мудрецов», «письмо Зиновьева» и под.

Во всех этих случаях имеется переход между невербальной и вербальной областями, чтобы вернуться к реагированию именно невербального уровня.

В качестве примера фонового воздействия можно упомянуть, скажем, «гипотезу» Сергея Филатова, в свое время три года проработавшего главой администрации Ельцина, который сегодня считает следующее: «Против Бориса Николаевича спецслужбы организовали закрытую пиаровскую кампанию по подрыву его авторитета. Особенно отрицательную роль сыграла его внутренняя служба [А. Коржакова - Г.П.]» («Столичные новости», 2001, 14 - 20 авг.). Это мнение конкретного лица, пост которого позволяет со всем вниманием отнестись к подобному высказыванию. По крайней мере, после ухода А. Коржакова выпущенная им книга действительно сыграла важную роль в создании отрицательного образа Ельцина, поскольку она сработала в модели резонанса, когда информация начинает подтверждать ходившие до этого в обществе слухи.

СЛУХИ + ИНФОРМАЦИЯ = РЕЗОНАНС

Кстати, при наличии слухов подлинная достоверность вводимой информации отступает на задний план. Это связано с тем, что слухи по сути своей представляют тот тип сообщения, который население на данный момент жаждет услышать.

Сам С. Филатов стал жертвой (опять же, в первую очередь, по его мнению) точечной операции, где информация вновь сыграла решающую роль. С одной стороны, в августе 1995 года его дочь задержали за спекулятивную перепродажу товаров, которая, как он считает, была инициирована А. Коржаковым. О чем написали газеты, и я как читатель помню и сегодня определенный шок, вызванный подобной информацией. С другой стороны, как он пишет, был и иной «выстрел»: «Примерно в декабре того же года в «Российской газете» появилась явно заказная статья под названием «Покровитель». Фамилия моя не называлась, но из нее совершению ясно следовало, что Филатов покровительствует евреям...

Вообще Россия дает массу разнообразных примеров информационных кампаний против своих государственных политических или экономических лидеров. И одновременно почти такое же количество опровержений. Например, руководитель Федеральной архивной службы России В. Козлов считает фальсифицированным известный дневник помощника М. Горбачева Анатолия Черняева, повествующий о форосском заточении президента СССР в августе 1991 г. («Версия», 2001, 31 июля - 6 авг.). Причиной подобной трансформации он считает попытку опровергнуть слухи о добровольной самоизоляции М. Горбачева.

Страны СНГ на сегодня все еще достаточно прохладно относятся к новым реалиям информационного общества, не проходит обучение даже с помощью такого явного информационного удара каким был и есть украинский «кассетный скандал». У нас нет академических институтов, работающим в этом направлении, мы все еще готовим специалистов исключительно одной сферы – журналистов. Они не являются аналитиками, они не могут разрабатывать информационные кампании, они не могут работать в области паблик рилейшнз. Все это следствие того, что власть продолжает оставаться непубличной: она никак не может выйти на процессы общения со своим народом, не умеет говорить не только о своих успехах, но и о своих провалах, которые не менее частотны.

Что имеется в мире по этим направлениям? Все страны ведут разработки по информационным войнам (по данным разведки (чужой) не менее 126 стран активно заработали в этой сфере). США имеют даже отдельные антипреступные и антитеррористические информационные программы, которые ведутся ЮСИА совместно с Министерством юстиции и ФБР. В США больше специалистов по паблик рилейшнз, чем просто журналистов. В 1995 году это соотношение составляло 150 тысяч к 130 тысячам. Отсюда следуют парадоксальные цифры, что 40% и более того, что мы получаем в качестве новостей на самом деле является результатом работы специалистов по паблик рилейшнз, то есть новостями сознательно организованными. Правда, в советское время мы, наверное, имели 99,99% новостей такого рода, и тут нам удалось обогнать даже Америку. Правда, по некоторым исследованиям и в США 70% сообщений имеют своим источником отнюдь не свободный поиск репортера. Это организованные пресс-конференции, сознательные утечки информации и под.

Что имеется, например, в Украине? Данная сфера лежит в области совершенно неуправляемой или некачественно управляемой со стороны государства. И государство должно в принципе поменять тип своего присутствия на информационном рынке, поскольку в его руках только 20% от всех СМИ. То есть стратегия информационного поведения государства должна стать совершенно иной, учитывающей эти совершенно иные реалии сегодняшнего дня. Пока единственной приметой нового стало создание Совета по информационной политике при Президенте Украины. А также новизну можно уви-

деть и в том, что в Концепцию реформирования политической системы, которая сейчас разрабатывается, закладывается отдельный раздел о роли СМИ в общественных процессах, в становлении открытого общества. Но всего этого явно недостаточно, поскольку мы имеем очень запущенную «болезнь» в своем информационном пространстве. Однако пока нет подготовки соответствующих специалистов ни в гражданских, ни в военных вузах, нет необходимой поддержки в академической среде. Болгария, например, имеет свой собственный журнал по информационной безопасности, не говоря уже о США, где выходят десятки книг, где военных переобучают новым реалиям информационной войны, которая меняет всю стратегию и тактику, наработанную в прошлом.

Сегодня мы очень чувствительны к политическим и экономическим темам нашей жизни, что отражается в определенном замораживании обсуждения этих проблем на национальном и региональном уровнях. Раз мы их не обсуждаем, то они консервируются и остаются с нами. Украина «боится» прямых телевизионных эфиров, трудных вопросов и нелегких ответов, все это ведет к процессам отторжения власти от населения, что результируется в падении рейтинга власти всех уровней. Хотя последние варианты теледебатов на украинских экранах показали большие возможности именного этого информационного жанра. Это были В. Филенко и Р. Бессмертный в «Табу» на ТРК «1 + 1». Это были С. Комиссаренко и Р Бессмертный, а также В. Долганов и М. Бродский на «СТБ в полночь». Нормальные собеседники, обладающие своими идеями, умеющие убеждать, они призваны изменить отношение украинца к политике и политикам. Кстати, пока никто, кроме Р. Бессмертного, не бросался так на амбразуру «кассетного скандала» со стороны власти.

Притчей во языцех стала критика УТ-1. Принимая все ее основные постулаты, следует иметь также в виду и то, что государственный канал несет на себе не только больший груз обязанностей, чем канал коммерческий (и потому они слабо сопоставимы друг с другом), но на нем лежит и больший груз «ценных указаний», поскольку число телефонов, способных позвонить сюда, гораздо больше. Все это выталкивает УТ-1 в совершенно иной формат, вызывающий огромный объем критических стрел в свой адрес. При этом следует также подумать и о том, что стрелы подобного рода летели всегда, кто бы ни возглавлял Национальную телекомпанию, поэтому здесь вина не персоналий, а избранной структуры. Возможно, что движение по пути к Общественному телевидению как раз и станет вариантом возможной реализации интересов всех задействованных при этом сторон. Однако принятый Закон об Общественном телевидении, требующий присутствия в наблюдательном совете представителей всех партий, при имеющихся ста с чем-то (а число их будет расти с каждым днем) партий в Украине делает невозможным функционирование подобного органа.

Что должно делать информационное пространство и чего оно не делает? Информационное пространство должно предоставить полигон для выдви-

жения и обкатки новых идей и новых лидеров, чтобы скамейка запасных игроков у нас не была удручающе маленькой. Информационное пространство должно давать полнокровную информацию о происходящих событиях, поскольку «кассетный скандал» продемонстрировал, что нет ни одного канала, который бы не освещал это событие с четким уклоном в одну или другую сторону. Как оказалось, у нас нет объективного освещения событий, поскольку все рассказы о происходящем шли только с восклицательным знаком. У нас вообще нет знака вопроса, журналисты всегда и все знают сами, практически не привлекая к анализу экспертов. Экспертное телевидение находится в зачаточном состоянии.

Государственные СМИ должны кардинально изменить характер своей работы, поскольку они находятся в меньшинстве: большая часть издания и телеканалов сегодня находятся в частной собственности. Они должны научиться давать качественный продукт, побеждающий в конкурентной борьбе информационный продукт другой стороны, как это имеет место, к примеру, в рамках работы службы коммуникации Белого дома. Данная служба даже координирует выпуск пресс-релизов всеми министерствами, чтобы все они не вышли, скажем, в пятницу, а в остальные дни администрация оказалась молчащей.

Информационное пространство призвано выполнять разные функции в зависимости от уровня, на котором это происходит. Можно выделить три отдельных уровня такого функционирования, каждый с совершенно разными задачами. Это уровни индивида, общества и государства.

Для индивида - речь должна идти о максимально открытом доступе к источникам информации, к знаниям в широком смысле этого слова. Каждое действие человека должно покоиться на обеспечивающей это действие информации, речь может идти о рекламе, коммерческой или политической, о прозрачности принятых решений органами власти, о полном информировании о происходящих в стране и за ее пределами процессах. Очень странным выглядит имеющееся до сегодняшнего дня полное отсутствие зарубежных корреспондентов у украинских СМИ, чего в принципе не может быть, поскольку мы всегда получаем из-за рубежа чужие интерпретации событий, а не свои. Значит, мы не формируемся как единый конгломерат граждан с единой точкой зрения на происходящие события.

Для общества - речь должна идти о возможности для каждой из политической или любой другой силы (например, общественной группы) иметь возможность высказать свою точку зрения. Региональные инетерсы как в той же мере общественно значимые, что и национальные, должны иметь возможность быть представленными во всей полноте. Новости не должны строиться в ущерб общественным интересам.

Для государства остается обеспечение функционирования всей информационной инфраструктуры, защита ее от информационных угроз и информационных атак. Государство должно вести свою собственную информационную

политику в максимально открытом режиме, обеспечивающим всем заинтересованным лицам доступ к той информации, которая предназначена для общественного использования. Только государство может обеспечить информирование зарубежной аудитории о происходящих в Украине событиях. То есть существует ряд функций, которые может выполнять только государство и которые на сегодняшний день никто не выполняет.

Основные параметры этих трехуровневых интересов можно суммировать в следующем виде:

Уровень	*Основные требования*
Индивид	Доступ к получению информации
Общество	Доступ к порождению информации
Государство	Эффективное функционирование всей системы

На сегодня эти уровни практически не работают. Индивид не имеет адекватной информации о происходящих в стране процессах. На экране и в печати он видит ограниченный круг лиц Новые идеи и тенденции не имеют возможности для выхода: они серьезным образом фильтруются СМИ вместо того, чтобы распространяться. СМИ сконцентрированы только на зрелищных событиях, во многом уходя в сторону от реальных проблем и болезней нашего общества. Отдельные лица (ученые, народные депутаты) почему-то мало интересны нашему обществу, хотя они несут за собой большой объем новых идей. Система СМИ, например, очень хорошо отражает жизнь попзвезд, но практически лишена интереса к реалиям тысяч людей. Например, с новыми идеями пытаются выйти к обществу народные депутаты М. Сирота, А. Чубатенко, Г. Балашов (каждый в отдельности). Но кто слышит эти идеи? Практически никто. Значит, что-то не так в датском информационном королевстве. Мы ставим заслоны там, где должно быть максимальное способствование распространению новых идей.

Каждые парламентские или президентские выборы информационное пространство начинает сотрясать множество противоречащих друг другу сил и требований. Возможно, это связано с непринятием таких подготовленных законопроектов, как "О политической рекламе", "О лоббировании" и многих других. Возможно с отсутствием нормального финансирования, которое может возникнуть только в системе работающей экономики. Сегодняшнее телевидение не может существовать за счет чисто телевизионных денег, зарабатываемых рекламой, поэтому оно содержится на «грязные» (из иных сфер)

деньги. Телевидение выступает в этом плане в качестве «переводчика» финансового капитала в политический, становясь средством влияния, которое в результате помогает решать экономические проблемы владельца финансовых потоков. Образуется следующий круг, идущий от винансов и к ним же возвращающийся.

Нам представляется что это особый вид информационного артера, определенная информационая феодальная система, которая пышным цветом расцвела на наших просторах. Возможно, это единственно правильный путь для сегодняшнего дня. Но одновременно это путь, который дает наилучшие результаты по искривлению информационного освещения в пользу интересов владельца финансов. Особенно ярко это продемонстрировала ситуация с НТВ, когда смена гендиректора, которая делается сегодня, поскольку акционерам неясно, куда пропадают десятки миллионов долларов, вызвала медиаскандал по всей стране. И даже мы, находясь на приличном отдалении, все равно слушали об этом скандале со всех украинских телеэкранов.

Сильная власть, сильная оппозиция и сильные СМИ являются обязательными атрибутами здорового общества. Если любой из этих компонентов будет слабым, то это сразу же деформирует общественную жизнь в стране. То есть и власть, и оппозиция должны быть заинтересованы в сильных СМИ. Для Украины это вдвойне важно, поскольку СМИ на сегодня являются единственным объединяющим всех граждан феноменом. СМИ позволяют вырабатывать интерпретации происходящих событий, способствуют порождению политической идентификации граждан, дают им возможные модели успеха, которые можно реализовать в данном обществе. Это очень серьезные задачи, которые никто другой не сможет решить адекватно и эффективно.

Анализируя причины распада СССР, Фрэнсис Фукуяма когда-то писал, что экономическое соревнование заставило Советский Союз выпустить на первые роли ученых, инженеров, поддержать сопутствующую им инфраструктуру образования, а у всех этих людей были иные представления о демократии, чем у партийных функционеров. То есть и хорошо работающая экономика также зависит напрямую от демократической структуры общества, которые во многом обеспечивается эффективно функционирующими СМИ. Украина сегодня с большими трудностями и с большим запаздыванием получает новые идеи, поскольку информационные потоки из других стран в виде книг и журналов старательно обходят Украину. Странно и то, что по причинам идеологического/политического характера Украина поставила заслон на вход русской научной книги (тот минимум, что есть покупается на базаре, что трудно себе представить в двадцать первом веке), хотя каждая такая книга заменяет финансирование целого отдела академического института. Если мы не можем заплатить за проведение исследований, то необходимо хотя бы облегчить покупку результатов этих исследований по цене бумаги, на которых они напечатаны. Сравните цену бумаги и цену годичной зарплаты отдела, и все станет понятно.

Информационная инфраструктура также способна ускорять прохождение определенных сообщений, а определенных тормозить, исходя из интересов данного общества. Она должна тормозить деструктивные идеи, задерживать распространение низкопробной халтуры, которую сегодня выдают за последние достижения украинской эстрады, воспитывая тем самым миллионы людей в рамках непонятных вкусов. Вообще в журналистской среде как-то исчезла профессия критика, хотя расцвела профессия «киллера». Мы вырастили уже добрый десяток профессионалов этого жанра способных переступать любые пороги. И не только «ради красного словца». Все это отражает новые типы задач, возникшие сегодня, но это задачи деструктивного свойства. Возможно, что со временем мы от них излечимся. Но после такого всплеска это будет трудно сделать. Прошлая специализация все время будет накладывать отпечаток на слова и действия журналиста, который волей или неволей сместился в несвойственную ему нишу.

Информационная инфраструктура общества должна развиваться, но это развитие было бы облегчено, если бы мы имели внятную и понятную всем, принятую всеми программу такого развития. В Украине должна быть создана соответствующая "Концепция реформирования информационной инфраструктура". Она должна определить несколько возможных точек, развитие которых осуществимо именно сегодня при недостаточном финансировании и при существенном столкновении политических и экономических интересов, имеющих место в сегодняшней Украине. Не имея такой концепции, мы будем вынуждены барахтаться в бесконечной череде проблем, плетясь в хвосте других стран, для которых информационная революция уже давно позади. Россия имеет Палату по информационным спорам, необходимость которой в рамках Украины также не вызывает сомнений. Мы должны самым тщательным образом собрать подобный опыт, чтобы реформировать свою собственную информационную инфраструктуру. Без ее адекватного функционирования будет невозможным дальнейшее экономическое, политическое, демократическое развитие Украины.

Новость как единица информационного пространства. Физическое пространство имеет свои пределы. Информационное пространство такого рода пределов не имеет. Оно бесконечно по возможностям приема все новой и новой информации. Бесконечное потенциально, оно имеет пределы, связанные с возможностями отдельного человека по переработке и запоминанию массивов информации. Оно в принципе может вообще существовать вне человека, потребляющего информацию, который может просто не заинтересоваться данным сообщением.

Информационное пространство активно структурируется понятием «новой/старой информации». Мы, к примеру, не читаем старые газеты, хотя информация там не является столь быстро устаревающей, как этого хочет сама индустрия по порождению информации. Мы структурируем информацию по важности/неважности для потребителя. Современная цивилизация также

жестко делит информацию на достоверную и недостоверную, где культура (высокая и массовая) порождают нечто в ином модусе, чем это принято по отношению к фактам.

Наложение физического пространства на информационное возможно только на отдельное сообщение, тогда возникает понятие начала-конца романа, фильма, телепрограммы. Но это параметры, продиктованные не с точки зрения информации, а сточки зрения ее носителя, который и имеет четкие физические ограничения.

Информационное пространство может члениться в процессе получения сообщения отдельным человеком. Тогда аналогом начала-конца физического плана может быть внимание-невнимание, запоминаемость отдельного сообщения. То есть границы информационного пространства возможны только с точки зрения отдельного человека и обусловлены чисто физиологически. Обойти эти границы пытаются привлечением внимания путем создания неординарных событий или оригинальных текстов.

Новость можно рассматривать как нормированное отклонение от нормы, в том плане, что новость не нарушает законы физического мира: люди, к примеру, не летают Новостью становится нарушение амплитуды ситуации, например, землетрясение или наводнение, которые явно выходят за пределы нормы. Военные действия также находятся за пределами нормы. Новостью становится начало-конец цикла: рождение человека, завода, партии и под. Собственно говоря, это то, что в прошлом первобытные племена маркировали своими обрядами инициации. Сегодняшнее общество маркирует определенные точки в бесконечном процессе действительностью с помощью превращения их в новость. Этот информационный продукт и направлен на фиксацию внимания массового сознания на значимых характеристиках происходящего вокруг. Тогда возникает понятная реакция, например, рождение теленка - не новость, рождение теленка с четырьма головами - новость. При этом новость не направлена на установление причинно-следственных отношений. Она сама по себе самодостаточна.

Эдвард Эпштейн предлагает еще такой критерий новости как относительная важность личностей, задействованных в событии (Epstein E.J. News from nowhere. Television and the news. - New York, 1973. - P. 144). Это действительно хороший параметр, но нам представляет, что он работает только для первых лиц. Список лиц следующих за ними столь велик, что не позволяет опираться на относительную важность этих персон. В этом случае рейтинг события будет важнее рейтинга персоны. Для первого лица все наоборот: присутствие первого лица делает из события новость первого ряда. Все остальные такой волшебной палочки превращающей события в новости, не имеют.

Новость позволяет управлять информационной пространством, поскольку информационное пространство чувствительно именно к новостям. «Дважды два - четыре» не является новостью, информационное пространст-

во отфильтровывает то, что уже содержится в нем, вынося на поверхность, с одной стороны, ненормированные события, с другой, события, значимые с точки зрения данного социума.

В чем отличие новости от романа, ведь и то, и другое лежат в плоскости виртуального мира. Новость сама по себе может быть менее виртуальной, но новость в рамках СМИ несет все приметы виртуальности, поскольку из миллиарда событий, происходящих в мире отбираются только тысячи. Обсуждению подлежат те условные десять новостей, которые попадают в информационную повестку дня, поскольку выделены в качестве первых по значимости для сегодняшнего дня. Процесс отбора колоссальным образом совершает процесс символизации новости, делая из нее не реальность, а модель реальности. Модель же в любом случае производит то или иное искривление реальности.

Новость, являясь элементом виртуального мира, отличается от других его элементом тем, что несет в себе максимальное число скрепов с действительностью. К примеру, комикс или роман мы уже не можем охарактеризовать подобным образом. Соответственно, «долгожительство» романа и новости различно, поскольку роман не привязан напрямую к действительности, он является информационной единицей и при другой реальной ситуации. Новость при изменении ситуации сразу же теряет свой статус новости.

Поскольку новость все равно отражает нормированный мир, поэтому она может быть как угодно малой, как это имеет место в сообщениях информационных агентств, так как потребитель информации знает, что такое землетрясение в принципе до того, как он услышит о землтерясении в какой-то стране в качестве новости. Новость в этом плане только указатель на стандартное отклонение от нормы в новой географической или временной точке. Статус новости сразу повысится, если в таком событии будут задействованы уроженцы страны зрителей или ее знаменитости, которые находились там в это время с визитом.

Массовая коммуникация возникает из процессов цикличности (периодичности) обновления информации об одном и том же объекте. Когда не было этой периодичности, возможны были рассказы о единорогах и под., поскольку не было возможности продолжить или опровергнуть данное сообщение. Затем возникает периодичность, например, первые газеты приноравливались к регулярности движения карет между городами.

Цикличность/периодичность и ее последствия меняют понимание новости, делая его таким, как мы привыкли рассматривать ее на сегодня. Таким образом, СМИ сформированы системностью, основой которой становится цикличность/ периодичность, позволяющая совершать постоянное обновление информации.

Художественная коммуникация не носит системного в этом плане характера. Герои редко переходят из романа в роман. А если это и происходит, то с потерей именно в художественности произведения, что показывает немногочисленный ряд продолжений романов.

Обновление информации в художественном произведении не носит бесконечный характер, все это связано с тем, что физическое пространство здесь ставит пределы пространству информационному - роман расположен на конкретном объеме страниц. Содержательно он также выстроен вдоль одного набора событий: детектив завершается раскрытием имени убийцы.

Художественная коммуникация в отличие от массовой стремится к процессу символизации происходящих событий. Символы человек не в состоянии обрабатывать на символическом уровне, для него требуется их материализация, которая позволяет остановить поток символов. Например, памятник «Родина-мать» или «Рабочий и колхозница».

Массовая коммуникация покоится на охвате все большего количества людей все более стандартизированными сообщениями. Чем больший объем получателей мы имеем, тем стандартизация становится явственнее. Отсюда объяснение клишированности языка СМИ, который не только видит мир сквозь ограниченный набор фреймов или стереотипов, но и на уровне формы рассказывает о нем языком клише.

Массовая коммуникация на сегодня оказалась единственным инструментарием, который позволяет охватить массовое сознание в ограниченный период времени. Художественная коммуникация может также позволить сделать это но за слишком долгий период времени. Но массовая коммуникация характеризуется и слишком динамичным обновлением своего фактажа, что постепенно привело к узко специализированным изданиям (типа журналов для кактусоводов или собирателей холодного оружия). Полное изменение фактажа в определеной степени разрушает системность восприятия этой информации. Она слишком разорвана, чтобы быть понятной. Мы, как в калейдоскопе перелетаем из страны в страну, чтобы затем задержаться на сводке погоды. Суммарная картинка мира имеет серьезную тенденцию к «разорванности», поэтому человек жаждет помощи в понимании ее, которую ему оказывают журналисты, политики, эксперты. Они становятся его гидами по этому слабо сводимому воедино миру.

Новость в структуре управления информационным пространством. Если новость является единицей информационного пространства, а управление им состоит в порождении новостей, то информационная борьба будет строиться на порождении нужого набора новостей, выталкивающих человека на определенные виды поступков. Это может быть дезертирство с поля боя или голосование за конкретного кандидата в президенты. Человек сделает этот выборы, опираясь на цепочку фактов, предоставленных ему.

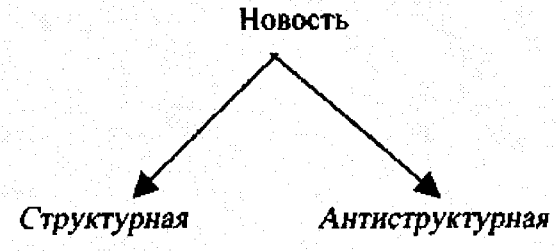
Иногда новость выбрасывается вперед, чтобы увидеть возможные варианты реакции массового сознания на этот новый вариант поворота события. То есть новость в данном случае служит не новостью, а определенной лакмусовой бумажкой. В другом случае новость вкладывается в уста менее иерархического лица, чтобы облегчить порождение этого же текста из уст первой особы. Например, можем привести такой пример, касающийся реак-

ции лейбористов в Англии на оборонные планы Америки: «В стане лейбористов пока царит неопределенность. В то время как премьер Тони Блэр, глава МИДа Робин Кук и министр обороны Джеф Хун стесняются открыто поддержать американскую инициативу, пресс-секретарь господина Блэра Алистер Кэмпбелл уже сказал, что план США - «хорошая идея». На что депутаты-лейбористы, большинство которых настроены против американских планов, а также лидеры консерваторов тут же заявили, что настоящим лидером Великобритании, оказывается, является вовсе не избранный премьер, а господин "Кэмпбелл" («Коммерсант. Украина». - 2001. - 8 мая). Кстати, американская реакция на это поведение премьера состояла в том, что Вашингтон остался недовольным его нерешительностью.

Новость является идеальной единицей, поскольку в ней как бы заинтересовано информационное пространство. Овладение искусством создания новостей становится ключом к управлению информационным пространством, поскольку новость это не то, что просто было показано по телевидению, а то, что в этом показе заинтересовало людей.

Одновременно новость является не автономной единицей, а кусочком, осколком картины мира. Новость, принимаемая в рамках данной картины мира, мы складируем в памяти не так, как новость, нарушающую картину мира. Летающий факир, к примеру, может согласовываться с нашей картиной мира только помещенный в раздел парадоксов.

С точки зрения информационной борьбы новость может носить структурный или антиструктурный характер, подразумевая под этим разделением то, работает ли новость на сохранение картины мира или пытается ее разрушить.



Новость как единица управления совершенно иным образом меняет акценты. Сегодня мы имеем дело с ИНФОРМАЦИОННОЙ ПОДГОТОВКОЙ, которая ведет к СОБЫТИЮ и завершается НОВОСТЬЮ. В случае полного управления этого мало. Акцент в этом случае должен стоять на ИНФОРМАЦИОННЫХ ПОСЛЕДСТВИЯХ (и не только информационных). С точки зрения советской системы в период перестройки в массовом порядке стали

порождаться антиструктурные новости, которые в результате приводят к разрушению структуры. Причем интересный парадокс заключался в том, что антиструктурные новости производили структурные СМИ, то есть СМИ внутреннего порядка, а не антиструктурные, под которыми можно было в тот период понимать зарубежные радиоголоса. Антиструктурные новости постепенно разрушают данную структуру мира, строя вместо нее новую.

Новость - это то, с чем имеют дело потребители информации. Однако в голове у них стирается то, что это на самом деле не подлинное событие, а его в определенной степени модельное представление. Потребителю информации представляется, что он имеет доступ именно к новостям как аналогу события. Именно в этом заключается интерес любых политических игроков к информационному пространству. Но аналога событию в информационном пространстве нет и быть не может из-за разной природы пространства реального и информационного.

Правда, следует сделать одно ограничение, отмеченное Ф. Тэйлором. Исследования, проведенные в Лидском университете по вопросу освещения войны на телеэкране, привели его к выводам, что новость по сути является не столько окном, сквозь который мы видим мир, а зеркалом (Taylor P.M. Global communications, international affairs and the media since 1945. - London etc., 1997). Получается следующее: публика получает ту , в данном случае, картинку войны, которая сама хочет увидеть. Если она не хочет видеть раненых, грязь и кровь, то СМИ ей этого не покажут Утрируя, можно продолжить эту тенденцию, что если публика хочет увидеть победу, она увидит победу, если поражение - то поражение

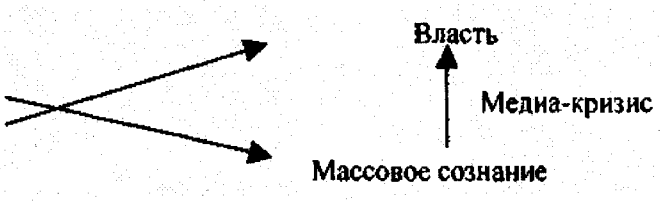
Структурные новости подтверждают имеющиеся у нас в голове представления о структуре мира, антиструктурные новости призваны перевести нас на новую картину мира. Вероятно, работе на последнем направлении серьезную помощь может оказать такое направление, как когнитивная терапия.

Отсюда следует важный вывод: теперь мы должны и на СОБЫТИЕ, и на НОВОСТЬ смотреть только и исключительно с точки зрения последствий. С точки зрения планировщика последствия сильнее любой новости и даже самого события. Это связано с тем, что и само событие и последующая за ним новость возникают в реальном мире только из-за нужды в данном виде последствий.

Медиа-кризис как катализатор. Информационная кампания может быть направлена как на одного человека, так и на все общество. Примером первого рода является информационная операция, в свое время инициированная Ю. Андроповым по воздействию на лидера итальянских коммунистов Э. Берлингуэра, который был заинтересован в поддержке Тито. На охоте в Завидово в мае 1979 г. Брежнев спросил у Тито, зачем он связался с неизвестно с кем, с пацанами, которые придумали какой-то еврокоммунизм. На что Тито ответил, что не может быть регионального, местечкового коммунизма, что еврокоммунизм - это евроглупость. Это сообщение направили в сторону

Берлингуэра тремя разными путями, чтобы увеличить их достоверность. В результате было достигнуто то, что и планировалось: разделение лидеров на годы, которое было вызвано сознательно проведенной информационной операцией. А Советский Союз мог не бояться объединения возможных лидеров еврокоммунизма. Медиа-кризис представляет собой такое же негативное событие, развертываемое ради воздействия уже не на индивидуальное, а на массовое сознание, но также осуществляемое, чтобы получить результаты, нужные именно коммуникатору.

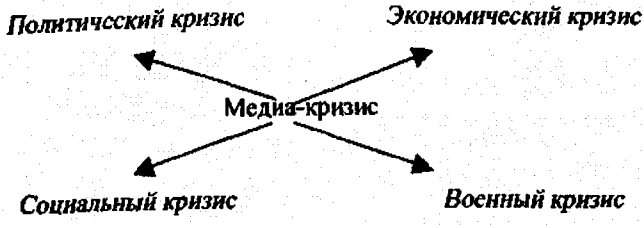
Медиа-кризис как кризис, проходящий в медиа-пространстве и необязательно соответствующий кризису в реальной жизни, активно используется в современных условиях. По сути любая демонстрация является попыткой «надавить» на власть с помощью силы улицы, которая всегда получает адекватное освещение в СМИ, тем самым осуществляя медиа-давление на власть и массовое сознание.



Власть при этом получает двойное давление: как со стороны медиа, так и со стороны массового сознания, которое также получило удар со стороны медиа.

Перед нами за последнее время прошли три активно разворачиваемых медиа-кризиса, в которых мы были хотя и пассивными, но участниками: раскрутка гибели «Курска», раскрутка «кассетного скандала», раскрутка смены руководства НТВ. Все они пришлись на близкий период времени, измеряемый одним годом. Поэтому вполне обоснованно можно искать в них общие черты. Среди них можно найти следующее: включение как можно большего числа участников (в данных примерах телевидение, власть, военнослужащие являются объектами, которые затрагивают всех), выведение на нападение всех, обвинение власти, обвинение защитников власти (объект воздействия всегда стремяться отсечь от союзников), постоянная смена ракурса, выступающих информационных объектов (в «кассетном скандале" – палатки, митинги, демонстрации, в случае НТВ митинги, встречи, прекращение вещания). Все это создает интенсивную информационную кампанию в которой каждый зритель может найти нечто для себя, поскольку «меню» сознательно делается максимально многоплановым.

Медиа-кризис интересен для тех, кто его создает, не сам по себе, а по типам возможных последствий, на которые он выталкивает. Последствия могут быть в политической, экономической, социальной, военной сферах.



И поскольку действие разворачивается ради воздействия на массовое сознание, то обязательным компонентом становится разработка определенной мифологии, легенды. Этот процесс можно обозначить как легендирование. Например, в случае бомбардировок в Югославии развернутый медиа-кризис говорил о сербах как о проводящих этнические чистки, чем восстанавливалась отсылка на фашистов. Было объявлено о ста тысячах могил, из которых потом удалось обнаружить только три, да и то этническую принадлежность трупов установить невозможно.

Медиа-кризис подчиняется определенным закономерностям, призванным удерживать внимание массового сознания. Можно перечислить следующие закономерности:

- драматургическое развертывание, где всегда есть герои и злодеи, первые - красивы и благородны, вторые - ужасны и отвратительны,
- зрелищность (в случае «кассетного скандала» такими примерами были стакан крови перед МВД, сожжение чучела и под.), все это типы событий, которые пересказываются для тех. Кто их не видел или не слышал о них, тем самым резко расширяется число потребителей данной информации,
- переключение внимания: медиа-кризис уводит внимание на тот аспект события, при этом гиперболизируя его, который может не быть приоритетным для аудитории, — асимметричность информационных атак, что особенно характерно для украинского «кассетного скандала», который пытается управлять вниманием массового сознания по аналогии с известным движением Гринпис.

Еще одной особенностью медиа-кризиса является перевод стрелок из одной плоскости в другую. В рамках него, как правило, уголовная плоскость сразу становится политической, экономическая сфера (как в случае НТВ) переводится в угрозу свободе слова и под. То есть происходит перевод в сторону, которая представляет большее поле для воздействия на аудиторию. У каждой аудитории есть свои точки уязвимости: управление медиа-кризисом состоит в постоянном возвращении именно к данным точкам, уводя при этом от тем, выгодных для противоположной стороны.

Медиа-кризис также активно эксплуатирует чувство страха. Пытаясь расширить число участников, все строится на том, чтобы поставить потреби-

теля информации, который отдален от эпицентра кризиса, в самую его сердцевину. По законам психологической войны нельзя максимализировать страх, если не давать путей того как его избежать. Например, в листовках о самой большой бомбе которая должна была быть сброшена на иракских солдат, обязательно подчеркивалось, что можно избежать гибели, если вовремя покинуть расположение части.

Медиа-кризис активно работает и над тем, чтобы приглушить рациональный компонент, активно эксплуатируется только эмоциональный компонент. Одним из примеров такого рода является проведение митингов в вечернее время, когда внимание слушателей ослабевает. Увеличение эмоционального компонента также можно увидеть в привлечении для воздействия известных персоналий, что хорошо видно на примере раскрутки ситуаций с НТВ. Митинг является принципиально эмоциональным полем, поскольку в нем нет места рациональным аргументам. Митинг разрешает бесконечное повторение, митинг требует от толпы грубо дифференцированных реакций: только «за» или «против». Никакие другие варианты неинтересны. Это связано с тем, что в двадцатые годы, предшественник кибернетики А. Богданов назвал выравниванием по низшим реакциям. Толпу можно выравнять только по ним, только они являются общими для всех, поскольку высшие реакции у всех разные.

В целом медиа-кризис действует по типу воздействия, придуманного в годы «холодной войны», когда неудовлетворенность одного сегмента аудитории переносилась на все общество. Например, свобода слова, значимая для интеллигенции, но не столь значимая для рабочего класса, продиктовывалась как болевая точка именно рабочему классу. И вся страна начинала обсуждать проблему свободы слова, хотя она не была приоритетной для всех. Та же модель имеет место во всех трех вариантах развернувшихся перед нами медиа-кризисов, которые во всех трех случаях были направлены против власти, что также объединяет их в единую группу.

Как перестройка оказалась возможной только с подключением гласности, которая интенсифицировала информционные потоки в нужном направлении, так и медиа-кризис строится на активной эсплуатации медиаструктур современного обшества. Очень часто при этом используется квазиинформация, под которой будем понимать непроверяемый фактаж. квазиинформация выдается за подлинную информацию, затем вся аргументация строится именно на ней. Сразу происходит переходит на одну интерпретацию данного события, которая становится базовой, все другие интерпретации даже не упоминаются, они отбрасываются как недостоверные, хотя в реальности это не так. Весь медиа-кризис разворачивается в плоскости, навязанной вводимой Квазиинформацией. И она уже не подвергается сомнению, что напоминает невозможность ответа на вопрос в виде «да» или «нет», когда вопрос сознательно сконструирован (типа «Часто ли вы бьете свою жену?», «Перестали ли вы воровать книги из библиотеки?»). Здесь негатив заранее

задан как непререкаемый факт, а все обсуждение будет вестись лишь в области объема этого негатива.

Медиа-кризис очень тяжело распознается аудиторией как искусственный, как неадекватный действительности, поскольку аудитория привыкла воспринимать сообщения СМИ только в формате правды. Он точно просчитан на точки уязвимости своей аудитории. Говорящий человек также располагает к тому, чтобы стать на его точку зрения из-за эмоциональности его воздействия. *Медиа-кризис взрывает медиа-бомбы, от которых практически нет защиты.* В случае украинского «кассетного скандала» он не имел последствий в виде стопроцентного захвата на свою сторону населения по одной простой причине. В теории пропаганды есть одно аксиоматическое положение: когда аудитория получает только позитивную информацию, то приход негативной информации, полностью меняет ее точку зрения. Когда же аудитория получает как позитивную, так и негативную оценку, то в этом случае введение негативной оценки уже не так болезненно, поскольку аудитория имеет против нее «прививку».

Медиа-кризисы придуманы не нами, но нам с ними надо уметь бороться. Поэтому первоочередной задачей украинского общества должно быть создание соответствующих структур по подготовке специалистов в рамках Министерства образования, по разработке академической науки в этом направлении в рамках Национальной академии наук, подготовке и работе специалистов по информационной борьбе в рамках Министерства обороны. Уроки медиа-кризисов должны быть пройдены не зря.

Сменковский А.

МЕТОДЫ ДВОЙНОГО ВОЗДЕЙСТВИЯ В МЕЖГОСУДАРСТВЕННЫХ ЭКОНОМИЧЕСКИХ ОТНОШЕНИЯХ

Неотвратимость участия социально-экономических систем в глобализационных процессах, усиление взаимозависимости национальных экономик и их подверженности влиянию наднациональных структур - как политических, так и экономических - исключают целесообразность каких бы то ни было дискуссий об участии в этих процессах в принципе. Речь должна идти о другом: каким образом обеспечить реализацию национальных интересов в таких условиях? Как максимально использовать колоссальные положительные возможности, предоставляемые глобализацией мирохозяйственных связей, и одновременно нейтрализовать ее не менее масштабное деструктивное влияние? Какую модель экономического развития и участия в международном разделении труда избрать? Представляется, что непредвзятый анализ возможных вариантов адаптации национальной экономики к тенденциям мирового развития более конструктивен, чем его огульное отрицание каким-нибудь идеологическим штампом вроде "безальтернативности интеграции в мировое экономическое сообщество".

Ибо в такого рода заклинаниях присутствует подмена понятий. Речь идет не об отрицании интеграции, а именно об анализе альтернативных форм ее осуществления и принятии на его основе оптимального решения.

Ниже рассмотрим аспект международных экономических отношений, связанный с деятельностью международных финансовых организаций, и в первую очередь - Международного валютного фонда (МВФ). Анализ последствий его политики в разных странах тем более важен, что на протяжении ряда последних лет согласованные меморандумы украинского правительства и МВФ фактически являются "экономической конституцией" Украины и выполняются куда последовательнее, чем, например, программы действий Кабинета министров.Официальные цели МВФ, зафиксированные в ратифицированных в 1945 г. Статьях Соглашений о МВФ и МБРР, предусматривают "благоприятствование международному валютному сотрудничеству", "расширению и сбалансированному росту" международной торговли; обеспечение "благоприятных отношений в валютной сфере между странами-членами"; недопущение "конкурентного обесценения валют"; предоставление помощи в создании многосторонней системы платежей по текущим операциям между странами-членами и в устранении валютных ограничений; предоставление странам-членам средств в иностранной валюте, которые позволяли бы им "исправлять нарушения равновесия их платежных балансов"; "сокращение продолжительности и уменьшение степени неуравновешенности международных платежных балансов стран-членов" [Articles of Agreement of the International Monetary Fund. // Washington: IMF, August 1985. - P.2-3.].

Таким образом, изначально МВФ предназначался для адаптации стран-членов к либерализации внешней торговли. Ключевой же задачей стало недопущение "конкурентного обесценения валют" (которое, как известно, является наиболее эффективной мерой улучшения сальдо внешней торговли), что предполагалось компенсировать предоставлением кредитов на поддержание торгового баланса.

(Заметим, что развитые страны, и в первую очередь США, никогда не придерживались этих принципов. Во все время существования МВФ то и дело вспыхивали "торговые войны", связанные с искусственным снижением курса той или иной валюты. Политика МВФ приобрела таким образом "экспортный" характер и была нацелена на развивающиеся страны).

Однако в этих странах МВФ столкнулся с куда более разнообразными методами протекционизма во внешней торговле, чем в развитых рыночных экономиках - от тарифных и нетарифных барьеров до регулирования себестоимости и прямой государственной поддержки экспортных производств. Видимо, именно поэтому МВФ воспринял монетаристские идеи так называемого "Вашингтонского консенсуса", а именно: устранение государства от хозяйственной деятельности; осуществление ограничительной денежной политики с целью сокращения темпов инфляции, автономизация центральных банков; минимизация бюджетного дефицита, сокращение бюджетных расходов

(прежде всего на социальную защиту и финансирование экономики); приватизация объектов государственной собственности; устранение барьеров внешней торговли; либерализация обменных курсов, и тому подобное. С этого момента политика МВФ окончательно приобрела двойственный характер, а задекларированные благие цели начали разительно отличаться от содержания программ финансовой помощи и полученных результатов. Впрочем, главная цель МВФ осталась прежней: лишить государства каких бы то ни было возможностей смягчить последствия либерализации внешней торговли.

На достижение названной основной цели (прямым или косвенным путем) направлены все прочие требования, особое место среди которых является ограничительная антиинфляционная политика. Представляется, что борьба с инфляцией в арсенале мер МВФ играет не только экономическую, но и важную пропагандистскую роль. С одной стороны, инфляция - одна из острейших социально-экономических проблем, непосредственно ощущаемых каждым человеком. С другой - методы противодействия инфляции просты (достаточно лишь ограничить рост денежной массы, а возникающие вследствие этого негативные явления - такие как рост задолженностей по зарплате и социальным выплатам - подавляющим большинством населения не рассматриваются как результаты антиинфляционной политики). Попытки же национальных правительств с целью оживления производства и внутреннего рынка смягчить рестриктивную денежно-кредитную или бюджетную политику немедленно дискредитируются обвинениями в раскручивании инфляционных процессов.

Важная роль отводится и лоббированию массовой приватизации. Причем предварительно с помощью вышеперечисленных инструментов стоимость приватизируемых объектов государственной собственности искусственно снижается (в ряде случаев - намного ниже рыночной).

Сегодня общепризнанным фактом являются крайне негативные результаты практической реализации этой политики во всех странах, в разное время легкомысленно прибегавших к помощи МВФ. Для иллюстрации причин ее разрушительности воспользуемся опытом Аргентины, которая, как правило, считается образцом удачного применения монетарной теории на практике [Argentina's economic reform program: relevance to Ukraine. 10/10 policy note #9. // The World Bank. - June 19, 1998.].

Программа либеральных реформ в этой стране была объявлена в марте 1991 г. министром экономики Доминго Кавалло. Она предусматривала реализацию стандартного набора рекомендаций МВФ, но ее главной составной частью была реформа денежно-кредитной системы, в том числе - введение режима "валютного комитета" (currency board) и жесткой привязки национальной валюты к доллару США. После денежной реформы весь объем национальной валюты был на 100 процентов обеспечен резервом иностранной валюты, для чего привлечены огромные кредиты банков США и мировых финансовых организаций. Фактически была введена бимонетарная система со

свободным обращением доллара, а прирост денежной массы поставлен в зависимость от прироста валютного резерва. Закон о центральном банке в сентябре 1992 г. ввел независимость совета директоров ЦБ от правительства. Право девальвации национальной валюты было изъято у министерства экономики и передано конгрессу, что сделало практично невозможным ее проведение.

На первый взгляд, темпы роста ВВП и успехи в преодолении инфляции в Аргентине впечатляют. (Хотя нельзя обойти вниманием тот факт, что самый высокий темп экономического роста наблюдался в 1991 г. - до начала реформы Кавалло, при темпе инфляции 84%). Но глубинная суть "аргентинского чуда" состоит в том, что валюта, необходимая для поддержки фиксированного курса песо, поступает в страну в виде иностранных кредитов и немедленно ее покидает благодаря огромному отрицательному сальдо внешней торговли, а последнее, в свою очередь, стимулируется завышенным курсом национальной валюты. Образовывается "замкнутый круг", а в "чистом остатке" остается задолженность по кредитам и процентам. Строится хорошо нам известная "долговая пирамида", первый обвал которой в Аргентине состоялся в 1995 году. В 1996 г. внешний долг страны достиг 93,8 млрд. долларов, а в 2000 г. - 120 млрд. долларов, что составляет 23% рынка долгов развивающихся стран. Мировой финансовый кризис 1997-1998 гг. нанес очередной сокрушительный удар аргентинской экономике, после чего она до сих пор не может выбраться из затяжной депрессии.

Особенно показателен тот факт, что крах экономической политики Кавалло в 1995 году не привел к отказу от нее, поскольку к тому времени страна (благодаря "currency board") лишилась остатков экономической независимости и была намертво посажена на "иглу" внешней помощи. Более того - спасение безнадежно больной аргентинской экономики в 2001 г. поручили тому же Д. Кавалло.

Известно, что страны Восточной Европы, первыми преодолевшие трансформационный кризис, в свое время сумели вовремя отказаться от выполнения рекомендаций МВФ. Среди стран же СНГ дольше и болезненнее других выходили из кризиса Россия, Украина и Молдова, наиболее последовательно и ортодоксально следовавшие этим рецептам.

Между тем реформы, проводившиеся, например, в Молдове, в свое время получили высокую оценку западных средств массовой информации. "Молдова - модель правильного реформизма - твердо собирается встать на путь оздоровления после экономического кризиса... Правительство, пользующееся репутацией реформистского, ...заслуживает положительных оценок и поддержки" ("Economist", март 1995 г.); "Молдова, по-видимому, действует лучше, чем многие другие бывшие советские республики, в построении политической демократии и рыночной экономики. США, Всемирный банк и Совет Европы оценивают ее реформаторские усилия как пример для экс-коммунистических стран" ("Washington Post", май 1996 г.).

С этими хвалебными оценками поразительно контрастирует характеристика результатов экспериментов МВФ в Молдове, данная другой международной финансовой организацией - Европейским банком реконструкции и развития - в 1999 году, когда их последствия проявились в полной мере: "Молдова - одна из беднейших стран Европы с высоким и возрастающим уровнем бедности и сокращающейся средней продолжительностью жизни. Система социальной защиты ощущает острый недостаток средств... Это подрывает системы образования и здравоохранения, а также другие области социальной сферы. Из 28% безработных согласно оценкам только 4% зарегистрированы и получают пособия" [Процесс перехода и экономические показатели стран СНГ. // ЕБРР, ноябрь 1999 г. - С. 39.].

Результаты радикальных рыночных реформ в Молдове, проводившихся в полном соответствии со стандартными рецептами международных финансовых организаций, налицо: спад производства продолжается, за чертой бедности оказалось 65% населения. Правительство М. Снегура, "пользовавшееся репутацией реформистского", бесславно ушло в отставку. А недавно монетаристские эксперименты закончились закономерным финалом: к власти триумфально вернулись коммунисты.

Еще *один свежий пример очередной "победы"* МВФ - *крах экономики* Турции. Обеспокоенное высокими темпами инфляции (которые, впрочем, не мешали экономическому росту), правительство страны объявило программу финансовой стабилизации, предусматривавшую известный "джентльменский набор" либерал-монетаристских мер: поддержку номинального обменного курса, повышение процентных ставок, приватизацию объектов государственного сектора экономики и т.д. В результате в экономике страны обострились кризисные явления. Ухудшилось сальдо торгового баланса, внешний долг по "аргентинской" схеме возрос до 110 млрд. долларов. 17 ноября 2000 г. в ответ на решение правительства проверить деятельность крупнейших банков, подозреваемых в "отмывании" денег, из страны сбежало 7,5 млрд. долларов иностранных инвестиций! Кульминацией нарастания кризисных явлений традиционно стал крах фондового рынка. Один за другим начали разоряться коммерческие банки (12 из 80 банков страны оказалось на пороге банкротства). Только за один день в марте 2001 г. индекс стамбульской биржи обвалился более чем на 30%. Сразу после этого с точностью повторился "синдром 17 августа" на валютном рынке. На протяжении одного дня банки скупили 7,6 млрд. долларов! Центральный банк Турции некоторое время пытался поддерживать курс лиры, истратив за неделю 4,5 млрд. долларов (треть валютных резервов), но потом отказался от этих потуг, поскольку, согласно заявлению ЦБ, "попытки стабилизации курса оказались недейственными и не способными удерживать рост спроса на доллары и восстановить уровень уверенности бизнеса и потребителей" [Президентский вестник, 2001, №12.].

Но для выхода из кризиса турецкое правительство не обнаружило ничего лучшего, чем снова обратиться за помощью МВФ!

Результаты реформ, осуществляемых по монетаристским рецептами, рикошетом бьют и по репутации МВФ, выступающего в качестве соавтора и спонсора этих реформ. Международная группа экспертов "Адженда-92" дала рекомендациям МВФ такую характеристику: "Предложенный МВФ путь развития восточноевропейских государств - это новая ортодоксальная идеология. Никогда и нигде в истории капитализма рынки не возникали спонтанно. Этот тезис подтверждает пример восстановления Европы после Второй мировой войны и экономический взлет Японии, которые основывались на государственном управлении и осторожной приватизации. Ни одно "экономическое чудо" не состоялось бы, если бы послевоенная Европа или Япония следовали рекомендациям МВФ, как это делают сейчас восточноевропейские страны" [Деловой мир. - 1992. - 2 июня.]. 7 мая 1992 г. представители департамента МВФ по связям с общественностью Х. Пуэнтес и М. Сигер на встрече с журналистами признали, что эксперты Фонда не обладают достаточным опытом перевода командно-централизованной экономики в рыночную и потому не исключают возможности ошибок в своих рекомендациях [Смыслов А. Международный валютный фонд: современные тенденции и наши интересы. // М.: Финансы и статистика, 1993. - С. 218.].

Тем не менее следует отметить, что неоднократные признания представителями МВФ или Всемирного банка ошибочности своих рекомендаций не приводят не только к их радикальному просмотру, но даже к минимальному корректированию. Наоборот, специалисты, которые более других руководителей МФВ и Всемирного банка отличались здравым смыслом, были вынуждены покинуть свои посты. Так, в последнее время оставили должности первый заместитель директора-распорядителя МВФ Стэнли Фишер, главный экономист МВФ Майкл Мусс, первый вице-президент и главный экономист Всемирного банка Джозеф Стиглиц. Даже убежденные монетаристы все чаще высказывают неудовольствие деятельностью МВФ и Всемирного банка. "МВФ стоит на раздорожье, со слабым руководством, слабыми познаниями в экономике и слабой поддержкой стран-участниц. Сочетание букв МВФ стало уже обычным, но получило неблагоприятный подтекст. Спросите любого пятикурсника о МВФ, и вы услышите очень обширную, но неизменно отрицательную характеристику", - заявил, например, Р. Дорнбуш, в свое время бывший главным экономическим советником МВФ и Всемирного банка [День, 2001, 23 мая, №89. - С.4.].

Впрочем, представляется, что ссылка на низкую квалификацию специалистов МВФ на самом деле является лишь попыткой отвлечь внимание мировой общественности от истинных задач, стоящих перед его руководством. Квалификация же исполнителей оказалась достаточной, чтобы поставить под полный контроль международного капитала экономики целого ряда стран. Как указывалось выше, международные финансовые организации в своей деятельности руководствуются мотивами, отличающимися от задекларированных, а именно - утверждением в странах "третьего мира" экономического порядка, выгодного мировым лидерам.

Ответственность за результаты политики МВФ легче всего было бы возложить на национальные правительства, так как именно они обращаются за финансовой помощью. Но и здесь используются механизмы двойного воздействия, крайне усложняющие проведение самостоятельного экономического курса.

Во-первых, психологически верно делается ставка на компрадорскую часть местной элиты, не способную устоять перед соблазном доступа к "дешевым" кредитам. Во-вторых, создается целая сеть "исследовательских центров", привлекаются средства массовой информации, ориентированные на "мобилизацию" этой части элиты, установление контактов с государственными чиновниками, пропаганду либерал-монетаристских идей.

Бывший советник по вопросам государственной политики в России, а ныне - руководитель Стокгольмского института экономики переходного периода Эрик Берглойф так описал требования, предъявляемые к подобным организациям: "большое значение имеет критическая масса... Относительно качества проводимых исследований не должно быть никаких компромиссов. Между качеством проводимых исследований и их конкретной значимостью для политического процесса нет никакого противоречия. Напротив, качество исследований государственной политики особенно важно: правительственные чиновники должны принимать решения, основываясь на высококачественных исследованиях. Другие задачи, например, налаживание контактов, должны решаться отдельно; каждая инвестиция в развитие способностей должна учитывать не только конкретные особенности исследователя или института, но и их взаимосвязь с общей политической ситуацией на мировой арене" [Берглойф Э. Как прекратить процесс "утечки мозгов" из стран с переходной экономикой? - Трансформация, 2000. - №3-4. - С.31.]. За облаченной в характерную для западных специалистов форму "новояза" фразеологией скрывается описание хорошо известного механизма влияния международных финансовых организаций на национальные элиты и политический истеблишмент.

Для проникновения международных финансовых организаций в сферу принятия решений на национальном уровне сегодня используются самые современные манипулятивные технологии.

1. **Абсолютизация источника информации и прикрытие авторитетом.** Рекомендации МВФ "подкрепляются" научным "весом" адепта монетарной теории, Нобелевского лауреата Милтона Фридмена, одновременно замалчиваются или дискредитируются критические оценки этой теории, высказываемые другими видными экономистами. Пропагандируются "успехи" монетаристской политики (чилийская, аргентинская модели, "шоковая терапия" по-польски, и т.д.), при этом игнорируется "обратная сторона медали".
2. **Тоталитаризм решений.** С самых высоких трибун раздаются утверждения наподобие "альтернативы сотрудничеству с международными финансовыми организациями не существует".

3. **Некогерентность утверждений.** Например, часто приходится слышать о том, что приход иностранных инвесторов непосредственно зависит от сотрудничества той или иной страны с МВФ. Между тем иностранных инвесторов привлекает возможность получения дохода, и МВФ тут ни при чем (скорее наоборот - он своими требованиями ухудшает условия для инвестирования, что было недавно доказано экспертами Украинского союза промышленников и предпринимателей и озвучено на съезде этой организации).
4. **Изъятие из контекста.** Так, инфляция объясняется сугубо денежными факторами, при этом игнорируются или отвергаются другие причины, такие как административные повышения цен.
5. **Создание образа врага.** Специалистам, взвешенно оценивающим эффективность сотрудничества с международными финансовыми организациями, навешиваются различные ярлыки - от "ретрограда" до "антирыночника".
6. **Активизация стереотипов.** Например, боязнь инфляции широко используется для дискредитации в общественном сознании нежелательных для МВФ вариантов национальной экономической политики ("нас опять хотят отбросить в 1993 год").

Между тем анализ политики, проводящейся под давлением МВФ на основе использования монетарной теории, позволяет утверждать, что она всегда характеризуется четко выраженной антисоциальной направленностью, сопровождается углублением структурных деформаций, погружением стран-реципиентов в болото внешних долгов. Учитывая это, циничными выглядят восторженные оценки монетаризма со стороны некоторых украинских экономистов: "Вся теория монетаризма проникнута заботой о создании самых лучших условий для всех экономических агентов общества (товаропроизводителей и потребителей). Но, подчеркиваем, для свободных, хорошо защищенных и, прибавим, для высокообразованных и законопослушных экономических агентов общества" (выделено в тексте. - А.С.) [Ющенко В., Лисицкий В. Деньги: развитие спроса и предложения в Украине. - К.: Скарби, 1998. - С.283.].

Обобщая вышесказанное, стоит заметить, что для повышения эффективности экономических реформ отечественным политикам целесообразно было бы не бездумно руководствоваться рекомендациями западных школьных учебников и не насаждать в Украине новации, примененные ранее в совершенно иных социально-экономических условиях и с более чем сомнительными результатами, а формировать экономическую политику с учетом местных реалий и анализа как положительных, так и отрицательных результатов реформ в соседних странах. Такую политику следует последовательно и настойчиво отстаивать на переговорах с международными финансовыми организациями (а не торговаться о мелочах, подписывая полные и безоговорочные капитуляции по всем стратегическим позициям).

Равным образом следует учитывать, что альтруизм не является свойством современных международных отношений. Их направляют правила жес-

точайшей конкуренции, а главная роль в экономическом уничтожении конкурентов отводится именно международным финансовым организациям.

Наконец, еще одно наблюдение, могущее сыграть определенную роль в переходе к более ответственным отношениям с международными финансовыми организациями: рано или поздно все правительства, исповедовавшие ортодоксальные либерал-монетаристские идеи, бесславно уходили с политической сцены.

Хант Ч. Зартарьян В.
РАЗВЕДКА - НЕРВ ЭКОНОМИЧЕСКОЙ ВОЙНЫ. ЭКОНОМИЧЕСКАЯ ВОЙНА*

Утверждения о разрушении и захвате японцами целых отраслей промышленности превратились уже в банальный штамп. Так, если взять производство фотооборудования, то во Франции и в Великобритании уже не осталось ни одного производителя любительских фотоаппаратов, а в ФРГ еще остающиеся на плаву доживают свои последние дни. В области производства мотоциклов в Западной Европе и в США осталось только несколько фирм, занимающихся производством машин специального назначения. Что касается бытовых электронных товаров широкого потребления, то уже сейчас крайне трудно купить высококачественный магнитофон или проигрыватель не японского производства. В ближайшее время наступит, по-видимому, черед средств информатики и автоматизации, телевидения высокой четкости и автомобилестроения. Но на этот раз японцы были столь любезны, что предупредили нас: "В области автомобилестроения выживут только пять крупных концернов: три японских и два западноевропейских", заявил недавно президент фирмы "Nissan" (Япония). Следует отметить, что наступление уже идет полным ходом, так как периферийные рынки (Африка, Ближний и Средний Восток, Юго-Восточная Азия) уже захвачены японцами. Именно поэтому Эдит Крессон, бывший министр внешней торговли, а сейчас премьер-министр Франции, заявила: "Я констатирую, что в ряде областей промышленности мы находимся на грани национальной катастрофы и при этом по-прежнему ничего не предпринимаем. Как же мы до этого дошли? "

После Второй мировой войны США, а вслед за ними и Западная Европа, безраздельно господствовали в мировой экономике. Затем пробил час деколонизации и быстрого роста мощи новых стран - Японии и четырех азиатских драконов (Южной Кореи, Тайваня, Сингапура, Гонконга). Нефтяной кризис 1973 г. на некоторое время замаскировал этот новый расклад сил. Кризис роста валового национального продукта в западных странах был отнесен на счет ОПЕК, то есть вместо объективного анализа ситуация объясня-

* Фрагмент из книги «Разведка на службе вашего предприятия» // Скиба Н.Е., Малыгин А.В., Бондаренко Е.И. Информационные войны. Хрестоматия

лось стремлением ОПЕК к получению сверхприбыли. Однако азиатские страны, энергетика которых находится еще в большей зависимости от внешних поставок, очень быстро оправились от кризиса. И только тогда Запад осознал, что ситуация в чем-то изменилась. Следует однако, отметить, что сигналов - предвестников было вполне достаточно. Так, начиная а 60-х годов, японские товары начали захватывать американский рынок. Вначале крупные американские компании с презрением и пренебрежением наблюдали за этим процессом, считая, что потребители быстро пресытятся этими дешевыми недоброкачественными товарами - побрякушками. В этом и заключалась их ошибка! Технико-экономический анализ позволил японцам определить наиболее выгодные виды товаров, а их до сих пор непревзойденное владение процессами производства позволило в конце концов разгромить конкурентов.

Однако и после этого мы продолжаем оставаться слепыми вплоть до настоящего времени, ярким доказательством чего является недавнее установление японской фирмой "Fujitsu" контроля над фирмой "ICL", которая являлась главным производителем компьютеров в Великобритании.

Статья о японской настольной игре Го, опубликованная во внутренней газете фирмы "Fujitsu", позволяет понять причины этого ее поступка, который, по всей видимости, подготавливался на протяжении долгого времени. В отличие от шахмат, цель игры Го заключается не в поражении пешек и фигур противника, а в захвате территории.

Иными словами, в настоящее время мы находимся на основном и решающем этапе глобализации японской промышленности средств информатики. Японская точка зрения была ясно изложена в одной из ведущих экономических газет Японии "Nihon Keizai Shimbun": Национальная промышленность против фирмы "IBM". Отныне вопрос заключается в следующем - сможет ли кто-нибудь еще, кроме фирмы "IBM" и японских компаний, выжить на мировом рынке? Десять лет назад дефицит внешнеторгового баланса Западной Европы в области средств информатики составлял 20 млрд. французских франков. В настоящее время он достиг 70 млрд. франков, а в 1993 г. превысит 100 млрд. франков. Приведенные цифры, а также многочисленные неудачные попытки объединения усилий западноевропейских фирм, имевшие место за последние 10 лет, ясно показывают, что японская стратегия основана на глубоком знании рынка, действующих на нем лиц, конкурентов и тенденций развития. Это является результатом долговременного использования всех возможностей экономической разведки во всех ее видах и проявлениях.

Послужат ли эти поражения уроком для Западной Европы? В этом можно усомниться, читая следующую заметку, опубликованную в "Financial Times" 14 августа 1990 г.: один из лондонских университетов, столкнувшись с сокращением финансовых средств, выделяемых британской электронной промышленностью на научно-исследовательские работы, принял решение о создании специального бюро по связям с японскими промышленными кругами и об организации междисциплинарного научно-исследовательского цент-

ра по полупроводникам, рассчитывая при этом на поддержку государства! Зная, что один из японских подходов для бесплатного получения результатов научно-исследовательских работ заключается в частичном финансировании научной кафедры или лаборатории, несложно прийти к выводу, что такой поступок сводится к предложению японцам купить того самого коня с помощью которого они возьмут приступом новую Трою.

Для правильного понимания ситуации необходимо учитывать, что экономическая война, о которой идет речь, ведется неравноценным оружием. Ведь речь идет не о борьбе между фирмами, а о сражении, в котором с одной стороны выступает нация, имеющая достаточно воли и средств для экономических завоеваний, а с другой – разрозненные фирмы. Так, когда в 60-е годы Министерство внешней торговли и промышленности Японии приняло решение о повороте японской промышленности в сторону развития информатики, то есть отрасли, которая была признана стратегической, то при этом министерство выделило определенное количество фирм, которые и должны выполнять эту задачу ("Fujitsu", "Hitachi", "NEC", "Toshiba", "Mitsubishi Electric" и "Oki Electric"), и оказывало им финансовую поддержку вплоть до того момента, когда они наконец превратились в доходные предприятия, т.е. примерно до 1980 г.! Следует добавить, что за право сохранить присутствие на японском рынке это министерство потребовало от фирмы "IBM" поделиться многими важными технологиями. А что сейчас осталось американского в японском филиале фирмы "IBM"? Этот пример прекрасно иллюстрирует японские приемы ведения экономической войны. Прежде всего японцы точно определяют те отрасли, которые им необходимо развивать. Затем они анализируют наличные силы и слабые места своих противников. И, наконец, они умеют терпеливо выжидать и не жалеют времени для достижения успеха. Третий пункт заключается в необходимости наличия достаточной воли к победе. Первые два пункта связаны, несомненно, со способностью и умением собирать и анализировать информацию. В настоящее время, как, впрочем, и в былые времена, стратегия тесно связана с информацией.

В IV веке до нашей эры великий китайский стратег Сун Цзе сформулировал следующий совет: "Самое важное в войне - это борьба со стратегией врага". Его стратегия выражает его намерения, которые могут быть выяснены только с помощью разведки. Поэтому разведка является подлинным нервом войны. В военной области большинство крупных поражений было связано с несостоятельностью разведки.

Чтобы убедиться в этом достаточно вспомнить о том, как генеральный штаб гитлеровской Германии отказался принять во внимание планы союзников о высадке на северном побережье Франции или об операции американцев в Иране, что привело к катастрофе. Точно так же, в экономической войне японские победы над Западом были одержаны благодаря глубокому знанию рынка, экономики, социальных факторов и технологий. А если все это сопоставить со странами, занимающимися, в основном, продажей сырья или

сельскохозяйственной продукции, единственной стратегией которых является стратегия картеля, то становится очевидным то, насколько важную роль играет разведка.

Говорят, что нервом войны является золото. Однако в экономической войне вознаграждение своих войск не производится за счет ограбления поверженного противника. Ведь цель заключается не в однократной продаже своих товаров, а в долгосрочном закреплении своих позиций на завоеванном рынке. Классические навыки и умения фирм и предприятий (маркетинг, производственная деятельность, финансовая деятельность, работа с кадрами и т.п.) оказываются недостаточными для ведения борьбы в этой ситуации. Для обеспечения гарантированного принятия правильных решений необходимо также научиться работать с информацией, поступающей с поля экономической битвы.

Сбор разведданных и разведслужбы (большие маневры). Естественно, человечество отнюдь не пребывало в ожидании того момента, когда будет дано точное определение понятия информация и будут созданы формализованные методы стратегической разведки. Многие государи, князья и генералы очень рано поняли все значение разведки для ведения войны и в области дипломатии, так как это, со всей очевидностью, было вопросом жизни или смерти. Возвратимся к китайскому стратегу Сун Цзе, который почти 2500 лет назад преподал следующий блестящий урок: "Если просвещенный государь или рассудительный генерал одерживают победу над противниками каждый раз, когда они переходят к действиям, то это достигается благодаря предварительной информации. Так называемая предварительная информация не может быть получена ни от духов, ни от божеств, ни по аналогии с прошлыми событиями, ни путем расчетов. Ее необходимо получить от человека, который знаком с ситуацией противника" ("Искусство войны").

Ближе к нашим дням такие государственные деятели, как Людовик XI, Ришелье и его верный святой отец Жозеф, Кромвель, чей заместитель государственного секретаря Джон Тюрлоэ "носил на своем поясе секреты всех государей Европы", Бисмарк, информируемый грозным Вильгельмом Штибером и многие другие сумели создать очень эффективные службы, наследниками которых являются современные разведслужбы.

Очень рано появилась также коммерческая разведка. С ее помощью, например, итальянские города-государства прокладывали путь на Восток. Так, в Венеции коммерческая разведка и государственная разведка были очень тесно переплетены между собой. Начиная с XI века все богатство, а, следовательно, мощь и выживание Венеции все в большей и большей степени зависели от торговли с Востоком и, естественно, от всех случайностей и опасностей, связанных с этим видом деятельности. Все купцы и дипломаты, отправлявшиеся в зарубежные страны, в обязательном порядке становились агентами разведки Светлейшего (титул правителя Венеции) как по коммерческим, так и по политическим вопросам. Благодаря этому маленькой респуб-

лике удалось занять ведущие позиции и сохранить их, несмотря на открытие новых океанских путей и появление больших государственных образований и великих держав.

Однако первая настоящая частная разведслужба была создана флорентийскими купцами-банкирами (эти виды деятельности в то время часто совмещались) в XIV веке. Затем такую разведслужбу создали Фуггеры из Аугсбурга, которые в XV и XVI веках входили в число крупнейших промышленников и дельцов. Они составили свое огромное состояние благодаря монополии на разработку медных и серебряных рудников в Центральной Европе, а затем постепенно занялись финансовой деятельностью, предоставляя кредиты и займы императорам и королям. В 1607 г. они разорились после череды банкротств в Испании. Под руководством Якоба Фуггера (1459 – 1525) функционировала высокоэффективная разведывательная сеть, основой которой служили многочисленные представительства фирм в различных европейских странах. Распространялось далее специальное информационно письмо, содержащее всю последнюю информацию о политических и коммерческих делах.

Высокой эффективностью своей разведслужбы прославились Ротшильды. В конце XVIII века пять братьев основали банки в пяти европейских столицах (Лондоне, Париже, Вене, Франкфурте и Неаполе). Они были убеждены, что раньше или позже Наполеон будет разбит. Они были также убеждены, что, чем дольше Наполеон останется на престоле, тем больше он разорит и истощит Европу. Поэтому они решили ускорить его падение. Они навербовали более 200 агентов и предоставили все свои разведанные, а также свои возможности и способности по межгосударственному переводу капиталов в распоряжение Англии. Все расходы они с лихвой покрыли с помощью ловкой биржевой аферы. Благодаря своим информаторам, Натан Ротшильд первым в Лондоне узнал о поражении Наполеона. Он немедленно приступил к массовой продаже своих акций. Все остальные биржевики сразу же последовали его примеру, так как решили, что сражение проиграли англичане. Когда цены упали до предельно низкого уровня, Ротшильд все скупил! Англичане первыми расширили деятельность своих секретных служб на область экономики. Главной ставкой в игре послужила текстильная промышленность. Благодаря технологическому превосходству, явившемуся результатом промышленной революции, Великобритания обеспечивала себе в области текстиля практически монопольное положение. Однако в конце XVIII в. представители южных штатов Америки не пожалели финансовых средств на организацию промышленного шпионажа на английских фабриках в Ланкашире, в результате чего им удалось получить чертежи прядильной машины. Это послужило отправной точкой для создания и развития хлопчатобумажной промышленности в Америке. Благодаря наличию дешевой, в большинстве своем рабской рабочей силы американская хлопчатобумажная промышленность представляла реальную угрозу для Англии. Поэтому последняя решила лю-

бой ценой защитить конкурентоспособность своей промышленности. Ей это удалось за счет максимальной эксплуатации пахотных земель и сельскохозяйственных угодий в своих колониальных владениях путем создания огромных хлопковых плантаций в Африке и Вест-Индии. Эту миссию успешно выполнил Генри Уикхем, который уже до этого великолепно себя зарекомендовал, когда нелегально вывез из Бразилии семена гевеи, разрушив тем самым монополию этой страны в области каучука.

В XVII и XIX веках хлопковая война развивалась по четырем направлениям: протекционизм, технологическое пиратство, территориальные захваты и война цен. В период между двумя мировыми войнами с помощью примерно этих же методов японская текстильная промышленность одержала верх над своими британскими и американскими конкурентами. Японское государство дошло даже до того, что компенсировало своим фирмам и предприятиям высокие таможенные пошлины.

Организация экономики Германии является синтезом прусского дирижизма (директивных методов государственного руководства экономикой) и динамизма Ганзейского Союза в сочетании с англосаксонскими методами. Ее создание стало возможным благодаря союзу между банками, промышленными картелями, торговыми домами, транспортными фирмами и государством. С помощью эмигрантов (в США, Бразилию и т.д.), дипломатических и консульских работников и широкой сети коммерческих фирм Германии удалось собрать всю информацию, необходимую ей для экспансии. Приведем в качестве примера отрывок из памятки коммивояжера, который является центральным звеном политики захвата внешних рынков. Кто ваши конкуренты? С какими товарами конкуренты действуют на рынке? В чем заключается стратегия конкурентов? В каких областях конкуренты имеют преимущества? В каких областях ваше предприятие является лидером? Может ли продукция вашего предприятия заменить товары конкурентов? Какие позиции занимает на рынке каждый из конкурентов? Существует ли в вашей отрасли фирма, которая задает тон? Существует ли какой-либо "порог", за которым следует реакция? Сталкивались ли вы с чем-либо таким в прошлом? Какие фирмы реагировали с особой частотой и активностью? Существуют ли у вашего предприятия дружеские связи с конкурентами? Кто поставляет информацию? Как используется эта информация?

Уже давно в Германии вся собранная информация сводится в тематические картотеки, что обеспечивает заметное превосходство в области технологии обработки информации. Причины нынешнего успеха германских фирм в странах Центральной Европы не могут быть объяснены без учета той огромной каждодневной работы, проделанной за последние 20 лет и позволившей создать сеть сбора информации по всем ключевым отраслям. С этой целью широко использовались многочисленные немецкоязычные общины и землячества в странах Центральной Европы. От них были получены рекомендации и советы о способах и приемах деятельности в условиях социалистической

экономики (черный рынок, коррупция и т.п.). Таким образом, Германия создала очень надежную сеть сбора информации и сейчас использует ее с большой пользой для себя.

Япония и Германия очень близки друг другу по многим методам и приемам деятельности: организация крупных коммерческих фирм, использование дипломатических работников для поддержки коммерческой деятельности, создание картотек по рынкам, конкурентам, товарам и т.п. Германия научилась у англичан использовать все преимущества, связанные с привлечением к работе интеллектуальной элиты. Британская интеллигенция часто вносила безвозмездный вклад в дело укрепления империи. Японцы распространили эту практику на всех инженерно-технических работников своей промышленности.

Вклад Советского Союза заключается в использовании методов манипулирования информацией: дезинформация, избыточная информация, недостаточная информация, резонансная камера. Так, Советский Союз постоянно практикует фильтрацию и тщательную дозировку информации, переводимой на иностранные языки. Такая тактика недостаточной информации оправдала себя, так как помешала западным странам точно определять цели Советского Союза. Кроме того, Советский Союз широко использует метод избыточной информации, который заключается, например, в публикации толстых докладов, заполненных недостоверными данными, которые подаются в качестве подлинной информации.

Не следует забывать, что еще в начале XIX века в Японии царил феодальный строй и страна была изолирована от внешнего мира. Трансформация в этой стране началась в 1867 г., когда император Медзи положил конец Сегонату (военной диктатуре) самурайского рода Токугава. Стремительное развитие Японии (за несколько десятилетий) не может быть объяснено без учета интенсивного использования разведметодов. Доказательством этого может служить история создания морского флота. В этой области Японии пришлось начинать с нуля, так как в эпоху правления Токугава страна пребывала в состоянии полной самоизоляции: поездки за границу были полностью запрещены, въезд иностранцев на территорию Японии был запрещен (за исключением въезда некоторых представителей Голландии и Китая на маленький остров Десима, расположенный вблизи Нагасаки), строительство морских кораблей также находилось под запретом. В 1853 г. визит в Японию Перри во главе небольшой американской эскадры, вооруженной пушками, явился большим потрясением, которое способствовало началу революции Медзи, а также побудило Японию приступить к созданию передового в техническом отношении флота во избежание повторения подобного унижения. Поэтому Япония разместила свои заказы на британских морских судостроительных верфях. Однако японцы при этом стремились получить только чертежи и техническую документацию. Как только они их получали, они сразу же аннулировали свои заказы. Затем, для постройки кораблей на основании добытых

чертежей и технической документации, японцы привлекли видных специалистов, таких, как Уильям Уайт. За несколько лет они построили судостроительные верфи, которые позволили создать мощный военный и торговый флот, бороздящий все моря и океаны нашей планеты. Доказательством высокого технического совершенства этого флота явился в 1905 г. разгром в Цусимском сражении русского флота эскадрой адмирала Того. Для сбора разведданных используются самые различные методы. Многие из них не отличаются особой порядочностью, однако все они являются неизменно эффективными: закупка товаров конкурента; неизменное присутствие на ярмарках, выставках, конференциях и т.п., при этом собирается вся доступная или оставленная по недосмотру документация и информация, фотографируется все, что возможно; посещение предприятий (в конце 70-х годов 1500 японских экспертов буквально наводнили Кремниевую (Силиконовую) Долину в Калифорнии, США); финансирование контрактов на выполнение научно-исследовательских работ за рубежом с целью проникновения в некоторые лаборатории (с этой целью в 1986 г. знаменитая "MIT" получила от японских фирм 10 млн. долларов); отправка на учебу за рубеж студентов и стажеров (только в США - 140 тыс. человек); бесконечные безрезультатные переговоры, в процессе которых постоянно запрашивается дополнительная информация; похищение чертежей и технической информации (см. историю создания японского флота); шпионаж и простое воровство (дело "IBM" против "Hitachi").

Все это не должно скрывать того факта, что большую часть информации обычно получают за счет чтения различных изданий. Доля получаемой за счет этого информации в среднем составляет 50 %, а по некоторым исследовательским лабораториям достигает даже 70%. Даже правительство Японии приняло во внимание этот факт и в 1957 г. организовало Японский научно-технологический информационный центр (JICST), который ежегодно анализирует 11000 журналов, в том числе 7000 зарубежных, 15000 технических отчетов и докладов и рассылает более 50000 резюме.

Затраты на разведку составляют в среднем 1,5% торгового оборота крупных концернов. Так, в фирме "NEC" информационной работой постоянно занимаются 250 человек. В фирме "Mitsubishi" 30 человек занимаются патентами, 50 человек занимаются только технологией и т.д. Как очень удачно заявил Коносуке Мацусита: "Вы, на Западе, совершаете два смертельных греха - ищите то, что уже было найдено, и покупаете то, что можно иметь бесплатно".

Японии удалось создать великолепную машину экономической войны, так как там сумели осознать, что информация является жизненно важным сырьем. Вынужденная силой открыться внешнему миру, эта страна, чтобы не превратиться в обычную колонию, должна была быстро интегрироваться в систему мировых обменов товарами и идеями, усвоить плюрализм, культуру, все последствия и достижения технологического прогресса. Несомненно, островное положение, обостренный национализм и клановая организация общества в Японии в значительной степени упростили информационный обмен

внутри страны и ограничили утечку информации за рубеж. Этот небольшой обзор ведущих стран, занимавшихся или занимающихся разведкой в экономических целях, был бы неполным без СССР. Начиная с НЭПа, периода либеризации с 1921 по 1929 гг. перед тотальной коллективизацией, государственным органам было поручено заниматься экономической разведкой. Для этого использовались различные способы – от объявления ложных конкурсов между зарубежными фирмами до закупки технологий с целью копирования. В 20-е годы главной целью этой деятельности являлись Франция и Великобритания, в 30-ые годы наступил черед Германии, а затем и США. Американская помощь в период Второй мировой войны позволила значительно расширить эту деятельность. Однако СССР никогда не рассматривался в качестве реального конкурента в области экономики. Поэтому с расширением холодной войны защитные меры были приняты только в военной области. Кстати, катастрофа "Ту-144", имеющего большое сходство с "Конкордом", продемонстрировала всю порочность простого копирования. Анализ обломков показал, что применявшиеся сплавы не обладали механическими свойствами, требуемыми для самолетов этого типа.

В нашем обзоре мы еще не коснулись двух стран – Франции и США. Пример США может послужить хорошим уроком. В отличие от Японии, которая с момента отказа от самоизоляции вынуждена была противостоять всему остальному миру, США, благодаря своим гигантским размерам, на протяжении долгого времени не интересовались событиями, происходящими за пределами их границ. Это становится в общем-то понятно, если учесть, что еще в 50-е годы доля внутреннего рынка США в мировой экономике составляла порядка 50%. Из-за таких огромных масштабов экономики в сочетании с доктриной попустительства американские фирмы ограничили свою разведдеятельность наблюдением за непосредственными конкурентами. Так, гигантские автомобилестроительные концерны Детройта были слишком заняты взаимной слежкой и не заметили японской угрозы.

Однако, даже почувствовав себя атакованными, США не реагировали. Потребовалось значительное время для того, чтобы эта страна осознала угрозу своей безопасности и предприняла ответные меры. Событием, ускорившим принятие таких мер, явился арест двух сотрудников японской фирмы "Hitachi" за попытку приобретения чертежей последней модели ЭВМ фирмы "IBM": их задержало ФБР 22 июня 1982 г.

Это событие раскрыло глаза американским властям, которые наконец-то заметили, что зависимость США от Японии в области электронных компонентов достигла 90%! Пентагон принял решение об ответных мерах. В 1988 г. адмирал Имман, бывший директор Агентства по национальной безопасности (АНБ), занимающегося прослушиванием, а также защитой линий связи, организовал два консорциума. Один из них был чисто исследовательским с капиталом 100 млн. долларов, а второй - научно-производственным с капиталом 250 млн. долларов.

Однако эти попытки завершились полу провалом. Хотя этим консорциумам и удалось передать несколько новых технологий своим членам, однако последним так не удалось избавиться от традиционной взаимной подозрительности и недоверия. Последний из таких консорциумов "US Memories", объединявший крупнейшие американские фирмы, работающие в области информатики (от "IBM" до "Digital", включая "Hewlett Packard"), также потерпел неудачу после того, как фирма "Intel" предпочла объединиться с японской фирмой "NMB Semiconductor". Последствия: американские фирмы контролируют только 15% своего внутреннего рынка, а японские фирмы захватили 75% мирового рынка.

Можно утверждать, что США, как впрочем, и Франция, обладают низкой культурой разведки. Это связано, по-видимому, с историческими и географическими условиями. Ведь речь идет о богатых странах, исторически слабо зависимых от внешнего мира, с доминирующим сельским хозяйством и малоуязвимых благодаря своему географическому положению, из-за чего они не проявляли особого интереса к событиям в других странах.

Однако целый ряд иных стран совсем по-другому относился к разведке, так как считал информацию залогом процветания и безопасности своего общества. Доказательством этого является пример Венеции, а также Англии времен королевы Елизаветы 1. В этом случае речь идет о торговых странах, обладающих обостренным чувством своей уязвимости и зависимости от внешнего мира. Так, Венеция должна была бороться за сохранение своей коммерции в Средиземном море, несмотря на противодействие со стороны Оттоманской империи. Что касается Англии, то она должна была защищать свое морское государство от Испании, Голландии и Франции. Общества этого типа обладают высоким сознанием своей национальной принадлежности и превосходства: "Самый худший из нас - лучше любого из них". Позднее и другие страны (бисмарковская Германия, императорская Япония, Россия Петра Великого, а затем и СССР, Китай Мао Цзе Дуна, Тайвань, Южная Корея и некоторые другие) обладали навыками того, что можно назвать "культурой разведки".

Ситуация во Франции. По масштабам Европы Франция является большой страной. Однако, как говорил Валери, Европа является всего лишь полуостровом Азии. До недавнего времени Франция являлась сельскохозяйственной и очень воинственной страной. Поэтому ее элита на протяжении долгого времени оставалась близкой к земле и не интересовалась коммерцией. Естественно, для ведения войны требовалась разведка, однако она в основном ограничивалась чисто военными аспектами и пренебрегала информацией экономического и социального характера, необходимой, например, для успешной коммерческой деятельности.

Трудолюбивые торговые и буржуазные семейства долго оставались во Франции исключением. Кстати, когда в 1789 г. им удалось изменить установленный порядок, то они заморозили свое состояние в земельных владениях

вместо того, чтобы вкладывать капитал в средства производства и положить начало, как в Англии, промышленной революции. А изучением и освоением мирового пространства занимались купеческие венецианские, генуэзские, ганзейские, голландские, португальские и британские династии. Тем не менее, благодаря активной военной политике и отдельным талантливым индивидуумам, Франции все же удалось создать колониальную империю. Однако ее развитие тормозилось нерешительностью и безразличием ее государственных сановников и политикой "железнодорожных" выборов.

Эти исторические и географические условия в большой степени объясняются отсутствием во Франции культуры разведки. Основой французской экономики долгое время являлось сельское хозяйство. Поэтому правящим классом являлись землевладельцы, вся деятельность которых делилась между неторговой и нетоварной экономической деятельностью практически обособленного характера и государственной службой военного характера. По тем же причинам отсутствовали благоприятные возможности для развития городов, хотя проводились ярмарки и работали торговые рынки. За исключением отдельных непродолжительных периодов (Людовик XI, например, был большим поклонником итальянских городов) центральные власти, ревностно дорожащие своими прерогативами, относились с нетерпимостью к существованию вольных городов, живущих за счет коммерции (особенно после отмены Нантского эдикта). Продолжением всего этого является высокая степень иерархизации общества, которая даже сегодня ясно просматривается при сравнении организационных структур французских фирм и фирм большинства других стран. Жесткая иерархическая структура в значительной степени тормозит нормальную циркуляцию информации, что объясняется боязнью поставить под сомнение свою власть.

Со своей стороны, французская интеллигенция, в отличие от английской, почти всегда относилась с презрением к любой деятельности, кроме умственной. При этом они презирали не только ручной труд, но также государственную и коммерческую деятельность. На этой основе развился комплекс превосходства, в соответствии с которым Франция считалась центром мира. Естественно, Европа и мир многим обязаны Франции, начиная с готических соборов и заканчивая идеей прав человека, включая картезианскую философию. Однако одним из порочных и вредных следствий этого явилось убеждение в том, что французам нечему учиться за пределами своей страны. Таким образом, за исключением нескольких кратких периодов эйфорической экспансии под предводительством самоотверженных деятелей, французы предпочитают оставаться дома.

Кроме всего прочего, одним из важных следствий всего этого является также полное отсутствие сотрудничества между государством и коммерческими фирмами. Лучшим доказательством этого является тот факт, что французские дипломаты традиционно испытывают святой ужас по отношению к коммерции. Являясь выходцами из семей, для которых дипломатия являлась одной из форм службы государю, они интересуются только политикой и отвер-

гают экономическую разведку как крайне малопочтенное занятие. Не желая пачкать рук, они передоверяют эту задачу коммерческим атташе, полная бесполезность которых сейчас является общепризнанной.

Ни одно из французских правительств после Второй мировой войны даже не попыталось взяться за разработку и проведение в жизнь глобальной стратегии коммерческой экспансии. Были только лишь созданы структуры материально-технической и тыловой поддержки, такие как Французская компания страхования и кредита внешней торговли, а также организации "DRE" и "CFCE". Этого явно недостаточно по сравнению с тем, что делают в этой области Германия и Япония.

Такое отсутствие государственного вмешательства выглядит тем более серьезно и странно, если принять во внимание, что Франция обладает давней и сильной традицией кольбертизма. Именно государственные власти часто брали на себя в этой стране инициативу по внедрению различных новшеств. Для того, чтобы убедиться в этом, достаточно вспомнить историю создания Севрской мануфактуры или историю внедрения в сельскохозяйственную практику выращивания картофеля. Когда в Англии и в Германии дороги и пути сообщения перешли в ведение местных общин и даже купеческих гильдий, то французские провинции в это же время переходили под власть короля.

Безусловно, экспортные успехи французских фирм являются достаточно очевидными. Однако, в отличие от японских фирм, которые еще в 30-е годы начали заключать между собой соглашения о ненападении, французские фирмы с давних пор имели обыкновение открыто бороться между собой. Так, например, в 60-е годы фирма "Thompson" вела борьбу с фирмой "CSF", в 70-е годы фирма "Alcatel" боролась с фирмой "Thompson", а совсем недавно велось сражение между фирмами "Bouygues" и "Dumez". Не будет преувеличением утверждать, что эта страна, обладающая большим творческим потенциалом, продемонстрировала явный дефицит желания и склонности к деятельности, требующей настойчивости и упорства. Становится одновременно смешно и печально, когда вспоминаешь о различных гениальных семействах автомобилей фирмы "Citroen", каждый раз новых и с длинной чередой поломок и возвратов. В то же время, фирма "Mersedes" совершенствовала свою модель автомобиля постепенно, вводя новые технологии только тогда, когда это было действительно необходимо и когда они были полностью отработаны.

Очевидно одно - невозможно ничего сделать без целеустремленной воли государства, которое должно в сотрудничестве с организациями предпринимателей и промышленниками выработать стратегию для этой новой формы войны. Речь идет не только о стратегии деятельности, но и о стратегии в области информации, так как пренебрежение последней равнозначно попыткам поймать черную мышь в темной комнате. С этой точки зрения полезным уроком должен послужить пример Японии и ФРГ. В этих странах экономическая политика определяется путем согласования между частными и государственными предприятиями, административными органами и банковской системой. Для этого Япония

объединила свои министерства промышленности и торговли, создав единое Министерство внешней торговли и промышленности, а ФРГ создала специальные структуры для согласования вопросов между предприятиями, банками и административными органами, что, в частности, достигается с помощью специальных фондов, финансируемых местными общинами и предприятиями.

Хотя в целом Франция не обладает высокой культурой разведки, было бы преувеличением утверждать, что у нее полностью отсутствуют традиции и навыки в этой области. Бурное воинственное прошлое Франции очень рано вынудило ее правителей приступить к созданию разведслужбы, деятельность которой была в основном направлена на политические и военные аспекты. Такие французские политические деятели, как Людовик XI и Ришелье, довели это искусство до совершенства.

В настоящее время во Франции в области экономики сосуществуют три формы практической деятельности этого типа: государственная поддержка стратегических отраслей (нефтяная промышленность, военная промышленность и т.п.), несколько высокоэффективных фирм ревностно охраняют свою компетентность и "ноу-хау" (фирмы "Michelin", "Shumberger", "Air Liquide", "Bouygues"), а также умения и навыки, импортированные из США рядом транснациональных корпораций ("IBM", "Texas Instruments", и т.п.). Таким образом, не может быть и речи о том, чтобы начинать полностью с нуля.

В вышеописанной ситуации естественным образом напрашивается вопрос: что делать? Успешный опыт Японии и Германии, а также Южной Кореи и скандинавских стран подсказывает необходимость деятельности в три этапа: по инициативе правительства установить тесные связи между предприятиями и государственным аппаратом; путем согласований определить долгосрочные экономические и коммерческие цели; создать на всех уровнях средства сбора и обработки информации, максимально при этом используя уже имеющиеся наработки и структуры, стремясь к получению экономии за счет эффекта масштаба (не забывая, что любой центральный орган должен работать на строго федеративной основе, а не выделяться в феодальную вотчину).

Для более конкретного разговора вернемся на некоторое время к фундаментальным понятиям, рассматриваемым в настоящей работе. Речь идет о базах и каналах. Подобно живому организму предприятие не действует изолированно. Ему необходимо иметь систему восприятия окружающей реальности для поиска ресурсов, необходимых для своего развития, и для защиты от хищников. Такой системой восприятия являются базы, указывающие на объект пристального внимания. Однако, если вы не находитесь в нужном месте, то даже самое лучшее в мире зрение не позволит вам ничего увидеть. Точно так же охотник или рыбак не располагаются, где придется. У них есть свои места. Такими местами, дорогами, пунктами, которые нельзя обойти, являются каналы.

С помощью этих двух основных понятий мы сможем определить, что следует сделать для того, чтобы помочь предприятиям эффективно наблюдать и следить за своим окружением. Прежде всего они должны провести работу

по определению баз. Это особенно важно для малых и средних предприятий, которые не располагают специализированным персоналом. Затем необходимо помочь им овладеть главными информационными каналами ("Текст", "Фирма ", "Консультант", "Беседа"). И наконец, если позволяют размеры организации, то необходимо внедрить различные компоненты системы стратегической информации (ССПИ и СТОИ). Это можно сделать с помощью курсов, родолжительностью в несколько дней, на которые будущий исполнитель этих функций ознакомится с основными методическими концепциями и научится ими пользоваться в соответствии со своими потребностями.

На более общем уровне необходимо: твердо придерживаться традиций, так как важнейшее значение имеет культура. Что касается технических аспектов, то ими сравнительно легко овладеть. Франция это не Германия и не Япония; обеспечить подготовку профессионалов, не злоупотребляя привлечением специалистов из военной области, где экономические аспекты недооцениваются, а зачастую просто плохо известны, и где делается чрезмерный акцент на "активную безопасность" (естественно, чрезмерный по отношению к требованиям экономической разведки, а не по отношению к военной разведке); привлечь крупные фирмы и концерны к проведению пропагандистских мероприятий, которые должны охватывать не только их персонал, но также их поставщиков субподрядчиков, клиентов; обеспечить координацию деятельности на региональном уровне; установить связи между правительственными органами и службами стратегической разведки крупных фирм и концернов; ввести преподавание основ этой деятельности в технических и коммерческих институтах, а также в подготовку исследователей для государственных организаций.

Сейчас не время ставить вопрос о принципиальной обоснованности и оправданности информационной деятельности. Никакая стратегия, никакая производственная и коммерческая политика, а следовательно и капиталовложения, научно-исследовательские работы, структурные изменения и т.д., не являются отныне возможными без углубленного изучения сил, движущих миром: технологии, экономики, политики и т.д. Сейчас более чем когда-либо, в еще только разгорающейся экономической войне единственно информация обеспечит решающее преимущество.

Хэмри Дж.

ЗАЩИТА ИНФОРМАЦИИ – ГЛАВНАЯ ЗАДАЧА НОВЕЙШЕГО ПЕРИОДА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ*

Защита жизненно важных информационных ресурсов станет "одной из главных задач в области национальной безопасности на ближайшие годы", – считает заместитель министра обороны США Джон Хэмри. Отметив, что на Пентагон возложена ответственность по защите 28 тыс. различных компьютерных систем, он предупредил, что оборона виртуального мира от киберне-

тической угрозы "требует не только технического решения, но и правильного управления и постоянного внимания к этому вопросу".

С точки зрения обеспечения безопасности, Соединенные Штаты пережили пять периодов, при этом переход от одного периода к другому означал переход от определенного прошлого к совершенно неопределенному будущему. Первый период длился с начала войны за независимость до середины 20-х годов 19-го века, когда роль Соединенных Штатов в системе международной безопасности, где все еще доминировала Европа, была ограничена.

С середины 30-х годов до конца 19-го столетия, пока шел процесс разрушения старой политической структуры Европы, мы, отделенные от нее Атлантическим океаном, занимались своими собственными делами. Этот второй период завершился с окончанием Первой мировой войны и возникновением Советского Союза. Третий период длился с 1920 по 1946 год и характеризовался глобальным экономическим спадом и одновременно подъемом международного коммунистического движения на фоне распада Европы. Эти события привели к кризису американской демократии и системы свободного предпринимательства во время Великой депрессии, а напряженность в области международной безопасности привела в конечном итоге ко Второй мировой войне.

В период холодной войны доминировал двухполюсный мир. Соединенные Штаты возглавляли движение международного сообщества, направленное на создание институтов для восстановления разрушенной экономики стран Европы и решение проблем в странах третьего мира, связанных с распадом старых европейских империй. В то же время Соединенные Штаты возглавляли движение стран свободного мира, направленное на сдерживание распространения коммунизма во всем мире, вплоть до развала Советского Союза.

В настоящее время происходит переход к новой эпохе, которая, по-видимому, будет характеризоваться возрождением старых факторов угрозы — национализма и этнических конфликтов. Еще одна сторона этого нового периода связана с ослаблением контроля и распространением современных технологий, а также динамичным развитием новых совершенно поразительных технических возможностей, которые несут в себе огромный потенциал как добра, так и зла. Сейчас мы живем в постоянном страхе из-за того, что "бесконтрольные ядерные ракеты" или химическое и биологическое оружие может попасть в руки террористов.

Новейший период в области обеспечения безопасности США будет также связан с проблемой кибернетической безопасности. Стремительный рост и распространение информационных технологий оказали существенное воздействие на все сектора американской экономики и правительство. Информационные технологии способствовали колоссальному экономическому развитию, качественно усовершенствовали средства связи и позволили американским предпринимателям участвовать в конкурентной борьбе более эффективно и успешно, чем когда бы то ни было. Соединенные Штаты и мир в

целом в очень серьезной степени опираются на информационную технологию — этого нельзя было вообразить еще буквально несколько лет назад.

Это особенно справедливо в отношении американских военных. Министерство обороны применяет информационные технологии, чтобы произвести, как мы говорим, революцию в военной сфере, которая охватывает передачу и обработку огромного объема информации для получения более достоверных разведданных, радикальное совершенствование средств управления и контроля, внедрение более современных методов работы и разработку более мощных систем вооружения. Эта революция имеет огромное значение, особенно если мы хотим сохранить способность защищать интересы США сегодня и подготовиться к отражению угрозы в будущем.

Революция информационных технологий охватывает все сферы деятельности Министерства обороны как в полевых условиях, так и в штабах. Очень скоро наши солдаты на уровне первичного подразделения будут иметь средства связи, которые позволят командирам точно знать о местонахождении каждого отдельного солдата, обстановке вокруг него и даже ритме сердца, то есть почти исчерпывающие сведения с поля боя. Наши моряки направляют домой с кораблей в открытом море послания по электронной почте, применяя технологию, очень схожую с той, которая используется для нацеливания крылатых ракет. Летчикам приходится сейчас отсеивать в перенасыщенном потоке информации ту, которая им необходима в полете.

Мы применяем новейшую технологию в сфере материально-технического снабжения для соединения передовых рубежей с тылом. К концу века мы обязались перейти к процессу закупок без оформления каких-либо бумаг. Созданное у нас Объединенное управление электронных программ обеспечивает закупку всего необходимого на уровне подразделений и широко использует основанные на Интернете электронные "торговые центры" для покупки всего — от ручек до гидравлических силовых приводов. Мы очень широко используем Интернет, начиная от оплаты транспортных расходов и заканчивая спутниковой связью, и добились огромных успехов в публикации материалов в электронных средствах информации.

Короче говоря, Министерство обороны США в полной мере использует потенциал микросхем для создания вооруженных сил 21-го века. Однако, при этом необходимо осознавать, что вместе с новыми технологиями приходят и новые опасности. Те же самые технические средства, которые позволяют нам достигать высокую эффективность, могут быть использованы для нападений в кибернетическом пространстве теми, кто не может нанести нам удар на обычном поле боя. Это совершенно другое — и очень важное — направление в области национальной безопасности. Технологические средства и возможности, которые ранее были доступны только государствам, стали доступны частным лицам. Защита информационных ресурсов станет поэтому одной из главных задач в области национальной безопасности на ближайшие годы.

Мало кто оспаривает тот факт, что защита информации имеет важное значение. В Министерстве обороны мы уже столкнулись с первой волной кибернетической угрозы как на учениях, так и в реальной обстановке. Для того, чтобы оценить степень нашей уязвимости, мы в прошлом году провели учение. Нашими "противниками" была группа из 35 человек, перед которыми была поставлена задача проникнуть в компьютерные системы Министерства обороны США. В их распоряжении имелись только общедоступные средства, готовые технологии и программное обеспечение, которое открыто продается или которое можно загрузить с Интернета. Действуя в таких условиях, эта группа в течение трех месяцев смогла атаковать нас, проникнуть в наши несекретные сети и фактически могла серьезно нарушить работу наших средств связи и систем энергоснабжения.

В феврале этого года мы испытали организованное нападение против компьютерных систем Пентагона в период интенсивного развертывания сил в районе Персидского залива. Оказалось, что это сделали два подростка из Калифорнии, но в тот момент такой удар мог оказаться гораздо серьезнее. Как наши учения, так и эти ограниченные удары сыграли роль предупредительных сигналов о том, что более серьезные удары обязательно последуют, вопрос лишь в том, когда и где.

Для предотвращения этой угрозы прежде всего надо изменить образ нашего мышления. Традиционно американцы думали о безопасности как об ограде вокруг двора, которая устанавливает границы и защищает огороженную территорию. Если в ограде появляется дыра, ее можно заделать и опять оказаться в безопасности. Такой образ мышления хорошо работал в прошлом, но в кибернетическом пространстве границы отсутствуют. Переход к будущему должен быть отмечен не только достижениями в области технологии, но и большей гибкостью мышления. Мы должны осознать, что безопасность в виртуальном мире требует не только технического решения, но и правильного управления и проявления постоянного внимания к этому вопросу.

Изменение образа мышления может оказаться одной из самых трудных задач. Не осознавая этого, мы сейчас предоставляем, например, потенциальным противникам информацию, на добывание которой они раньше тратили сотни миллионов долларов, проводя разведывательные операции. У нас был один военный объект, у которого, как считалось, была прекрасная страница в Интернете. На ней была изображена проекция объекта с воздуха, где были обозначены здания с надписями "Операционный центр" и "Центр технической поддержки". Эта страница очень нравилась общественности, но в то же время предоставляла ценную информацию для наведения на цель тем, кто хочет нанести нам ущерб.

Более широко осознавая связанные с этим проблемы, необходимо предпринять конкретные меры по защите наших информационных данных. В прошлом году Министерство обороны США попыталось определить потребности по защите нашей информационной инфраструктуры. Темпы развития

информационной технологии осложняют эту проблему. В Министерстве обороны имеется 28 тыс. различных компьютерных систем, причем все они совершенствуются и заменяются. Но необходимо понять их уязвимые места. Задача защиты информации схожа с войной, и мы соответствующим образом подходим к ее решению, назначив для координации усилий командира Объединенной тактической группы по защите компьютерной сети Министерства обороны. Министерство обороны вносит также большой вклад в работу Национального центра защиты информации и Управления защиты важнейшей информации при Президенте США.

Безусловно, необходимо предпринимать и другие действия. В настоящее время 95 процентов наших коммуникаций осуществляется по обычным телефонным и факсимильным линиям, в результате чего важным элементом защиты информации становится шифрование. Одним из наиболее опасных сценариев действий в виртуальном мире может стать такой, когда наши бойцы получат ложные сообщения, которые будут их дезинформировать. Поэтому без надежного шифрования вся информационная инфраструктура, от которой мы зависим, оказывается уязвимой. В ответ на эту угрозу мы сейчас работаем над тем, чтобы в рамках Министерства обороны можно было гарантировать цифровое "удостоверение личности" пользователей и разработать надежную систему связи на основе публичного шифровального ключа. Мы должны усовершенствовать процесс кодирования с тем, чтобы информация, которую мы передаем и обрабатываем с помощью электронных средств, была в безопасности и поддавалась проверке.

Министерство обороны предпринимает также важные шаги по обеспечению безопасности сети в более широком плане. Мы устанавливаем средства контроля за системами связи и работаем над обеспечением контроля конфигурации в условиях постоянно изменяющейся и динамичной среды. Мы устанавливаем программные блокировки, создаем центры контроля за сетями, цифровые опознавательные коды и создаем инфраструктуру безопасности.

Защита информации, шифрование и безопасность сетей составляют одну из самых серьезных проблем, с которыми когда-либо сталкивалось Министерство обороны. Используя последние достижения в области информационной технологии, необходимо обеспечить доступ к информации, на которую мы опираемся, и ее защиту. Мы предпринимаем огромные шаги в этом направлении, однако предстоит еще многое сделать. В это трудное время необходимо использовать опыт специалистов по информационной технологии как в Министерстве обороны, так и в частном секторе и правительстве, чтобы защитить жизненно важные для нас компьютерные системы. Мы должны сделать так, чтобы наша страна так же успешно функционировала в условиях современного периода в обеспечении безопасности, как и в прошлом.

ЧИННИКИ ЕСКАЛАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ. АНАЛІТИЧНА ДОПОВІДЬ УЦЕПД *

До основних загроз інформаційній безпеці України, на думку експертів УЦЕПД, можуть бути віднесені наступні: обмеження свободи слова та доступу громадян до інформації; руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов; маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл; обмеження можливостей органів державної влади приймати адекватні рішення; порушення штатного режиму функціонування (руйнування) критично важливих інформаційних мереж, систем управління; несанкціонований витік таємної, конфіденційної та іншої інформації з обмеженим доступом; спотворення (знищення) інформаційних ресурсів, програмного забезпечення; низький рівень інтегрованості України в світовий інформаційний простір.

Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер — вони охоплюють усі сфери життєдіяльності людини, суспільства та держави. В наступних двох підрозділах аналізуються внутрішні та зовнішні чинники ескалації загроз.

Внутрішні чинники ескалації загроз.

Проведений аналіз засвідчує, що рівень інформаційної безпеки в Україні, за окремими ознаками, наближається до критичної межі, за якою — втрата демократичних принципів і засад діяльності держави, повернення до авторитаризму, ізоляція України на міжнародній арені.

Сьогодні саме чинники політичного характеру провокують ескалацію головних загроз в інформаційній сфері, ставлять під сумнів реалізацію прав громадян на свободу слова. Передусім, це впровадження політичної цензури, тиск на ЗМІ, прояви політичного екстремізму стосовно журналістів, недостатя відкритість органів державної влади для громадського контролю, перетворення ЗМІ на засоби масової пропаганди. Серед інших негативних чинників, що аналізуються в цьому підрозділі, — неефективна податкова політика, монополізація окремих сегментів інформаційного простору, неприбутковість ЗМІ та їх вибіркова підтримка органами державної влади, старіння та руйнація інформаційної структури та ін.

Впровадження політичної цензури.

У вітчизняних та закордонних ЗМІ неодноразово оприлюднювалися факти, що свідчать про намагання впровадити в Україні політичну цензуру [1]. Особливо гостро це питання постало після оприлюднення заяви колишнього офіцера безпеки М.Мельниченка, який звинуватив Президента України в протиправних діях, спрямованих на обмеження свободи слова в Україні [2]. Непоодинокими є факти, коли журналістам відмовляють в акредитації в органах державної влади, що обмежує доступ журналістів і громадян до інформації [3].

Впровадження політичної цензури засновниками ЗМІ. На думку експертів, під таке визначення підпадають дії Федерації професійних спілок України щодо припинення в 1999р. видання «Профспілкової газети» та журналу «Профспілки України», мотивовані нібито тим, що вони не відповідають цілям засновників [4]. Загальнонаціональні телеканали або практично монополізовані державою (УТ-1, УТ-2), або належать власникам, які підтримують політику діючої влади і визначають політичний курс ЗМІ відповідно до її інтересів. В результаті, на думку колишнього голови Комітету Верховної Ради з питань свободи слова та інформації, народного депутата України І.Чижа, «після президентських виборів в Україні практично немає опозиційної преси, яка б існувала на загальнодержавному рівні» [5].

Аналогічні процеси розгортаються і в регіонах. Так, редактор газети «Ракурс» М.Сєверин закликав правління Луганської обласної організації Союзу журналістів України вжити заходів щодо захисту регіональних ЗМІ від протиправних дій керівників підприємств, організацій, які мають відношення до виробництва та реалізації продукції ЗМІ [6]. Здійснення протиправних дій щодо газет «Днепровская правда», «Кіровоградська правда», «Полтавська думка», припинення виходу окремих програм телерадіомовних організацій зафіксовані в документах, прийнятих Верховною Радою. Згідно з заявою голови підкомітету Парламентської Асамблеї Ради Європи (ПАРЄ) з питань ЗМІ Тіті Ісохоокана-Асунмаа (Tytti Isohookana-Asunmaa), 10-ти регіональним і місцевим українським газетам не дозволили опублікувати інформацію про «справу Г.Гонгадзе» [7].

Переважна більшість громадян переконані, що в Україні існує політична цензура.

Більше двох третин (69,4%) респондентів, опитаних УЦЕПД у жовтні 2000р., вважають, що політична цензура в Україні «існує» або «скоріше існує». Крім того, більше половини (52,3%) громадян погоджуються з думкою іноземних експертів, які включили Україну до списку 10-ти держав, в яких свобода слова порушується найбільше (не погоджуються — лише 17,5%).

Наявність політичної цензури в Україні визнається на міжнародному рівні. Моніторинговий та Юридичний комітети ПАРЄ ухвалили рішення звернутися до Бюро ПАРЄ (керівний орган Асамблеї в період між її сесіями) з пропозицією включити до порядку денного січневої (2001р.) сесії ПАРЄ окремим питанням дебати зі справи Г.Гонгадзе [8]. Проблемам свободи слова і цензури в українських ЗМІ відводиться значна частина ефірного часу зарубіжних радіопрограм — «Радіо Свобода», ВВС та ін.

Намагання ввести цензуру в мережі Інтернет шляхом розширення повноважень силових структур викликає особливе занепокоєння.

Україна частково повторює російський шлях: у Росії спеціальна система оперативно-розшукових заходів, що дозволяє контролювати зміст повідомлень електронної пошти, учасників електронної комерції, була впроваджена

в 2000р. [9] Аналогічні заходи намагалися запровадити й в Україні, причому за рахунок операторів мережі. Однак, відповідні зміни до Закону України «Про підприємництво», подані Президентом України, були відхилені Верховною Радою [10]. Зроблено ще одну спробу впровадити ці положення — шляхом прийняття Закону України «Про телекомунікації». Законопроект передбачає розширення повноважень Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України щодо контролю інформаційних потоків в інформаційних мережах. У законопроекті міститься також спірне положення (п.1 статті 46) про узгодження (не ознайомлення, а саме узгодження) операторами телекомунікаційних мереж своїх інвестиційних програм, проектів будівництва мереж, а також надання послуг міжміського та міжнародного зв'язку з Генеральним штабом ЗС та Службою безпеки України.

Наведені дані свідчать про намагання органів державної влади впровадити політичну цензуру в Україні в друкованих та електронних ЗМІ, мережі Інтернет, причому як на загальнодержавному, так і на регіональному рівні [11]. В існуванні політичної цензури впевнена переважна більшість громадян України, і ця проблема вже отримала розголос у міжнародних організаціях. Впровадження політичної цензури суперечить демократичним перетворенням у суспільстві, обмежує права громадян на отримання та поширення інформації, формує в світі імідж України як недемократичної держави.

Тиск на ЗМІ з метою зміни їх політичного курсу. Економічні санкції.

У січні 1998р. було припинено видання газети «Правда України». За свідченням колишнього голови Комітету Верховної Ради з питань законодавчого забезпечення свободи слова та засобів масової інформації В.Понеділка, наказ щодо припинення виходу газети «було забезпечено надто блискавичними, жорсткими, узгодженими діями абсолютно не підпорядкованих Міністерству інформації відомств — митниці, ДП «Укрпошта», податкової адміністрації, Контрольно-ревізійного управління, Міністерства фінансів, місцевої державної адміністрації і, що найстрашніше, — Міністерства юстиції та Генеральної прокуратури України» [12]. В жовтні 2000р. було призупинено вихід газети «Сільські вісті» — Державна податкова адміністрація оштрафувала редакцію газети на суму понад 2 млн. грн. За свідченням народного депутата України І.Бокія, було заборонено продавати редакції папір та друкувати газету. Такі дії розцінювалися як наслідки політичної орієнтації газети, що перебуває в опозиції до діючої влади [13]. Журналісти видання заявили про намір оголосити з 17 жовтня 2000р. безстрокове сухе голодування, до відміни заборони на вихід газети. Наприкінці жовтня 2000р. газета поновила друк [14].

Тиск посадових осіб на судову владу.

В грудні 2000р. міністр оборони О.Кузьмук направив листа голові Верховного Суду В.Бойку, в якому намагався втрутитися в діяльність судових органів з метою зміни окремих судових рішень. Зокрема, міністр стверджував,

що судова влада була упередженою, коли визнала неправомірними претензії підприємства «Струм» до газети «Сегодня»[15].

Невиправдано високі суми відшкодування моральної шкоди як засіб тиску на ЗМІ.

В 1999р. до ЗМІ було подано 2258 позовів, згідно з якими вони мали сплатити позивачам понад 90 млрд. грн. [16], що в кілька разів перевищує обсяг державного бюджету України. Примітно, що 55% позовів були ініційовані державними службовцями. За свідченням голови Національної спілки журналістів України І.Лубченка, подібні позови розглядаються в п'яти-шести судах щоденно [17]. За даними Фонду гласності, до 70% таких справ мають відверто недобросовісний характер і спрямовані на приборкання преси фінансовими засобами.

При цьому, термін «моральна шкода» не має чіткого визначення в українському законодавстві. За кілька рядків тексту позивач може вимагати сплати багатотисячних і навіть мільйонних компенсацій, виплатити які ЗМІ не в змозі [18]. Так, за цитування народного прислів'я до тижневика «Зеркало недели» був поданий позов у розмірі 50 млн. грн. Сума компенсації, яку повинна була сплатити газета «Киевские ведомости» міністру внутрішніх справ Ю.Кравченку, становила 9 млн. грн. За три з половиною роки існування газети «День» до неї подали 45 судових позовів на суму 3,5 млн. грн. [19] Лише за І півріччя 2000р. до журналістів Вінницької обл. подано 13 судових позовів, за якими позивачі вимагають відшкодувати понад 163 тис. грн. за завдану журналістськими матеріалами моральну шкоду [20].

Переважна більшість громадян України впевнена в необхідності обмеження суми компенсації моральної шкоди. Такої думки дотримуються більше двох третин (69,4%) респондентів, опитаних УЦЕПД у жовтні 2000р. Примітно, що протест проти абсурдних сум компенсації моральної шкоди висловила й міжнародна правозахисна організація «Репортери без кордонів».

Необхідність обмеження сум судових позовів до ЗМІ не викликає сумніву. Наступними кроками мають стати: утворення Експертних рад досудового розгляду позовів до ЗМІ, розробка методик обчислення сум відшкодування і, головне, — забезпечення незалежності судових органів.

Прояви політичного екстремізму стосовно до журналістів набувають форми фізичних розправ.

За даними міжнародної неурядової організації Комітет захисту журналістів [21], у 2000р. в світі при виконанні своїх професійних обов'язків загинули 24 журналісти (в цьому списку є й прізвище Г.Гонгадзе). За роки незалежності до українських журналістів неодноразово застосовували насильницькі методи, окремі журналісти загинули за загадкових обставин. Примітно, що жертвами насилля ставали представники ЗМІ, які проводили журналістські розслідування, публікували критичні матеріали про владу або кримінальні угруповання. Таємничо загинули народний депутат України, журналіст В.Бойко, черкащанин І.Грушецький, кримчанин О.Мотренко, одесит

Б.Дерев'янко. І цей список не є вичерпним. Методи фізичного насильства застосовувалися до журналістів І.Сподаренка, В.Скачка, І.Погорєлової, О.Ляшка та ін. [22].

Переважна більшість (68,4%) громадян, опитаних УЦЕПД у жовтні 2000р., вважають, що серед негативних наслідків, яких можуть зазнати журналіст або видання після публікації критичних матеріалів, найбільш імовірною є фізична розправа над журналістом. З приводу тривожної ситуації в інформаційному просторі Верховна Рада прийняла 15 червня 1999р. Звернення до Ради Європи, ОБСЄ, міжнародних парламентських організацій, парламентів і урядів європейських країн, аби «об'єднаними зусиллями ... відстояти конституційні положення щодо захисту ... свободи думки і слова, вільного вираження поглядів і переконань». 13 грудня 2000р. пройшло засідання Комітету ПАРЄ з питань культури та освіти, присвячене ситуації зі свободою слова в Україні. Згідно з заявою членів Комітету, вони «дуже стурбовані повторенням актів агресії, переслідувань і вбивств журналістів. Ніякої свободи слова не може бути в атмосфері терору і страху» [23].

Значна частина випадків насильства та загибелі представників ЗМІ не розкриті правоохоронними органами. На жаль, фізичні розправи над журналістами посилюють так звану самоцензуру, обмежують професійні можливості журналістів. Їх загибель породжує атмосферу страху не лише серед журналістського корпусу, а й у суспільстві загалом. Це стримує демократизацію суспільного життя, створює негативний імідж України в світі.

Неприбутковість більшості ЗМІ суспільно-політичного спрямування зумовлює їх залежність від держави та фінансово-політичних кіл.

Переважна частина українських ЗМІ є малорентабельними або взагалі збитковими, а тому вони розподілені між впливовими фінансово-політичними колами. Низька рентабельність ЗМІ зумовлена наступними чинниками.

Високі ціни на папір.

Ціна на друкарський папір є досить високою, до того ж вона постійно зростає. Тонна офсетного паперу на початку 2001 р. коштувала $800-900, газетного – $650-700 (у травні 2000 р. – $500-520). Високі ціни на папір роблять видання більшості друкованих ЗМІ нерентабельним. За оцінками фахівців, рентабельними є видання, що мають щоденний тираж біля 100 тис. примірників. Таких газет в Україні одиниці – більшість же мають тираж на рівні 3000-4000 примірників.

В Україні склалася критична ситуація із забезпеченням видання друкованої продукції власним папером. Потреби складають 80-90 тис. тонн газетного та офсетного паперу щорічно, причому вітчизняні паперові комбінати випускають лише 25% необхідних обсягів. До того ж, якість вітчизняного паперу є низькою, а тому більшість газет і друкарень взагалі від нього відмовляються. За цих умов, Росія – як монопольний постачальник паперу – має змогу диктувати цінову політику (закупки в інших державах обходяться ще на 15-20% дорожче).

Невиправдано високі податки.

На відміну від Росії, в Україні податком на додану вартість оподатковуються папір, друкування газет і журналів (поліграфічні послуги), що підвищує їх собівартість. Крім того, існує ввізне мито на поліграфічне обладнання та імпортний папір. Навіть добровільні пожертви та гранти оподатковуються податком на прибуток у розмірі 30%.

Монополізація окремих видів послуг.

Державне підприємство «Преса України» (входить до сфери управління «Укрпошти») фактично є монополістом на ринку друкарських послуг, насамперед, газет формату А2 та 16-полосних видань. Окремі типографії надають послуги на 20-25% дешевше, ніж «Преса України», однак вони не мають розгалуженої системи розповсюдження преси в регіонах. Укладаючи договори на друкування видань у 2001р., ДП «Преса України» обумовило можливість призупинення виконання замовлень на будь-якому етапі, виходячи з власних міркувань. Не виключено, що ця договірна умова може слугувати підставою для припинення виходу того чи іншого видання з причин політичного характеру [24].

ДП «Укрпошта» — це єдина організація-монополіст, що здійснює доставку преси в регіони залізницею; їй належать усі поштові вагони. Законом встановлені досить високі тарифи на доставку преси — до 40% собівартості видання [25]. Створення конкурентного підприємства «АМИР Киевские ведомости», що розгорнуло власну мережу доставки преси в регіони автотранспортом, дало можливість друкованим ЗМІ зменшити відповідну статтю витрат на 20-25%, порівняно з вартістю послуг ДП «Укрпошта» [26]. Що стосується роздрібного продажу преси, то ця сфера поступово переходить на ринкові засади, однак у багатьох регіонах монополія підприємств колишньої державної мережі кіосків «Союздрук» зберігається дотепер.

В Україні монополізовані й інші галузі надання інформаційних послуг: міжнародний, міжміський та місцевий телефонний зв'язок, первинна магістральна мережа телекомунікацій, мережі передачі даних та ін. З боку державних структур спостерігається намагання закріпити таке становище. Так, законопроект «Про телекомунікації» (стаття 29) передбачає передачу прав оперативно-технічного управління мережами всіх операторів зв'язку Національному центру на базі ВАТ «Укртелеком» — монополіста в цій галузі. В Указі Президента України «Про деякі заходи щодо захисту інтересів держави в інформаційній сфері» № 346 від 22 квітня 1998р. визначені лише три підприємства, які можуть здійснювати передачу даних за кордон: ВАТ «Укртелеком», «Укркосмос», «Інфоком», що теж є видом монопольного обмеження.

Обмеженість рекламного ринку.

Надходження від рекламних послуг не забезпечують розвиток українських ЗМІ. За експертними оцінками, ринок телевізійної реклами складає $35 млн. на рік, що в 10 разів менше обсягів російського або польського ринку. За цих умов, навіть провідні телекомпанії можуть покрити лише поточні

витрати. До того ж, у 2000р. значно знизили активність на українському рекламному ринку компанії Procter & Gamble та Stimorol, що входять до п'ятірки найбільших рекламодавців. Рекламний ринок може ще більше скоротитися, оскільки Національна Рада України з питань телебачення і радіомовлення вирішила встановити граничні розцінки на рекламні послуги на загальнонаціональних телеканалах (за погодженням із Міністерством фінансів), що по суті є антиринковим заходом. До того ж, Рада вимагає від телекомпаній надавати інформацію про рекламодавців, договори з ними, ціни на рекламні послуги тощо. По суті, такі дії Ради порушують права компаній стосовно конфіденційної інформації та комерційної таємниці.

Обмеженість інвестицій.

Внаслідок політичної нестабільності, неефективної податкової політики, відсутності крупних вільних капіталів всередині країни серйозні інвестиції в розвиток українських ЗМІ є скоріше виключенням, аніж правилом. Порівняно кращі показники мають Студія «1+1», Інтер, «Новий канал». До того ж, українське законодавство обмежує частку іноземних інвестицій у статутному капіталі вітчизняних телерадіомовних організацій лише 30% від його загального обсягу, що не сприяє залученню зовнішніх інвесторів.

Вибіркова фінансова підтримка ЗМІ з боку держави створює нерівні фінансові умови діяльності періодичних видань. Так, 23 серпня 2000р. Кабінет Міністрів прийняв рішення про пільгову доставку через ДП «Укрпошта» 106-ти періодичних видань [27]. Крім того, державні друковані ЗМІ мають додаткові переваги — вони отримують папір із державного резерву за цінами, приблизно на 30% нижчими від ринкових. Водночас, держава не надає належної підтримки дитячим, культурологічним, освітнім і науковим виданням, що є більш важливим за нинішніх умов.

Зазначені фактори зумовлюють неприбутковість переважної частини ЗМІ, особливо суспільно-політичного спрямування [28]. Це не дає можливості реалізувати інформаційні проекти як бізнесові, здатні приносити прибуток. Поява нових інформаційних продуктів у країні практично завжди чітко зорієнтована на виконання завдань політичного характеру в інтересах засновників, державних кураторів або фінансових груп, які орієнтуються на діючу владу. Тому фактично всі телерадіоканали та переважна частина друкованих ЗМІ розподілені між впливовими фінансово-політичними колами. ЗМІ зорієнтовані не стільки на поширення інформації, скільки на здійснення впливу на владу, суспільство і на розвиток політичного процесу. Функція інформування зводиться до мінімуму, перетворюється на пропагандистську. ЗМІ монопольно залежать від фінансових спонсорів і практично не залежать від потреб громадян — споживачів їх продукції. ЗМІ стають важливим елементом політичного капіталу, доводять «корисність» фінансово-політичних угруповань для влади. Це породжує самоцензуру журналістів, поширення необ'єктивної інформації, зниження соціального статусу журналістів, особливо в регіонах, плинність кадрів у ЗМІ та інші негативні явища.

За умов, що склалися, журналісти центральних видань не можуть почувати себе вільними у висвітленні суспільно-політичних подій у країні, їм загрожує втрата роботи з досить високим рівнем оплати [29]. Журналісти, які працюють у державних ЗМІ, прирівняні за своїм статусом до державних службовців, теж не можуть бути вільними в своїх діях. Це негативно позначається на об'єктивності матеріалів, а відтак — порушує права громадян на отримання достовірної інформації, знижує довіру до журналістів. За даними опитування, проведеного УЦЕПД у грудні 2000р., журналістам повністю довіряють лише 18,9% громадян України (вчителям — 52,2%, політикам — 2,8%).

Попри значне число журналістів, відчувається брак професіоналів високого рівня (попит на яких відчутно зростає в період виборчих кампаній). Це породжує практику переманювання журналістів з одного ЗМІ до іншого, запрошення журналістів з інших країн.

На жаль, кращі вітчизняні фахівці залишають політичну журналістику, переходять до іншої, наприклад, розважальної сфери. Помітно зростає й кількість анонімних публікацій — користуючись псевдонімом, журналісти (а також пересічні громадяни, державні службовці) намагаються донести до громадськості інформацію з найгостріших питань і водночас уникнути можливих утисків.

Місцеві ЗМІ мають незначну фінансову підтримку, яка, до того ж, обмежується короткими сплесками політичної активності в період виборів. Тому журналісти місцевих видань практично не мають можливості знайти гідно оплачувану роботу — їх місячний заробіток становить 150-250 грн. Це знижує престиж професії журналіста.

На думку більшості (52,6%) громадян, опитаних УЦЕПД у жовтні 2000р., саме фінансова незалежність ЗМІ та журналістів найбільшою мірою сприяла забезпеченню свободи слова в Україні. Більше третини (37,7%) респондентів переконані, що необхідно змінити ставлення до ЗМІ з боку органів державної влади [30].

Поширення неправдивої або конфіденційної інформації про особу без її згоди.

Цей чинник негативно впливає на стан інформаційної безпеки, порушує права громадян. В Україні широко розповсюджена практика замовних статей з метою дискредитації окремих громадян і посадових осіб, в яких оприлюднюється свідомо неправдива або конфіденційна інформація [31].

Майже половина респондентів (49,2%), опитаних УЦЕПД у жовтні 2000р., погоджуються з тим, що в Україні існує практика замовних статей. Ще 28,5% опитаних скоріше погоджуються з цим (протилежної думки дотримуються лише 6,2% респондентів).

Неправдива інформація і так званий «компромат» активно поширюються через Інтернет [32]. Для цього створюються навіть спеціалізовані web-сайти, наприклад, compromat.ru. Розміщена в Інтернет інформація, навіть як-

що web-сайти зареєстровані в інших державах, поширюється дуже швидко і може нанести моральної шкоди громадянам України. Таким чином в Інтернет були розповсюджені неправдиві відомості, наприклад, про народного депутата України А.Деркача, які передрукували українські видання [33].

Потенційні можливості для поширення конфіденційної інформації про особу (без її згоди) створені в довідкових службах, житлово-експлуатаційних конторах, бібліотеках, кадрових органах, лікарнях та інших установах, в яких зберігаються персональні дані. Доступність цієї інформації створює передумови для протиправних дій, в т.ч. шантажу або компрометації громадян [34].

Отже, поширення свідомо неправдивої або конфіденційної інформації стає важливим чинником інформаційної безпеки, завдає шкоди фізичним і юридичним особам, порушує їх права.

Негативний вплив ЗМІ на суспільну свідомість і психіку громадя.

Застосування ЗМІ новітніх технологій дозволяє суттєво впливати на суспільну свідомість населення. Соціологічне опитування, проведене УЦЕПД у лютому 2000р., засвідчило, що громадяни України активно сприймають пропагандистські кліше, які нав'язуються засобами масової інформації, зокрема, в період виборчих кампаній та референдумів [35]. Нерідко досить деструктивним є вплив державних ЗМІ. Приміром, висвітлюючи «справу Г.Гонгадзе», державний телеканал УТ-1 оприлюднює інформацію переважно однобічного спрямування, негативно висвітлює діяльність народних депутатів і загалом дискредитує Верховну Раду як законодавчий орган країни [36]. Це не сприяє розвитку громадянського суспільства, підвищенню ролі й відповідальності Парламенту. Загалом, таку політику керівництва державного телебачення, що фінансується за рахунок платників податків, не можна вважати прийнятною в державі, яка обрала демократичний шлях розвитку.

В інформаційному просторі України переважає інформація негативного змісту. Такий висновокновок експертів УЦЕПД підтверджують і 43% громадян, опитаних соціологічною службою УЦЕПД у грудні 2000р. (діагр. «Інформація, що переважає в інформаційному просторі України»). Протилежну точку зору підтримали лише 15,7% респондентів. З тим, що в інформаційному просторі України переважає інформація, яка сприяє зміцненню поваги громадян до влади, погоджуються лише 15,6% респондентів. Водночас, 43,6% опитаних переконані, що переважає інформація, яка компрометує владу в очах громадян.

Така оцінка інформації пояснюється, з одного боку, тривалим кризовим станом суспільства, неефективними діями владних структур, а з іншого – спрямованістю ЗМІ на висвітлення переважно негативних аспектів життєдіяльності держави та суспільства. Очевидно, що свідомо чи несвідомо, але ЗМІ створюють додатковий негативний вплив на психіку громадян.

Пропаганда насильства, жорстокості та порнографії.

Останнім часом в Україні з'являється все більше фільмів, книг і журналів, у яких пропагуються насильство, жорстокість і порнографія. Моніто-

ринг телеефіру засвідчив, наприклад, що протягом тижня на трьох каналах телебачення (УТ-2 разом зі Студією «1+1», Інтер та СТБ) демонструється в середньому 45 художніх фільмів (не враховуючи телесеріалів), з них до 50% — це фільми з елементами насильства [37]. Водночас, у державному бюджеті на 2001р. не виділено коштів на створення державного телеканалу «Культура», який міг би запропонувати глядачеві альтернативу. Отже, це завдання Програми діяльності Уряду не буде виконане і в 2001р.

Законодавство України не передбачає обмежень на поширення еротичних видань або на показ фільмів з елементами насильства, жахів і порнографії на загальнодоступних телеканалах.

Поширення таких матеріалів у національному сегменті мережі Інтернет також не врегульоване законом. В Україні створений спеціалізований орган — Експертна комісія Міністерства культури і мистецтв України, яка дає висновки щодо наявності в тому чи іншому фільмі елементів порнографії або насильства. На підставі цих висновків, Міністерство приймає рішення про відмову в реєстрації та видачі прокатного посвідчення на: (а) фільми, трансляція яких може завдати шкоди моральному та фізичному вихованню, культурному розвиткові громадян; (б) фільми порнографічного характеру; (в) фільми, що пропагують війну, насильство, жорстокість [38]. Національна Рада України з питань телебачення і радіомовлення заборонила з 1 грудня 2000р. показ таких фільмів по телебаченню до 22:00, але проблема потребує вирішення на законодавчому рівні [39].

Законодавство України не внормовує масову пропаганду вчень та релігійної практики релігійних культів тоталітарного характеру, що поширюються в Україні [40]. Не зроблено належних висновків із судового процесу над керівниками «Білого братства», який офіційно встановив факт деструктивного впливу на психічне здоров'я людини релігійної практики цієї організації, негативного досвіду інших держав.

Між тим, пропаганда новітніх релігійних вчень та релігійної практики, що включає елементи нейро-лінгвістичного програмування людини, набуває поширення через електронні ЗМІ. За даними моніторингу, здійсненого експертами УЦЕПД, обсяг часу телепроповідництва в 2000р. зріс, порівняно з 1999р., у півтора рази; практично на кожному з місцевих радіоканалів ведуть мовлення проповідники новітніх культів, які застосовують методику нейролінгвістичного програмування.

Поширення проповідництва новітніх релігійних культів із застосуванням новітніх методик впливу уможливлює маніпуляцію свідомістю людини і може мати негативні суспільні наслідки, а відтак — потребує більш глибокого вивчення й адекватного реагування з боку держави. Загалом, в інформаційному просторі України є достатньо чинників негативного (іноді деструктивного) впливу на суспільну свідомість і психіку громадян. Результатом їх дії може стати руйнування моральних цінностей, духовного здоров'я людини та суспільства.

Обмеження доступу населення до ЗМІ, позбавлення значної кількості користувачів в Україні доступу до альтернативних джерел інформації

Низький рівень життя громадян України обмежує їх доступ до інформації. Якщо за радянських часів при середній зарплаті 180 руб. (пенсії — 120 руб.) газета коштувала 3-4 коп., то в 2000р. при середній зарплаті 247 грн. (пенсії — 60 грн.) газети в середньому коштували 40-50 коп. Тобто кількість газет, які можна придбати на одну середню зарплату зменшилася в 8-10 разів, на одну пенсію — майже в 25 разів. Зростання цін на газети та журнали в 2001р. лише погіршить ці показники.

Українські вчені не мають фінансових можливостей для доступу до Інтернет-ресурсів. У вересні 2000р. середня зарплата працівників науки становила 335 грн. [41]; водночас, сучасний комп'ютер коштував близько $600, місячний доступ до Інтернет – $20-50, плата за послуги телефонного зв'язку – близько $20. Отже, доступ до Інтернет-ресурсів українському вченому обійшовся б у 10 місячних зарплат (працівнику освіти – 20 зарплат).

Лише 25,1% громадян, опитаних УЦЕПД у грудні 2000р., оцінюють рівень доступності інформації як високий (діагр. «Рівень доступності інформації для населення України»). Водночас, більше третини (36,6%) респондентів вважають його незадовільним. Обмеження доступу широких верств населення до інформації спричиняє «внутрішнє» звуження інформаційного простору України, стримує розвиток інтелектуального потенціалу суспільства.

Недостатня відкритість органів державної влади для громадського контролю. Незважаючи на певні позитивні зміни, порівняно з радянськими часами, органи влади, насамперед — силові структури, залишаються закритими для ефективного громадського контролю. В Україні ще не вдалося створити дієву систему зворотних зв'язків між владою і громадськістю, вплив населення на прийняття важливих державних рішень практично відсутній. Об'єктивна й повна інформація про діяльність державних структур недоступна не лише пересічним громадянам. Приміром, правоохоронні органи дозволяють собі надавати навіть Парламенту неперевірену, неповну, спотворену, невірну інформацію про розслідування гучних кримінальних справ. Це провокує сумніви, домисли, знижує довіру населення до влади загалом.

Незадовільна практика надання інформації громадянам та організаціям. Фактично, не діє стаття 32 Закону України «Про інформацію», яка регулює питання отримання громадянами інформації від державних органів. Порушуючи вимоги закону, органи державної влади часто ігнорують звернення громадян, надають неповну або недостовірну інформацію – в цьому неодноразово мали можливість пересвідчитися й експерти УЦЕПД.

Про незадовільну роботу державних органів зі зверненнями громадян ідеться і в Першій щорічній доповіді Уповноваженого Верховної Ради України з прав людини. Наприклад, до Міністерства внутрішніх справ у 1999р. надійшло майже 21 тис. звернень, але лише 3550 (16,9%) з них були вирішені [42].

Рішенням Уряду керівникам органів центральної виконавчої влади надане право визначати інформацію для службового користування [43]. По суті, це додаткове (поза рамками закону) обмеження прав громадян на отримання інформації.

Низькою є поінформованість населення про важливі аспекти державної політики. Це засвідчують результати опитувань, проведених УЦЕПД протягом 2000р. Наприклад, лише 11% громадян вважають себе достатньо поінформованими про ситуацію в Збройних Силах, 48% – нічого не чули про зміст указів Президента України стосовно адміністративної реформи, більше половини (53,4%) респондентів – нічого не знають про Програму «Партнерство заради миру», в рамках якої здійснюється співробітництво України з НАТО.

Недостатня відкритість органів державної влади порушує права громадян та юридичних осіб на отримання інформації, унеможливлює створення зворотних зв'язків між владою та громадськістю, є свідченням неефективності державної інформаційної політики.

Нерозвиненість і низькі темпи розвитку інформаційної інфраструктури України.

Комплекс телемовлення. Вичерпуються технічні можливості розвитку телебачення на існуючій технічній базі, залишилося не більше 15-20% неосвоєного частотного ресурсу [44]. Відставання від розвинутих країн в обладнанні телекомунікаційних мереж зв'язку складає в окремих випадках два покоління [45]. Технічне обладнання державного телебачення залишається на рівні 60-70-х років, на нього припадає до 90% загальних витрат на електроенергію в цій галузі. За прогнозами, до 2003р. аналогове телебачення, на якому базується державний комплекс телемовлення, має бути витіснене цифровим.

Комплекс радіомовлення. Через руйнування ліній радіофікації та несвоєчасне їх відновлення, внаслідок відсутності у підприємств необхідних коштів, кількість радіоточок постійно зменшується, особливо на селі. Підгалузь радіомовлення є збитковою (в 1999 р. рентабельність склала мінус 27,5%). Одна з причин – низька абонентська плата за користування радіоточкою (50 коп. на місяць). Крім того, Національна радіокомпанія України з 1997р. не проводить оплату рахунків за користування каналами звукового мовлення для поширення своїх програм – її борг станом на 1 січня 2000р. становив 19,5 млн. грн. [46] Якщо ремонт мережі дротового мовлення в сільській місцевості здійснювати лише за рахунок абонентської плати, то для цього потрібно 10 років. Відсутність коштів не дає можливості здійснити радіофікацію 2200 населених пунктів (7,3% їх загальної кількості) [47].

Поліграфічний комплекс. Потребує докорінного переоснащення матеріально-технічна база державних поліграфічних підприємств. Значну частину заходів, передбачених Державною програмою розвитку національного книговидання та преси на період до 2000р., виконати не вдалося. Протягом

останніх трьох років централізовані капіталовкладення для реконструкції та технічного переоснащення підприємств галузі не виділялися. Можливості підприємств здійснити матеріально-технічне переоснащення за рахунок власних ресурсів є обмеженими. В умовах спаду виробництва, їх потужності використовуються лише на 35-40%. Через два-три роки вийдуть із ладу районні друкарні [48].

Інфраструктура мережі Інтернет. Держава може забезпечити не більше 20% коштів, необхідних для розвитку мережі Інтернет, водночас, сприятливих умов для залучення внутрішніх і зовнішніх приватних інвестицій ще не створено. Законодавчо не визначене правове поле розвитку й використання Інтернет, що не виключає введення правових норм, які будуть стримувати його розвиток.

Податкова політика стосовно компаній, що працюють в Інтернет, теж залишається невизначеною (розповсюдження на них загальних норм оподаткування не завжди відповідає умовам діяльності в середовищі Інтернет [49]). Діяльність Інтернет-провайдерів в Україні є неприбутковою, оскільки кількість користувачів мережі є незначною (і не дає можливості знижувати вартість послуг). Водночас, висока вартість послуг Інтернет-провайдерів, операторів зв'язку, імпортної комп'ютерної техніки та програмного забезпечення стримують розширення кола користувачів мережі. З огляду на наведені чинники, без впровадження податкових пільг розраховувати на крупні інвестиції в інфраструктуру Інтернет немає підстав.

Нерозвиненість інформаційної інфраструктури знижує конкурентоспроможність вітчизняних виробників інформаційних послуг, стримує інтеграцію України в світовий інформаційний простір.

Недосконалість законодавчої бази та механізмів її застосування. Численні факти порушень чинного законодавства свідчать про його неефективність. За результатами перевірок, виявлено 47 організацій кабельного телебачення, що діють без дозвільних документів [50] і надають послуги населенню; 12 інформаційних агентств, що не перереєструвалися відповідно до Закону України «Про інформаційні агентства» та продукують інформацію для радіо та телебачення України [51]. Їх матеріали поширюються з порушенням чинного законодавства, зокрема, про вихідні дані. В Україні діють 29 телерадіокомпаній, які повністю або частково передали власні канали мовлення іншим юридичним або фізичним особам, що забороняється законом. 7 грудня 2000р. Національна Рада України з питань телебачення і радіомовлення попередила зазначені телерадіомовні організації про порушення чинного законодавства, в т.ч. норм, за якими власна (українська) продукція телерадіоканалів повинна складати не менше 50% її загального обсягу [52]. За експертними оцінками, в Україні 90% аудіо-відеоринку займає продукція піратського походження [53]. В країні виробляється 75 млн. неліцензійних компакт-дисків, що експортуються до країн СНД, Центральної та Східної Європи [54].

Недосконалою є правова база, що регламентує використання новітніх інформаційних технологій та визначає нові види злочинів, вчинених з їх використанням [55]. Такий висновок підтверджують наступні приклади. В Україні активно створюються Інтернет-видання, видаються електронні копії друкованих ЗМІ, однак ця сфера діяльності не врегульована чинним законодавством. Закон не визначає такі поняття, як «електронна форма контракту», «електронний цифровий підпис» — це стримує впровадження систем електронного документообігу, розвиток в Україні електронної комерції [56].

Невирішеною залишається проблема адміністрування української доменної зони .ua. Зараз воно здійснюється не в Україні, а в США, що з багатьох причин є неприйнятним. Важливим кроком на шляху створення Національного реєстратора доменних імен зони .ua стало підписання 16 листопада 2000р. спеціального Меморандуму між Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ та вітчизняними Інтернет-провайдерами. Окремі експерти висловлюють застереження щодо можливого надмірного втручання в цю сферу з боку держави (тим більше, що інтереси держави представляє правоохоронний орган — СБУ). В переважній більшості країн світу національні реєстратори створюються виключно провайдерами.

З метою збагачення нерідко реєструються домени, назва яких співпадає з прізвищами відомих політиків, кіноакторів, співаків, компаній. Законодавче регулювання цих питань в Україні є недостатнім, спеціалізовані судові (позасудові) органи, які б мали їх розглядати, відсутні [57].

В Україні недостатньо розвинуті норми кримінального законодавства, що визначають коло та види злочинів з використанням новітніхінформаційних технологій, встановлюють покарання за їх вчинення. Стаття 198-1 Кримінального кодексу «Порушення роботи автоматизованих систем» неповністю охоплює склад злочинів, які можуть бути вчинені з використанням Інтернет, зокрема, шляхом проведення «хакерських» атак; неточно відображає об'єкт злочинного зазіхання.

Наприклад, законом встановлено кримінальну відповідальність за «розповсюдження технічних і програмних засобів для незаконного втручання в автоматизовані системи і здатних спричинити перетворення або знищення інформації чи то носіїв інформації». Таке формулювання може мати надто широке тлумачення. Навіть законні дії (продаж комп'ютерів) можна вважати такими, що підпадають під дію цієї статті, оскільки саме за допомогою комп'ютерів здійснюється таке «втручання». Теоретично, можна притягти до відповідальності й за продаж звичайного молотка як «технічного засобу», який був використаний для «знищення носіїв інформації» (дискет) [58]. Складність застосування зазначеної статті обумовлена й тим, що доводити винність особи у вчиненні злочину із застосуванням новітніх технологій досить важко [59], тим більше, що в правоохоронних органах України немає достатньої кількості досвідчених у цій сфері фахівців.

Неузгодженими є принципи національного законодавства з європейським. Прикладом може слугувати внесений до Верховної Ради законопроект «Про телекомунікації», який суттєво розширює втручання держави в інформаційну сферу, повноваження державних органів щодо ліцензування та сертифікації, що суперечить принципам адміністративної реформи в Україні та законодавству Європейського Союзу.

Загалом, чинне законодавство не створило надійних запобіжних механізмів, які б унеможливили (мінімізували) нанесення шкоди фізичним і юридичним особам України за умов впровадження новітніх інформаційних технологій. Отже, воно потребує вдосконалення.

Зовнішні чинники ескалації загроз.

Зовнішні чинники негативного впливу на інформаційну безпеку України зумовлені протиріччями між національними інтересами України та інтересами іноземних суб'єктів економічної та політичної діяльності. До основних зовнішніх чинників ескалації загроз можна віднести наступні.

Діяльність іноземних розвідок та інших організацій, спрямована на отримання інформації з обмеженим доступом. За даними правоохоронних органів України, іноземні спецслужби щороку докладають чималих зусиль, щоб отримати в нашій державі доступ до таємної інформації. На початку 2000р. Службою безпеки України були виявлені сім агентів іноземних спецслужб з числа громадян України (в 1999р. — 10), депортовані 117 осіб [60].

У сфері захисту воєнно-економічного потенціалу лише за матеріалами військової контррозвідки протягом 1999р. було порушено понад 400 кримінальних справ, засуджено 176 злочинців, попереджено заподіяння збитків державі на суму 55 млн. грн. і понад $15 млн., повернуто до бюджету держави 7,5 млн. грн. [61].

Підрозділи української контррозвідки запобігли спробі громадянина однієї з країн Азіатсько-тихоокеанського регіону одержати від посадових осіб України в обхід існуючого порядку технологічну документацію на ремонт деяких видів військової техніки. Якби його афера вдалася, це могло б обернутися Україні економічними втратами на суму понад $500 тис. [62].

Аналогічні спроби спостерігаються з боку іноземних країн, компаній, різноманітних фондів з метою незаконного використання інтелектуального потенціалу України. За експертними оцінками, до 20% крупних і середніх компаній в Україні є об'єктом комерційного шпигунства.

Для збору інформації з обмеженим доступом використовуються й законні методи: контракти з вченими, науковими установами, коли за невеликі суми купуються винаходи або результати багаторічних досліджень вітчизняних науково-дослідних установ; програми фінансово-технічної допомоги, в рамках виконання яких отримується доступ до інформації конкуруючих компаній, збирається інформація про кон'юнктуру українського ринку тощо.

В Україні рівень захищеності інформаційних мереж є недостатнім, що створює передумови для витоку інформації з обмеженим доступом. З початку 2000р. Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ в Україні розпочаті роботи по створенню системи державної експертизи засобів і систем захисту інформації. Впроваджені базові нормативні документи в сфері технічного захисту інформації [63]. Однак, за оцінками фахівців, все ще недостатньо захищена інформація з обмеженим доступом, що використовується органами державної влади, конфіденційна інформація громадян, а також інформація, що містить комерційну таємницю [64].

За експертними оцінками, проблема захисту службової (нетаємної) інформації, що передається через канали Інтернет, залишається нерозв'язаною. Це питання вже протягом кількох років знаходиться на «вирішенні» в згадуваному Департаменті, але конструктивних рішень, крім відключення від комп'ютерних мереж, поки що не запропоновано [65].

Потенційні можливості для несанкціонованого витоку (блокування, спотворення тощо) інформації з обмеженим доступом створює й закупівля державними органами комп'ютерів та засобів зв'язку з програмним забезпеченням, не адаптованим до вимог замовника. Приміром, закупівля комп'ютерів за рубежем не виключає можливості встановлення так званих «закладок» ще на рівні виробника. Відповідні команди щодо блокування системи можуть бути закладені і в програмному забезпеченні, в т.ч. при проведенні його оновлення. В ЗМІ вже ставилося й інше актуальне питання — щодо необхідності пошуку балансу між інтересами держави та зарубіжних компаній, що поставляють спеціальну техніку для військових формувань України [66].

Отже, витік таємної, конфіденційної та іншої важливої інформації становить реальну загрозу інформаційній безпеці України. Її ескалація може призвести (і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру для держави, завдання шкоди юридичним і фізичним особам України.

Міжнародна комп'ютерна злочинність (комп'ютерний тероризм). Розвиток комп'ютерних мереж та інформаційних технологій супроводжується поширенням комп'ютерної злочинності. За оцінками, розповсюдженими на X Конгресі з профілактики злочинності (квітень 2000р., Відень), загальний дохід від комп'ютерних злочинів становить $500 млн. на рік. За даними ФБР, у 1999р. в США число злочинів, пов'язаних із використанням комп'ютерів, порівняно з 1998р., подвоїлося (із 547 до 1154) [67]. Збитки від комп'ютерних злочинів сягають $3,5 млрд. на рік і збільшуються щорічно на 35%; збитки від середнього комп'ютерного злочину складають $560 тис. [68].

За даними американського Інституту комп'ютерної безпеки *(Computer Security Institute)*, найбільш широко хакерами використовуються наступні методи: підбір ключів, паролів (brute-force) — 13,9% від загальної кількості; заміна IP-адрес [69] *(IP-spoofing)* — 12,4%; ініціювання відмови в обслуговуванні [70] *(denial of service)* — 16,3%; аналіз трафіку [71] *(sniffer)* —

11,2%; сканування [72] *(scanner)* — 15,9%; підміна, нав'язування, переупорядкування або зміна даних, що передаються мережею *(data didling)* — 15,6%; інші методи — 14,7% [73].

В Україні комп'ютерна злочинність ще не набула значних масштабів, але її прояви вже зафіксовані. Так, у 1995р. з банку «Україна» шляхом проникнення до його комп'ютерної мережі було викрадено майже $4 млн. (злочинця вдалося виявити). В 1997р. на кілька годин була заблокована робота українського Інтернет-провайдера «Глобал Юкрейн» (і, відповідно, — його численних клієнтів: державних установ, банків, підприємств та ін.) через те, що російська фірма «Демос» буквально завалила сервери «Глобал Юкрейн» «електронним сміттям». У грудні 2000р., за інформацією головного інженера компанії «УкрСат» І.Дядури, були здійснені кілька «атак» з метою знищення офіційного web-сайту Президента України [74]. Тоді ж, у грудні 2000р., була зафіксована інформаційна диверсія проти Інтернет-провайдера «УкрНет», що мала на меті отримання інформації про поштові скриньки компанії. Зростає кількість випадків шахрайства з платіжними картками: кількість таких випадків становить 3% від загального обсягу здійснених операцій, тоді як максимально допустимий рівень складає 0,3-0,7%.

Отже, міжнародна (і внутрішня) комп'ютерна злочинність становить реальну загрозу інформаційній безпеці України внаслідок слабкої захищеності інформації з обмеженим доступом та високого рівня залежності комп'ютерних мереж від іноземних виробників програмного забезпечення.

Високий рівень присутності зарубіжних держав в інформаційному просторі України. На каналах українського телебачення (включаючи офіційні), в кіно- та відеопрокаті переважає зарубіжна продукція, перш за все, виробництва США та Росії [75]. Майже 13% телеаудиторії України [76] постійно переглядають програми РТ — завдяки супутниковій трансляції, кабельним мережам, звичайному прийому в прикордонних областях.

На 2000р. для передплати в Україні було запропоновано 1995 назв газет і журналів Росії і лише 846 — України. Щоденний тираж видань «Аргументы и Факты. Украина», «Комсомольская правда. Украина», «Труд. Украина», «Известия. Украина» складає понад 807 тис. примірників. Ці газети зареєстровані в Україні, але публікують переважно матеріали базових, російських видань. Деякі російські газети та журнали поставляються до України контрабандним шляхом.

В результаті, російські ЗМІ здійснюють помітний вплив на формування громадської думки в Україні, про що свідчать дані про рівень довіри до них з боку українського населення. За результатами опитування, проведеного УЦЕПД у жовтні 2000р., повністю та деякою мірою довіряють російським телеканалам 38,1% респондентів; радіостанціям — 33%; друкованим ЗМІ — 28,3%.

На книжковому ринку України панівне становище, за експертними оцінками, посідають російські видання. Це призводить, зокрема, до значних

фінансових втрат. За даними Державного комітету телебачення і радіомовлення, до 40 млн. книжок російського походження ввозяться в Україну нелегально. На кожного жителя України припало три книги російського походження, проданих в Україні. В результаті, Україна втратила близько 500 млн. грн. [77].

Високий рівень присутності зарубіжних ЗМІ в українському інформаційному просторі, за умови низької конкурентоспроможності вітчизняних мас-медіа, зумовлює можливість формування громадської думки в інтересах зарубіжних держав, а також здійснення інформаційних експансій проти України.

Спрямований інформаційний вплив на Україну та її суб'єктів з боку іноземних держав або конкуруючих компаній. Аналіз світового та вітчизняного досвіду інформаційної діяльності дозволяє дійти висновку про існування потенційної загрози проведення проти України підготовлених інформаційних операцій. В розвинутих країнах інформаційна зброя стала однією з головних складових воєнного потенціалу, яка дозволяє перемагати в локальних воєнних конфліктах або розв'язувати воєнні конфлікти взагалі без застосування збройних сил. У Стратегії національної безпеки США для нового століття інформаційні війни розглядаються серед головних загроз національним інтересам Сполучених Штатів [78]. Спеціальні інформаційні операції не обмежуються воєнно-політичною сферою. Об'єктами інформаційної експансії можуть бути економічні структури (як державні, так і недержавні).

Україна вже неодноразово була об'єктом інформаційних диверсій. Як правило, напередодні укладання українськими підприємствами контрактів на поставку зброї або надання військово-технічних послуг у зарубіжних ЗМІ розпочинаються масовані кампанії зі звинувачення України в постачанні зброї до «гарячих» точок: танків і літаків для талібів; танків для Уганди, вертольотів для Сьєрра-Леоне; танків і літаків для руху УНІТА [79]. З цього приводу начальник Управління контролю над озброєнням та військово-технічного співробітництва МЗС України О.Семенець зазначив: «Неодноразові ретельні розслідування, проведені як компетентними відомствами України, так і спеціальними групами експертів ООН, підтвердили безпідставність та бездоказовість таких заяв. Можна припустити, що ця інформація створюється «на замовлення» і є проявом недобросовісної діяльності конкурентів України на світовому ринку озброєнь [80].

Можливості ж України в поширенні якісної об'єктивної інформації обмежуються її слабкими позиціями в світовому інформаційному просторі. До нинішнього часу країна не має повноцінного супутникового телеканалу та цілодобового закордонного радіомовлення: останнім часом обсяги закордонного радіомовлення скоротилися більш ніж удвічі, досяжність – зменшилася майже втричі; єдиною телеорганізацією, що веде мовлення через супутник, є недержавний канал СТБ. У державному бюджеті на 2001р. кошти на створення державного супутникового каналу не передбачені. Українське державне

телебачення характеризується недостатнім творчим рівнем програм, відтоком кваліфікованих фахівців, відсутністю розгалуженої закордонної інформаційної мережі, застарілим технічним забезпеченням, що призводить до нездатності конкурувати з іноземними телевізійними компаніями. Українська книга також не може конкурувати зі своїми зарубіжними аналогами – ні за якістю видання, ні за ціною [81].

Недостатньо ефективною залишається робота Державного інформаційного агентства України (Укрінформу). Кореспондентська мережа агентства зорієнтована переважно на збір закордонних новин для України, а не на продукування та поширення інформації про Україну через зарубіжні агентства та ЗМІ.

Спрямований негативний інформаційний вплив на Україну та її суб'єктів може призвести до втрат політичного, економічного, воєнного та іншого характеру. Запізнення із проведенням державою відповідних контрзаходів призводить до погіршення репутації України та її економічних суб'єктів, до фінансових втрат у зовнішньоекономічній діяльності. Міжнародний імідж України формується переважно зарубіжними ЗМІ, які діють в інтересах інших держав або економічних конкурентів України.

Високий рівень конкуренції на світовому ринку інформаційних послуг та технологій. Значний економічний ефект впровадження комп'ютерних засобів та новітніх інформаційних технологій в усі сфери виробництва, ефективність їх використання для забезпечення оперативності, адекватності управління зумовлюють високий рівень конкуренції на світовому ринку інформаційних послуг та технологій. Крім того, входження до світового інформаційного простору вимагає уніфікації інформаційних технологій за стандартами найбільш розвинутих країн. Це дозволяє їм диктувати в цій сфері свої правила розвитку, посилювати політичне та економічне лідерство.

Водночас, впровадження новітніх інформаційних технологій об'єктивно веде до створення глобального інформаційного простору, що засвідчує, зокрема, стрімкий розвиток мережі Інтернет, яка охоплює вже 228 країн світу [82]. Кількість користувачів Інтернету в світі у серпні 2000р. становила 660 млн. чол., щодня мережа поповнюється 189 тис. персональних комп'ютерів.

Високого ступеню інтегрованості в світовий інформаційний простір можуть досягти лише країни з високим науково-технічним потенціалом і культурно-освітнім рівнем населення. Про це свідчить та обставина, що близько 90% користувачів Інтернет проживають у розвинутих країнах, частка населення яких становить лише 15% населення світу.

Стан і темпи продукування та впровадження новітніх інформаційних технологій в Україні не відповідають світовим тенденціям розвитку глобального інформаційного простору, внаслідок чого українська інформаційна продукція та послуги є недостатньо конкурентноспроможними.

За даними опитування, проведеного УЦЕПД у грудні 2000р., 43% громадян оцінили рівень інформатизації українського суспільства як низький, ли-

ше 14,3% – як високий. Потужна конкуренція на ринку інформаційних послуг та технологій у поєднанні з низькою конкурентоспроможністю української інформаційної продукції та послуг ставлять під сумнів перспективи інтеграції України в світове інформаційне співтовариство в найближчому майбутньому. Слід відзначити, що 40% громадян, опитаних УЦЕПД у грудні 2000р., оцінюють рівень інтегрованості України в міжнародний інформаційний простір як низький, лише 8,5% – як високий.

Враховуючи основні тенденції сучасного світового розвитку, можна стверджувати, що держави, які не мають відповідних передумов для інтеграції в світовий інформаційний простір, ризикують залишитися на узбіччі світової цивілізації. Така перспектива загрожує новим поділом країн світу за ознакою рівня розвитку інформаційної сфери.

Негативні тенденції розвитку інформаційного простору України, неефективність державної інформаційної політики, кризовий стан економіки країни, створюють передумови для ескалації загроз інформаційній безпеці України.

За окремими ознаками, рівень інформаційної безпеки в Україні наближається до критичної межі, за якою — втрата демократичних принципів і засад діяльності держави, повернення до авторитаризму, ізоляція України на міжнародній арені.

Сьогодні саме чинники політичного характеру провокують ескалацію головних загроз інформаційній безпеці, ставлять під сумнів реалізацію прав українських громадян на свободу слова. Передусім, це впровадження політичної цензури, тиск на ЗМІ, прояви політичного екстремізму стосовно журналістів, недостатня відкритість органів державної влади для громадського контролю, перетворення ЗМІ на засоби масової пропаганди.

Органи державної влади намагаються впровадити політичну цензуру в друкованих та електронних ЗМІ, мережі Інтернет, причому як на загальнодержавному, так і на регіональному рівні. В існуванні політичної цензури впевнена переважна більшість громадян України; проблема свободи слова в Україні отримала розголос в міжнародних організаціях. Впровадження політичної цензури суперечить демократичним перетворенням у суспільстві, обмежує права громадян на отримання та поширення інформації, формує в світі імідж України як недемократичної держави.

З метою зміни політичного курсу ЗМІ на них здійснюється тиск шляхом економічних санкцій, вибіркової фінансової підтримки з боку держави, невиправдано високих сум відшкодування моральної шкоди, втручання посадових осіб у діяльність судової влади.

Непоодинокими є прояви політичного екстремізму щодо ЗМІ, які набувають форм фізичної розправи з журналістами. Значна частина випадків насильства над журналістами та їх загибелі не розкриті правоохоронними органами. Фізичні розправи над журналістами посилюють так звану самоцензуру, обмежують професійні можливості представників ЗМІ. Їх загибель породжує

атмосферу страху не лише серед журналістського корпусу, а й у суспільстві загалом. Це стримує демократизацію суспільного життя, створює негативний імідж України в світі.

Тяжкий податковий прес на ЗМІ, високі ціни на папір, монополізація окремих видів інформаційних послуг, обмеженість рекламного ринку та інвестицій, низька платоспроможність населення зумовлюють неприбутковість переважної частини ЗМІ, особливо суспільно-політичного спрямування. Це не дає можливості реалізувати інформаційні проекти як бізнесові, здатні приносити прибуток.

Поява нових інформаційних продуктів у країні практично завжди чітко зорієнтована на виконання завдань політичного характеру в інтересах засновників, державних кураторів або фінансових груп, які орієнтуються на діючу владу. Тому фактично всі телерадіоканали та переважна частина друкованих ЗМІ розподілені між впливовими фінансово-політичними колами.

ЗМІ зорієнтовані не стільки на поширення інформації, стільки на здійснення впливу на владу, суспільство і на розвиток політичного процесу. Функція інформування зводиться до мінімуму, перетворюється на пропагандистську. ЗМІ монопольно залежать від фінансових спонсорів і практично не залежать від потреб громадян — споживачів їх продукції. ЗМІ стають важливим елементом політичного капіталу, доводять "корисність" фінансово-політичних угруповань для влади. Це породжує поширення необ'єктивної інформації, самоцензуру журналістів, зниження їх соціального статусу, особливо в регіонах, плинність кадрів у ЗМІ та інші негативні явища.

Кращі вітчизняні фахівці залишають політичну журналістику, переходять до іншої, наприклад, розважальної сфери. Помітно зростає й кількість анонімних публікацій — користуючись псевдонімом, журналісти (а також пересічні громадяни, державні службовці) намагаються донести до громадськості інформацію з найгостріших питань і водночас уникнути можливих утисків.

Низький рівень життя громадян України обмежує їх доступ до інформації. Українські вчені не мають фінансових можливостей для доступу до Інтернет-ресурсів. Обмеження доступу широких верств населення до інформації спричиняє «внутрішнє» звуження інформаційного простору України, стримує розвиток інтелектуального потенціалу суспільства.

В інформаційному просторі України існують чинники негативного (іноді деструктивного) впливу на суспільну свідомість і психіку громадян, що уможливлює маніпуляцію свідомістю людини і може мати негативні суспільні наслідки. Результатом дії цих чинників може стати руйнування моральних цінностей, духовного здоров'я людини та суспільства.

Органи державної влади залишаються недостатньо відкритими для громадського контролю, що порушує права громадян та юридичних осіб на отримання інформації, унеможливлює створення зворотних зв'язків між владою та громадськістю, є свідченням неефективності державної інформаційної політики.

Недосконалою є правова база, що регламентує використання новітніх інформаційних технологій та визначає нові види злочинів, вчинених з їх використанням. Численні факти порушень чинного законодавства свідчать про його неефективність. Неузгодженими є принципи національного законодавства в інформаційній сфері з нормами міжнародного права.

Витік таємної, конфіденційної та іншої інформації з обмеженим доступом становить реальну загрозу інформаційній безпеці України. Її ескалація може призвести (і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру для держави, завдання шкоди юридичним особам і громадянам України.

Реальну загрозу інформаційній безпеці України становить комп'ютерна злочинність – внаслідок слабкої захищеності інформації з обмеженим доступом та високого рівня залежності комп'ютерних мереж від іноземних виробників програмного забезпечення.

Високим є рівень присутності зарубіжних ЗМІ в інформаційному просторі України, що за умови низької конкурентоспроможності вітчизняних масмедіа зумовлює можливість формування громадської думки в інтересах зарубіжних держав, а також здійснення інформаційних експансій проти України.

Україна та її суб'єкти зазнають спрямованих негативних інформаційних впливів, що може призвести до втрат політичного, економічного, воєнного та іншого характеру. Відсутність ефективної профілактики, запізнення із проведенням державою відповідних контрзаходів призводить до погіршення репутації України та її економічних суб'єктів, до фінансових втрат у зовнішньоекономічній діяльності. Міжнародний імідж України формується переважно зарубіжними ЗМІ, які діють в інтересах інших держав або економічних конкурентів України.

Потужна конкуренція на світовому ринку інформаційних послуг та технологій у поєднанні з низькою конкурентоспроможністю української інформаційної продукції та послуг за умови збереження нинішньої ситуації ставлять під сумнів перспективи інтеграції України в світове інформаційне співтовариство в найближчому майбутньому.

Враховуючи провідні тенденції сучасного світового розвитку, можна стверджувати, що держави, які не мають відповідних передумов для інтеграції в світовий інформаційний простір, ризикують залишитися на узбіччі світової цивілізації. Така перспектива загрожує новим поділом країн світу за ознакою рівня розвитку інформаційної сфери.

Посилання:

1. Інформаційна безпека України: Виклики для Національної безпеки держави. – Національна безпека та оборона, 2001, №10.

Шафрански Р.

ТЕОРИЯ ИНФОРМАЦИОННОГО ОРУЖИЯ *

При демократии общество контролирует выбор средств, которые используют люди в процессе своей деятельности, в том числе и средств вооруженной борьбы. Только в том случае, если намерения людей имеют под собой как моральную основу, так и технологическую, этот выбор будет разумен. Но если о моральности не задумываются, то возникает эффект домино: теряется поддержка со стороны общества, не используются передовые достижения технологии, и в результате вооруженные силы остаются без средств вооруженной борьбы. В рамках данного подхода данная статья постулирует теорию информационного оружия в общем контексте средств вооруженной борьбы и предлагает способы использования информационного оружия на стратегическом и оперативном уровне.

Сейчас уже имеются средства, позволяющие создать информационное оружие, и так как информационное оружие является таким мощным оружием, как войска, так и гражданское население должны быть защищены от него. К воздействию информационного оружия уязвимы все. Правительство должно принять решение — разрабатывать ли средства информационного оружия или преследовать в судебном порядке тех, кто разрабатывает такие средства. Это решение должно быть принято на основании тщательного анализа всех деталей и с пониманием моральных и этических рисков информационного оружия. Помимо учета всех рисков при принятии решения о создании информационного оружия, люди должны понимать принципы действия этих средств и теорию их использования до того как они начнут применяться.

Под информацией будем понимать содержимое или значение сообщения. Целью средств вооруженной борьбы является воздействие на информационные системы врага. В широком смысле информационные системы включают в себя все средства, с помощью которых противник получает знания или выдвигает гипотезы (knowledge and belief systems). Для военных информационные системы представляют собой средства, посредством которых противник получает информацию о состоянии боевых действий и управляет войсками. В совокупности информационные системы являются объединением знаний, гипотез, процессов принятия решения и систем противника. Результатом информационных атак на любом уровне является дать противнику информацию, заставляющую его прекратить вооруженные действия.

По какой причине противник может прекратить боевые действия? Существует ряд возможных причин: невозможность управлять вооруженными силами, деморализация, получение информации (истинной или предполо-

* http://psyfactor.org/infowar3.htm

жительной) о том, что войска уничтожены, или о том, что более выгодно прекратить войну, чем продолжать воевать. Эти «сообщения» о прекращении войны могут различаться как по содержимому, так и по смыслу, как например: «Ваша контратака провалилась» или «Ваши собственные люди не поддерживают вас в войне, в которой убивают детей». Хотя методы передачи сообщений, вынуждающих прекратить войну, могут меняться, смысл сообщений остается неизменным — прекратить войну.

По мере развития социальных институтов информационные системы усложнялись, а процессы принятия решения становились все более сложными. Финансово-промышленные организации, возникшие на базе доминантных политических структур увеличивали сложность систем по мере увеличения своей деятельности. Появились сети информационных взаимосвязей между работниками умственного труда — самая современная форма институциональной структуры, и их количество, а также доступность средств информационной технологии резко увеличилась.

По мере развития информационной технологии информационные системы привели к появлению знания, или ноу-хау, которое позволяло делать остальные институциональные формы более эффективными.

По мере развития социальных институтов совершенствовались и способы вооруженной борьбы между людьми. Устрашающие звуки барабана, знамена и гонги времен Су Цзы при информационной технологии стали утонченными психологическими операциями.

Целью войны стало не уничтожение, а управление, согласно Джону Аркуилле и Давиду Ронфельдту. Информационная технология в наше время делает возможным «управление» при минимальном насилии и кровопролитии. На первый взгляд это кажется хорошим. Но при внимательном рассмотрении это может оказаться опасным. Тщательный анализ поможет определить, что это на самом деле.

Что такое вооруженное столкновение(warfare)? Вооруженное столкновение — это ряд смертоносных и не приводящих к смерти процессов, предпринимаемых для подавления враждебных действий противника.

В этом смысле вооруженное столкновение не является синонимом «войне». Вооруженное столкновение не требует объявления войны, или существования условия, понимаемого людьми как «состояние войны». Вооруженное столкновение организуется группами людей, контролируемыми государством, финансируемыми государством или действующими самостоятельно. Вооруженное столкновение — это враждебные действия по отношению к врагу. Целью вооруженного столкновения не обязательно является убить врага. Цель вооруженного столкновения — просто покорить врага. Фактически верхом мастерства является покорение врага без его смерти. Противник покорен, когда он ведет себя таким образом, что его действия соответствуют тем, которые мы, агрессор или обороняющийся, ждем от него.

Пытаясь подчинить себе волю врага, мы должны иметь четкое представление о том, какое невраждебное поведение мы от него ожидаем, и какого враждебного поведения мы хотим избежать.

Когда вооруженные силы одного государства сталкиваются с вооруженными силами другого государства, правительство определяет, какое невраждебное поведение ожидалось от врага. Когда в вооруженном конфликте сталкиваются две группировки — клана или партизанских отряда — лидер группы решает, какое невраждебное поведение желательно. В обоих случаях лидерами групп принимаются решения по определению целей, методов и желаемого постконфликтного состояния.

Поэтому является мифом, хотя и распространенным и удобным, что в вооруженном столкновении участвуют государства или группы.

Решение организовать вооруженный конфликт, включая решение прекратить вооруженный конфликт, принимается лидерами государства или группы.

Аналогично, именно враждебные намерения вражеских лидеров должны быть подавлены, чтобы вооруженное столкновение было успешным. Члены групп или граждане государства, могут повлиять на решение лидера, но подавляться должна враждебность именно верхушки. Если лидерство переходит к другому человеку или группе людей, то должна быть подавлена враждебность именно этой группы. Информационная война может помочь отобрать ореол «избранников небес» у вражеских лидеров.

Величайшим открытием, которое привело к началу информационной эры, было понимание того, что все в окружающем мире может быть представлено в виде комбинации нулей и единиц. Эти комбинации могут быть переданы в электронном виде как данные и собраны на приемном конце, образуя информацию.

Согласно плодотворной работе Аркуиллы и Ронфельдта, информация — Это нечто большее, чем содержимое или смысл сообщения. Скорее, информация — Это «любое различие, которое создает различие». Информационная война — это форма конфликта, в которой происходят прямые атаки на информационные системы как средство для воздействия на знания или предположения противника. Информационная война может проводиться как часть большего и более полного набора военных действий — сетевой войны (netwar) или кибервойны (cyberwar) — или выступать в качестве единственной формы ведения военных действий. Большинство видов оружия — слова, используемого для описания смертельных и несмертельных средств ведения вооруженного конфликта — может быть применена только против внешних врагов. Средства же ведения информационной войны, хотя чаще всего и применяются против внешних врагов, могут быть использованы и против внутренних противников. Например, государство или группа обычно не использует пушки или бомбы против своих граждан или членов; тем не менее, средства ведения информационной войны могут быть использованы, использовались, и будут

использоваться как против внешних, так и против внутренних врагов. Информационное оружие в Третьем Рейхе, например, было всенаправленным.

Информационная война – это вооруженные действия, направленные против любой части систем знаний или предположений врага. «Противник» – это любой, чьи действия противоречат целям лидера. Вне государства это может быть «образ врага» или «не мы».

Внутри, врагом может быть предатель или путешественник, любой, кто противостоит или недостаточно поддерживает лидера, который управляет средствами информационной войны. если члены группы не поддерживают цели лидера в ходе боевых действий, внутренняя информационная война (включая такие вещи, как пропаганда, ложь, террористические акты и слухи) могут быть использованы в попытке заставить их быть более лояльными к целям лидеров.

Вооруженное столкновение и его связь с тем, что мы знаем или предполагаем. Независимо от того против какого врага она объявлена, информационная война имеет конечной целью использовать информационные средства для воздействия (манипулирования или атаки) на системы знания и предположений некоторого внешнего врага. В ходе войны, например, для внешнего врага полезно знать, или, по крайней мере, предполагать, что другое государство или группа объединились против него. Информационная война, которая ведется как для того, чтобы граждане государства действовали согласованно, так и для того, чтобы внешние враги полагали, что их враг воюет с ними единым строем, используется для доведения этого знания до умов лидеров противника.

Слабость знаний и предположений. Системы знаний — это системы, которые созданы и действуют для выявления верифицируемых феноменологических индикаторов или десигнаторов, трансляции этих индикаторов в воспринимаемую реальность, и использования этих первичных ощущений для принятия решения и действий. Системы знаний организуются в соответствии с научными принципами и подкрепляются научным методом. То есть, системы знаний созданы, чтобы собирать эмпирические данные путем наблюдений для выдвижения гипотез, проводить тесты, подтверждающие или отвергающие эти гипотезы, и использовать эти открытия как основу дальнейших действий. Системы предположений — это такие системы, которые прямо или косвенно ориентированы на использование как эмпирических данных в форме верифицируемых наблюдений, так и данных другого сорта или недостоверных данных(кошмары, фобии, психозы, неврозы, и все другие порождения подсознания, и коллективное бессознательное), которые не подтверждаются, или которые, по крайней мере, нелегко подтвердить.

Согласно Джону Бойду на процесс или акт ориентации (то что Бойд называет большим О в цикле наблюдение-ориентация-принятие решения) также могут повлиять генетическое наследие или культурные традиции. Поэтому ориентация американских лидеров отличается от ориентации, ска-

жем, японских или китайских лидеров. Ориентация капиталистов и их лидеров отличается от ориентации социалистов и их лидеров.

В отличие от систем знаний системы предположений являются очень индивидуальными.

Почему? Они включают в себя элементы бессознательного и подсознательного, о которых их носитель может и не подозревать.

Хотя целью информационного оружия и являются умы лидеров врага, будет ошибкой думать о враге как об одном уме. На самом деле враг — это много отдельных врагов, и у каждого свой ум. Но это только слегка усложняет проблему.

Например, если враг рассредоточен, то отдельные умы могут быть атакованы по отдельности, используя факт изоляции в свою пользу атакующими. если же враг сконцентрирован (и более половины людей планеты будет жить в городах к 2020 году и будет доступна воздействию большого числа информационных атак), атаки должны проводиться против большой группы людей.

Даже если так, целью вооруженной борьбы является подавить враждебные намерения лидеров и лиц, принимающих решение. Это может быть сделано с помощью прямых атак, воздействующих на знания или предположения лидеров или манипуляцию с ними, или косвенных атак, направленных на знания или предположения тех, на кого лидеры полагаются при принятии решения. Лидеров и лиц, принимающих решение, обычно легко выявить в любой организации. Когда организация имеет средства вооруженной борьбы, как правило у этой организации есть иерархическая характеристика.

Поэтому знания и предположения лиц, принимающих решение, являются ахиллесовой пятой иерархий.

Системы знаний, так как они более научны, являются менее подверженными культурным и иррациональным факторам, чем системы предположений, но как системы знаний, так и системы предположений входят в состав каждой системы принятия решения, где есть люди.

То, что известно, включая методы, с помощью которых оно стало известно, может быть проверено в связи с чем-либо еще и определено как либо верное, либо неверное, правдивое или ложное. Предположения не подвергаются всем этим проверкам. Более того, предположения не менее значимы, чем эмпирически полученные знания. Как знания, так и предположения влияют на принятие человеком решения. Так как целью вооруженной борьбы является повлиять на поведение противника путем влияния на принятие им решения, информационные атаки должны быть направлены как против систем знаний, так и против систем предположений.

Если противник представляет собой коалицию нескольких центров, в этой коалиции может существовать несколько систем предположений. Все они могут быть побеждены. Коалиция не обязательно должна быть

группой государств или объединением групп людей. Коалиция может быть образована людьми внутри государства или какой-либо группы. Клаузевиц был прав, когда сделал вывод о потенциальной слабости союзов и коалиций.

Более того, лидеры и лица, принимающие решение, представляют собой более выгодную цель для прямых или косвенных атак.

Эпистемиология целей атак. Система — цель информационной войны может включать любой элемент в эпистемиологии противника. Эпистемиология включает в себя организацию, структуру, методы и достоверность знаний. На стратегическом уровне цель кампании информационной войны — повлиять на решение противника, и как следствие, на его поведение таким образом, чтобы он не знал, что на него воздействовали. Даже тогда, когда этой цели трудно достичь, она все-таки остается конечной целью кампании на стратегическом уровне. Успешная, хотя и незавершенная информационная кампания, проведенная на стратегическом уровне, приведет к решениям противника (а следовательно и его действиям), которые будут противоречить его намерениям или мешать их выполнению.

Успешная информационная кампания, проведенная на оперативном уровне, будет поддерживать стратегические цели, влияя на возможность врага принимать решения оперативно и эффективно. Другими словами, целью информационных атак на операционном уровне является создание таких помех процессу принятия решения врагом, чтобы противник не мог действовать или вести войну координировано и эффективно. В информационной войне целью является гармонизация действий на оперативном уровне с действиями на стратегическом уровне, чтобы объединенные, они заставляли противника принимать решения, которые бы приводили бы к действия, которые помогали достигать нам наших целей и мешали бы противнику добиваться выполнения своих.

На стратегическом уровне лидерам, продумывающим план ведения информационной кампании, нужно знать ответы как минимум на три вопроса:

Во-первых, какова связь информационной кампании с глобальными целями кампании?

Во-вторых, что мы хотим, чтобы вражеские лидеры знали или предполагали по завершению кампании? То есть, каково желаемое эпистемиологическое состояние и следовательно критерий успеха операции?

В-третьих, какие средства ведения информационной войны являются лучшими для достижения установленного критерия успеха? То есть как будут связаны средства с результатом?

На операционном уровне нашим лидерам также нужно иметь ответы на ряд вопросов.

Будет ли запрещено атаковать некоторые цели и применять некоторые средства в информационных атаках? Достижимо ли желаемое эпистемиологическое состояние вообще и везде, или только существуют промежу-

точные состояния, достижимые в специфических географических районах, в специфической последовательности, или в специфических секторах информационных боевых действий. Кроме того, следует ответить на вопросы об управлении и сигналах.

Кроме того, лидерам на оперативном уровне нужно знать, когда будут завершены атаки и средства, посредством которых будет передан сигнал о прекращении атаки. Это важные вопросы, так как информационное оружие может вызвать косвенное разрушение систем знаний и предположений у атакующих.

В худшем случае ответ противника может включать контратаки против дружественных информационных систем, что по большому счету не отличается от побочных разрушений «огневой поддержки».

Цели атак в информационной войне. Чем более зависим противник от информационных систем при принятии решения, тем более он уязвим к вражескому манипулированию этими системами. Программные вирусы воздействуют только на те системы, в которых есть программы. Средства радиоэлектронной борьбы могут быть применены только против вооруженных сил, использующих радио и электронику. Электромагнитные пушки не будут воздействовать на вражеских курьеров. Хотя эти и предполагает, что только постиндустриальные государства или группы уязвимы в информационной войне, обратное также может иметь место по двум причинам. Во-первых, доиндустриальное или аграрное общество все-таки имеет уязвимые эпистемиологические системы. Так как информационная война может вестись против всей эпистемиологии врага в целом, то и примитивные общества уязвимы в информационной войне. Во-вторых, индустриальные общества могут приобрести большую часть их телекоммуникационной структуры у более развитых постиндустриальных обществ.

В государствах или группах с высоким уровнем развития техники набор целей атак на стратегическом уровне очень богат: телекоммуникации и телефония, космические спутники, автоматизированные средства ведения финансовой, банковской и коммерческой деятельности; энергосистемы; культурные системы; и весь набор оборудования и программ, на основании которых враг получает знания. Стратегические информационные системы в высокотехнологичных государствах часто дублируются на оперативном уровне. Все они уязвимы для атаки. Информационная война не должна откладываться до тех пор, пока враждебность не станет открытой. Лидеры противника не захотят воевать, если они предполагают одно из следующего: что насилие — это плохо, или что у них не будет союзников, или что на них будут наложены санкции, препятствующие продолжению войны, или что их индустриальная база не сможет обеспечить победу в длительной войне, или что их вооруженные силы не готовы.

Чем выше технологические возможности государства и чем больше число его взаимодействий с другими группами(включая внутренние груп-

пы) или государствами, тем более государство уязвимо в информационной войне. Эта уязвимость будет возрастать по мере увеличения размеров сетей или числа и объема транзакций.

Демократии не являются менее уязвимыми, чем тоталитарные режимы, хотя демократические социальные системы, такие как группы, могут быть несколько более устойчивыми к выводу из строя. Но аппарат управления ее экономикой уязвим. Банки, финансы, торговля, путешествия и управление воздушным движением становятся все более зависимыми от информационной технологии.

По мере того, как растет зависимость от информационных систем, вооруженные конфликты, организуемые террористами, религиозными экстремистами, враждебными бизнесменами, против информационных систем будут составлять реальную угрозу. Информационное оружие в их руках может быть направлено на Энергосистемы или средства связи, обслуживающие конечную цель. Одновременные атаки на различные узлы могут иметь стратегический эффект. То есть они могут воздействовать на знания и волю лидеров.

Шимілл Т., Уїльямс Ф., Данлеві К.
ПРОТИДІЯ ЕЛЕКТРОННІЙ ВІЙНІ*

Термін "електронна війна" викликає в уяві багатьох людей зловісні смертоносні програми, що спричиняють зупинку комп'ютерних систем, вихід з ладу систем озброєння та знищують звеличувану технологічну досконалість у безкровній боротьбі. Це уявлення, в якому кібернетична війна, ізольована від більшого конфлікту, ведеться в абсолютно іншому просторі, ніж традиційні військові дії і являє собою безкровну альтернативу небезпеці та втратам сучасної війни, є досить привабливим, проте нереалістичним. Такий сценарій можливий, але маловірогідний. Електронна війна майже обов'язково матиме реальні фізичні наслідки.

З розвитком комп'ютерних технологій у структурі сучасних військових організацій, спеціалісти з військового планування почали сприймати їх як ціль і як зброю, тобто, як будь-які інші складові й сили військових ресурсів. Як і інші компоненти сучасного військового потенціалу, електронні сили, вірогідно, будуть інтегровані в загальну бойову стратегію як складова об'єднаної військової кампанії. Проте комп'ютерні технології відрізняються від інших військових ресурсів, оскільки вони є невід'ємною частиною інших складових сучасних армій. З такої точки зору їх можна розглядати, як принципово важливий компонент, від якого залежить діяльність багатьох військових структур, чим при нагоді можуть скористатися вороги.

В усіх країнах світу розробляються і впроваджуються кібернетичні технології, що мають завдати шкоди системі контролю і управління супро-

* НАТО ревю – http://www.universum.org.ua

тивника, його тиловому забезпеченню, транспорту, системам раннього попередження та іншим важливим елементам збройних сил. Дедалі більше держав усвідомлює важливість використання кібернетичних стратегій, які можуть відіграти ключову роль у вирівнюванні, або й посиленні військового потенціалу. Менші країни, які ніколи не могли б змагатися зі своїми більш потужними сусідами щодо звичайних військових ресурсів, тепер можуть розвинути таку спроможність, доцільне застосування якої може дати їм стратегічну перевагу. Як було зазначено у результатах дослідження, проведеного корпорацією RAND в середині 90-х років, загальні витрати на ведення електронної війни є дуже незначними. Тож не дивно, що країни, військові структури яких є менш залежними від високих технологій, вважають таку залежність потенційною ахіллесовою п'ятою своїх супротивників.

Суспільства та економіка розвинутих постіндустріальних країн є вкрай залежними від взаємопов'язаних комп'ютерних інформаційних та комунікаційних систем. Вдосконалення саме по собі перетворилося на джерело вразливості, яку можуть використати супротивники. Виведення з ладу цивільних інфраструктур може стати привабливою можливістю для країн і недержавних сил, що прагнутимуть розпочати асиметричну війну, але є неспроможними у традиційному військовому сенсі. Інформаційні інфраструктури є настільки важливими, що дедалі більше і більше країн розглядають атаку проти них як еквівалент стратегічного удару.

Традиційна межа між війною та миром стає нечіткою. Такий розвиток подій можна було передбачити ще за часів холодної війни, але він став очевидним під час боротьби з тероризмом, що розпочалася після 11 вересня, коли терористи атакували Міжнародний торговельний центр і Пентагон. Можна передбачити, що комп'ютерні інформаційні системи держав НАТО стануть ціллю постійних атак нетрадиційних ворогів, головною метою яких є фізичне знищення та виведення з ладу, і які не залишать поза увагою будь-яке слабке місце.

У цьому контексті важливо зазначити, що кібернетична війна не зводиться до знищення веб-сайтів супротивної нації, організації або політичного руху. Навіть, якщо такі заходи супроводжують інші ворожі дії (як це відбувалося під час повітряної кампанії НАТО в Косові в 1999 році), такі напади на веб-сайти мають радше сприйматися як своєрідна форма навмисного дратування або хуліганських написів на стінах, а не як справжня електронна війна. Однак існує щонайменше три рівні електронної війни: електронна війна як компонент військових операцій; обмежена електронна війна і необмежена електронна війна.

Коли сучасні збройні сили беруть участь у військових діях, головною метою стає досягнення інформаційної переваги або інформаційного домінування в бойовому просторі. Це потребує виведення з ладу ворожої системи протиповітряної оборони, блокування і/або знищення радарів, таке інше. Головна мета, в термінології Клаузевіца, згустити "туман війни" для супро-

тивника і розвіяти його для власних сил. Цього можна досягти прямими ударами, спрямованими на підрив ворожих систем інформації, обробки даних і зв'язку, або через напад на ці системи зсередини, тобто не через знищення системи, а через позбавлення її спроможності функціонувати. Така форма електронної війни зосереджується майже виключно на військових електронних цілях.

Обмежена електронна війна передбачає, що інформаційна інфраструктура розглядається, як засіб, ціль та зброя для здійснення нападу, майже без (або зовсім без) застосування реальних заходів на підтримку нападу. Як засіб, інформаційна інфраструктура формує вектор доведення удару до цілі—часто через систему взаємодії між ворогом і його союзниками, що забезпечує обмін даними та користування ресурсами, або через ширшу мережу зв'язку. Внутрішній агент може напряму ввести шкідливу комп'ютерну програму в мережу супротивника.

Як ціль нападу, інфраструктура перетворюється на засіб підриву спроможності супротивника. Комп'ютерна мережа використовується для вдосконалення організаційного забезпечення. Пошкодження мережі зменшує ефективність або унеможливлює виконання операцій, що залежать від функціонування мережі. Погіршення роботи мережі може змусити супротивника вдатися до дублювання засобів проведення операції і відтак виявити свої вразливі місця. Зниження якості даних може навіть змусити супротивника поставити під сумнів адекватність інформації, необхідної для прийняття рішень. Як зброю нападу інфраструктуру можна використати для атаки на саму себе — або через введення шкідливого програмного забезпечення, або через навмисне використання її недоліків. Обмежена електронна війна такого гатунку може вестися задля затримання підготовки супротивника до військового вторгнення, використовуватись як складова економічної боротьби або як засіб маневрування, що супроводжує, як правило, кризу або поглиблення конфронтації між державами.

Однак необмежена електронна війна, на відміну від обмеженої, є більш вірогідною і становить серйознішу загрозу. Цей тип електронної війни має три головних характеристики. По-перше, масштаб її значно більший, як і кількість цілей, серед яких не розрізняються цивільні та військові; не робиться розмежування між внутрішнім фронтом та театром бойових дій. По-друге, необмежена електронна війна має фізичні наслідки і реальні жертви, з яких деякі є результатом навмисних дій, спрямованих на руйнацію і завдання фізичної шкоди, а деякі є наслідком того, що можна назвати "ерозією" системи цивільного контролю і управління в таких галузях, як контроль за повітряним рухом, керівництво службами реагування на надзвичайні ситуації, управління водо- та енергозабезпеченням. По-третє, до фізичних жертв додаються глибокі соціальні та економічні наслідки.

Необмежена електронна війна, як правило, орієнтована на завдання шкоди в ключових галузях національної інфраструктури країни-супротивни-

ка, серед яких енергетика, транспорт, фінанси, водозабезпечення, комунікації, служби надання допомоги в надзвичайних ситуаціях та власне інформаційна інфраструктура. Ця війна не знатиме кордонів між державним і приватним сектором і, за умов достатньої координації і технічної досконалості, матиме як негайні, так і відстрочені наслідки. І нарешті, необмежена електронна війна буде супроводжуватись значними реальними жертвами, економічним і соціальним занепадом.

Пошкодження електронних систем набуває нового значення: вже не йдеться лише про доступ до Інтернету, а про роботу систем, що забезпечують функціонування ключових елементів національних інфраструктур, тобто систем, в яких довгі перебої неприпустимі. Припинення роботи систем виробництва і постачання енергії, наприклад, матиме значні наслідки для діяльності медичних закладів і служб надання допомоги, для забезпечення зв'язку і управління. Неспроможність спеціальних служб великих міст надати адекватну допомогу тим, хто її потребує, призведе не тільки до загибелі людей, а й до втрати довіри до уряду і сумнівів щодо його спроможності забезпечити захист населення і роботу основних служб. Коли стане відомо, що терористичний напад завдав шкоди іншим складовим інфраструктури (зв'язок, транспорт, водопостачання), страх і недовіра населення почнуть роз'їдати соціальну основу суспільства. Напад на фінансову інфраструктуру зашкодить нормальному функціонуванню бізнесу і викличе сумніви щодо безпеки зберігання коштів населення, їх банківських рахунків, інвестицій та особистих заощаджень. Функціонування військової мережі (а в ній використовуються комерційні засоби зв'язку) також загальмується, що вразить систему командування і управління, тилового забезпечення і матиме негативні наслідки для рівня готовності збройних сил і проведення операцій. В умовах необмеженої електронної війни віртуальні атаки можуть мати реальні, істотні й далекосяжні наслідки.

Іронія ситуації полягає в тому, що ті країни (наприклад, Сполучені Штати та їх союзники), які спроможні здобути перевагу і домогтися інформаційного домінування в електронній війні, що є частиною військових операцій, водночас є і найбільш вразливими державами в умовах необмеженої електронної війни. Однак є можливість вжити заходів, що зменшать цю вразливість.

Електронна війна принципово не відрізняється від звичайної реальної війни. Якщо вона ведеться державою, то стає частиною чітко визначеної стратегії й доктрини, елементом військового планування і відбувається в межах конкретних параметрів. В результаті цього існує можливість застосувати аналіз та забезпечити своєчасне запобігання майже так само, як це робиться в умовах звичайних військових операцій. Існує декілька способів зменшення вразливості в умовах електронної війни. Серед них можна назвати передбачення і аналіз, запобігання і стримування, заходи забезпечення оборони, зменшення наслідків завданної шкоди та відновлення.

Твердження Клаузевіца, що війна є продовженням політики іншими засобами, можна застосувати для розробки і впровадження надійної системи запобігання електронній загрозі. Будь-якому нападу, електронному чи звичайному, як правило, передує певна політична конфронтація. Усвідомлення зростання політичної напруги, інформація та аналіз даних щодо розвитку спроможності до електронної війни, виявлення та оцінка ознак підготовки до атаки—все це дає можливість своєчасно запобігти електронному нападу. В процесі розробки методологій запобігання їх можна поєднати з координованою комплексною стратегією виживання, що посилить вірогідність розпізнавання, реагування та відновлення після електронного нападу.

Методології запобігання мають особливе значення в контексті складності виявлення та аналізу досконало розробленої електронної атаки. Розпізнавання нападу на електронну мережу на фоні випадкових факторів (таких, як раптовий сплеск попиту на певну інформацію в мережі) або похибок впровадження (таких, як помилки частини оперативної системи сервера, що забезпечує рух інформації) є досить довгим і важким процесом. Навіть після визначення факту нападу, захист системи потребує кореляції численних даних (якість яких є сумнівною) для кращого розуміння складових факторів атаки. Тільки після цього можна виробити рішення щодо кращої стратегії реагування. Погіршення роботи системи, якості даних та послаблення її потужності ускладнюють цей процес, особливо, якщо дані є сумнівними.

Заходи запобігання та стримування є дуже складними у кібернетичному світі, частково через анонімність нападників. Однак в умовах необмеженої електронної війни майже завжди можна знайти певні натяки на джерело атаки. Отже, одне з питань, на яке країнам НАТО доведеться шукати відповідь, полягає в тому, чи такий напад потребує електронної відсічі, чи удари у відповідь мають завдаватися в реальному світі або чи треба поєднувати обидві можливості. Поняття взаємодії, ескалації та стримування, які нам стали відомі за часів холодної війни, потребують перегляду в світлі нових факторів реальності. Наприклад, стратегія стримування може бути застосованою і в кібернетичному просторі — щонайменше в умовах необмеженого електронного нападу.

Однак є підстави розраховувати на можливість розробки успішної стратегії оборони. В сучасних умовах здійснення електронного нападу агресор майже завжди певний час має перевагу. Але в довгостроковій перспективі переваги отримують захисники електронної мережі, якщо їм вдається визначити засоби здійснення нападу та заблокувати їх через "латання" слабких місць системи та ізоляцію каналів зв'язку мережі. Більше того, інформаційні мережі можна істотно зміцнити. Важливі функції мережі можна ізолювати задля збереження спроможності системи виконувати головне завдання. Фізичний захист системи та відповідна підготовка персоналу зменшує загрозу зловмисних внутрішніх дій. Треба розробити такі засоби захисту та виявлення втру-

чання в мережу, які забезпечать систему запобігання і реагування як для державних, так і для приватних інфраструктур.

І, нарешті, необхідно забезпечити відповідні можливості для зменшення завданої шкоди і відновлення. Технічні розробки мережі мають містити поняття стійкості й живучості системи (що частково пов'язані із наявністю інших засобів виконання основних завдань), з урахуванням важливості одночасної підготовки планів, що забезпечать значно меншу взаємозалежність електронної мережі при стабільному виконанні головних функцій і завдань. Ізольовані локальні мережі, спроможні ефективно і безпечно працювати без широкого розгалуження зв'язку, безумовно, мають великі перспективи.

Все значно легше сказати, ніж зробити. Існує багато різних перепон на шляху вдосконалення захисту електронних мереж від зловмисних дій. Питання безпеки, як правило, привертають увагу після, а не під час розробки електронних мереж. Урядові органи і бізнес-структури мають різне уявлення про безпеку і засоби її гарантування. Залежність від комп'ютерних мереж досить часто сприймається як належне. Межі відповідальності державних структур часто бувають нечіткими та заплутаними через невизначеність та дублювання повноважень. Але всі ці труднощі можна подолати, якщо існує політична воля, організаційне забезпечення, ретельне планування та комплексне впровадження. Оборонне планування має охоплювати і віртуальний світ, якщо ми прагнемо зменшити фізичні втрати в реальному житті.

Шпиро Ш.
СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ И ТЕРРОРИЗМ. НЕОБХОДИМА ЧЕТКАЯ СТРАТЕГИЯ*

11 сентября 2001 года миллионы людей во всем мире в ужасе и оцепенении следили за прямой телевизионной трансляцией террористических атак на Нью-Йорк и Вашингтон. Глобальные средства массовой информации преодолели расстояния, национальные границы и разницу во времени и донесли весь ужас терроризма почти до каждого уголка Земного шара. В нынешней борьбе против терроризма они стали решающим плацдармом боевых действий.

Действенная стратегия в отношении средств массовой информации является существенным элементом международных мер, направленных против терроризма. Вызов, брошенный терроризмом, состоит в следующем: как средства массовой информации в атмосфере жесткой конкуренции смо-

* Журнал «Международная политика» 2001 № 12 – http://www.auditorium.ru/conf/conf5/conf5materials.php?PHPSESSID=86aa891130180c8a4557ac994a3a02da

гут сохранить демократическую ответственность и одновременно предоставить общественности исчерпывающую информацию, не превращаясь при этом во всемирную пропагандистскую трибуну террористов для выражения их ненависти.

Международный терроризм всегда преследовал цель привлечь внимание СМИ к своим насильственным акциям. Особенно в Европе начиная с 70-х годов терроризм превратился, кажется, в инструмент, при помощи которого внимание общественности обращается на политические требования экстремистских маргинальных групп.

Элемент насилия в терроризме зачастую представлялся второстепенным. Важнее было добиться того, чтобы сообщения о нем доминировали в заголовках газетах и телевизионных репортажах. В действительности некоторые европейские террористические группировки, особенно северо-ирландская ИРА и баскская ЭТА в Испании, разработали политику "сведения количества жертв к минимуму": они предупреждали полицию о готовящихся терактах, чтобы можно было бы своевременно эвакуировать людей. Однако эти предупреждения почти всегда были сопряжены с телефонными звонками в местные средства массовой информации, служившие своего рода гарантией того, что у журналистов и операторов будет достаточно времени, чтобы своевременно оказаться на месте предполагаемого взрыва.

Исламские террористы в последние годы не проявляют подобного внимания к жизням людей, напротив, они разработали совершенно четкую стратегию, нацеленную на большое количество человеческих жертв и максимальное освещение событий в репортажах корреспондентов. Если цель террористов состоит в том, чтобы попасть в СМИ, то, как считают некоторые комментаторы [1], ответственные демократические средства массовой информации для предотвращения дальнейших терактов должны снизить уровень своего внимания к терроризму. Но этот подход не учитывает огромное конкурентное давление в отрасли СМИ, которое гарантирует: в какой-нибудь газете или на каком-нибудь телевизионном канале террористы всегда будут услышаны, даже если другие СМИ от их информации откажутся.

Стратегия в отношении СМИ. Так как террористы для достижения своих целей используют средства массовой информации, то война против терроризма должна включать в себя также стратегию в отношении СМИ: ареной современной войны может быть как телевизионный экран, так и настоящее поле битвы. Репортажи о военных действиях в СМИ оказали влияние не только на меры, предпринимаемые другими государствами, они решающим образом повлияли на общественное мнение внутри собственной страны. Это влияние будет увеличиваться в той мере, в какой средства массовой информации благодаря технологическому прогрессу окажутся в состоянии предоставлять информацию быстрее, в большем объеме и лучшего качества.

В современных СМИ решающую роль играет скорость передачи информации. Если во время второй мировой войны сводки новостей за неде-

лю могли подвергаться редакторской и цензурной правке в течение нескольких дней, прежде чем они попадали в эфир, то нынешняя аудитория требует, чтобы информации о сегодняшних конфликтах поставлялась в течение часов или даже минут. Стратегия в отношении СМИ на период конфликтов стала интегральной составной частью каждого военного плана и любой военной операции.

Вьетнам. Стратегия в отношении СМИ во время конфликтов за последние три десятилетия прошла различные фазы. Война во Вьетнаме – первая, которой была приклеена этикетка "телевизионной войны", – впервые внесла в каждый американский дом весь неприкрытый ужас современной войны. Журналистам было разрешено присутствовать при всех боевых действиях, при этом старались убедить общественность, что Соединенные Штаты эту войну выиграют. Однако данная свобода передвижения журналистов означала также, что они были везде и готовили репортажи о вещах, которые военные предпочли бы сохранить в тайне, как, например, информацию о резне в Май Лай в 1968 году [2].

Руководство Соединенных Штатов Америки, включая президента Линдона Б.Джонсона, придерживалось той точки зрения, что следует вести сражения на двух фронтах, один из которых проходит в джунглях Юго-Восточной Азии, другой - у себя дома, это "фронт средств массовой информации". Американский генерал Вильям К.Вестерморленд считал, что молодое поколение журналистов-пацифистов, делавших свои репортажи о Вьетнаме, смешивало объективное освещение событий и политические влияние. Неудачи американских войск во Вьетнаме породили недоверие к СМИ со стороны разработчиков стратегий в области политики безопасности США. После войны во Вьетнаме журналисты воспринимались американскими военными в качестве силы, которую нужно скорее контролировать, чем поддерживать. Эта установка почти два десятилетия накладывала свой отпечаток на американскую стратегию в области средств массовой информации.

Война в Персидском заливе. Во время войны в Персидском заливе в 1991 году эта перемена в отношении СМИ была очевидна. Фундаментальная убежденность: "средства массовой информации были виновны в том, что США проиграли войну во Вьетнаме" – затрудняла свободу передвижения журналистов из-за воспоминаний об их репортажах об американской армии в Юго-Восточной Азии. При разработке своей стратегии в отношении СМИ американские военные учитывали: необходимо контролировать доступ журналистов в зоны ведения боевых действий, чтобы предотвратить появление негативных репортажей, которые могли бы представлять опасность для действий военных.

Результатом стало то, что доступ для средств массовой информации к театру ведения боевых действий в Саудовской Аравии ограничивался теми журналистами, которые получили соответствующее разрешение в американских ведомствах. Лишь около 120 журналистов добились разрешения

делать репортажи обо всех американских частях в Персидском заливе, при этом каждый их шаг контролировался также строго, как доступ к спутниковым телефонам и передающим устройствам. Так как Ирак после развертывания боевых действий выслал практически всех зарубежных журналистов, то мир зависел от драматических репортажей корреспондента Си-Эн-Эн Петера Арнетта из окруженного Багдада.

Телевизионные репортажи о войне в Персидском заливе также существенно отличались от сделанных в свое время во Вьетнаме. Если во время вьетнамской войны на зрителей постоянно обрушивался поток кадров, полных крови, сожженных тел и бесчисленных жертв, то о войне в Персидском заливе телезрители получали по-медицински стерильные картинки о высокоточных, "умных" бомбах, точно поражавших свою цель. Размытые кадры, полученные при помощи закрепленных на ракетах камерах, создавали образ войны скорее в виде безобидной компьютерной игры, а не человеческой трагедии. Использование понятия "хирургические воздушные налеты" создавало впечатление медицинской операции, а не массированных бомбардировок.

Развитие стратегии в отношении средств массовой информации на период конфликтов не ограничивалось только США: в Германии в 90-ые годы политическая сдержанность относительно применения военного насилия за пределами национально-государственных границ постепенно пошла на убыль, когда германские вооруженные силы начали принимать участие в многонациональных операциях под эгидой Организации Объединенных Наций. Чтобы добиться большей легитимации и поддержки общественности, Федеральное министерство обороны преследовало политику открытости в отношении репортажей СМИ о военных операциях за рубежом; первое крупное из них с участием германских соединений – в 1993 году в качестве составной части миротворческого контингента UNSCOM в Сомали – сопровождала целая армия журналистов, численность которых превышала численность задействованных в этой миссии германских военных. Репортажи журналистов способствовали успокоению общественного мнения в Германии, особенно многочисленного электората социал-демократов и "зеленых", которые первоначально отвергали применение военной силы в качестве инструмента внешней политики.

Косово. Четкая стратегия в отношении средств массовой информации с самого начала была интегрирована в планирование НАТО своей операции в Косово в 1999 году. Штаб-квартира НАТО в Брюсселе мастерски инсценировала ежедневные пресс-конференции, которые передавались в прямом эфире по всему миру и сообщали об успехах альянса в борьбе против сербской армии (4). Сербские телестудии и передающие станции подверглись бомбардировкам с целью вывода из строя пропагандистской машины Белграда. Поскольку в Косово журналистов не осталось, то сообщения о ведении боевых действий представляли собой ничто иное как повторение официальной позиции НАТО.

Успех натовской стратегии в отношении средств массовой информации обеспечил высокий уровень общественной поддержки проводимой компании. Человеческая трагедия косовских беженцев затмила собой тот факт, что многие первоначальные утверждения НАТО о развитии событий в реальном театре боевых действий оказались далеки от действительности. Сотни сербских танков, об уничтожении которых поступали сообщения, позднее были показаны целыми и невредимыми, когда после окончания боевых действий они пересекали границу Сербии. Утверждение НАТО о ведении в Косово "чистой войны" породили в СМИ ожидания, которые просто не могли быть осуществимы в условиях современной войны. Недостаточная готовность признать факт ошибочных налетов на мирный конвой уничтожила доверие средств массовой информации к официальной позиции НАТО и дало повод для критики в плане возможной манипуляции со СМИ.

Атаки, приуроченные к лучшему времени вещания. За недавними террористическими атаками на Нью-Йорк и Вашингтон последовал целый поток сообщений в СМИ о терроризме и его причинах. Органически присущее средствам массовой информации противоречие: с одной стороны, предоставлять населению информацию, с другой – посредством этого способствовать террористической пропаганде – наглядно проявилось 10 октября 2001 года в призыве американского президента Джорджа В.Буша ко всем средствам массовой информации мира не транслировать обращения находящегося в розыске террориста бен Ладена(5). Хотя Буш в качестве обоснования своих опасений в отношении трансляции речей бен Ладена привел то, что в них могут содержаться инструкции для т.н. "кротов" (тайных агентов), тем не менее цель предельного уменьшения влияния бен Ладена и его сподвижников в СМИ стала неотъемлемой составной частью американской антитеррористической политики в области безопасности.

Представляется, что даже выбор времени американских военных ударов по "Талибану" был вызван не только военной необходимостью, но и количеством телевизионных включений в лучшее вещательное время: первые американские налеты по Афганистану были произведены в субботу – т.е. в такой день, когда большинство американцев находятся дома, и у них есть время подольше посидеть у телевизора.

Однако когда удары по Афганистану были расширены, американское правительство, похоже, вновь стало преследовать ограничительную стратегию в отношении СМИ. Только очень немногие журналисты получали доступ к тем частям американской армии, которые были задействованы в войне против "Талибана", а пресс-конференции Пентагона ограничивались повторением готовых штампов и историями об успехах американской армии. Следует однако признать, что некоторая информация, касающаяся военных операций, и не должна быть доступна общественности: зачастую военные успехи зависят от внезапности и секретности.

Четкая и открытая стратегия в отношении средств массовой информации. *Однако борьба против терроризма разворачивается* не только в горах Афганистана, но также на улицах американских городов и в европейских столицах. Американское правительство должно посредством четкой и открытой стратегии в отношении средств массовой информации создать прочный фундамент для своих военных ударов и политического наступления.

В рамках военного планирования эффективная стратегия в отношении средств массовой информации должна состоять из трех основных элементов:

- снабжение СМИ информацией, чтобы они могли передавать актуальные сводки и вести репортажи непосредственно с места событий;
- признание ошибок и разъяснение их причин, а также меры по их исправлению;
- достижение определенного уровня открытости по отношению к средствам массовой информации, который усиливает взаимное доверие.

Военные стратеги, занимающиеся СМИ, должны учитывать и потребности средств массовой информации, а не только потребности военных. Необходимо обратить внимание на следующие факторы: сроки сдачи материалов в печать или эфир, технические условия, возможности для киносъемки, соблюдение стандартов передачи информации, правовые условия — с целью создания такой рабочей обстановки, которая способствовала бы и поддерживала бы эффективную подготовку репортажей для СМИ. Каждый журналист знает: отсутствие новостей или старые новости — это плохие новости.

Военное планирование, соответствующее потребностям СМИ, является не циничным использованием средств массовой информации, а еще одним эффективным оружием в войне. В конце концов, террористы также широко используют СМИ, как и все страны, которые пытаются одержать над ним победу.

Перед 11 сентября Усама бен Ладен также хорошо продумал и спланировал свою собственную стратегию в отношении средств массовой информации. Арабская телекомпания "Аль-Джазира", единственная, которая была допущена талибским режимом в Афганистан, транслировала снятые накануне интервью с бен Ладеном и его соратниками, где звучали призывы к священной войне против Соединенных Штатов Америки.

Борьба против международного терроризма обещает быть длительной и сложной. Свободные средства массовой информации являются существенной составляющей демократического общества, они также могут внести свой вклад в защиту демократических свобод. Независимость СМИ гарантирует, что в любой дискуссии будет представлено множество точек зрения. Военачальники должны признать, что передача информации общественности служит не только повышению уровня доверия к правительству, но и усилению моральной основы борьбы с терроризмом.

Международные усилия, направленные против терроризма, требуют

наряду с координацией стратегий в отношении СМИ между правительствами стран, ведущих борьбу против терроризма, еще и участия глобальных средств массовой информации, которые понимают свою демократическую ответственность, причем сегодня более, чем когда-либо. Объективное и критическое освещение событий не противоречит обязанности защищать именно те свободы, которые как раз и пытаются уничтожить террористы. Действенная стратегия в отношении средств массовой информации, направленная на борьбу с терроризмом, должна гарантировать: те свободы, которые хотят защитить страны с демократическим устройством, не будут уничтожены посредством их усилий по борьбе с терроризмом.

ПРИМЕЧАНИЯ

1. Paul Wilkinson The Media and Terrorism? Terrorism and Political Violence? Jg.9, Nr.2, 1997, 51-64
2. В деревне Май Лай американские солдаты уничтожили свыше 100 мирных жителей. Поначалу военные держали информацию об этой резне в секрете, но год спустя она все-таки попала в американские средства массовой информации. Ср., например, Michael Bilton and Kevin Sim Four Hours at My Lai, New York 1992.
3. Susan Carruthers The Media at War, London 2000. - С.113.
4. Ср.: Walter Jertz Krieg der Worte, Macht der Bilder, Bonn 2001[В.Ерц Война слов, власть кадров. Бонн, 2001] Генерал Ерц был пресс-секретарем НАТО во время операции в Косово и отвечал за ежедневные пресс-конференции.
5. Си-Эн-Эн и Би-Би-Си обещали, что эта просьба будет учтена при составлении будущих передач.

ДОКУМЕНТИ

Пятьдесят седьмая сессия
Пункт 84 *с* повестки дня
Резолюция, принятая Генеральной Ассамблеей
[по докладу Второго комитета (A/57/529/Add.3)]
57/239. Создание глобальной культуры кибербезопасности

Генеральная Ассамблея,

отмечая растущую зависимость государственных органов, предприятий, других организаций и индивидуальных пользователей от информационных технологий в плане предоставления насущно необходимых товаров и услуг, ведения дел и обмена информацией,

признавая, что по мере все большего вовлечения стран в информационное общество возрастает необходимость обеспечения кибербезопасности,

ссылаясь на свои резолюции 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о создании правовой основы для борьбы с преступным использованием информационных технологий,

ссылаясь также на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года и 57/53 от 22 ноября 2002 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности,

сознавая, что эффективная кибербезопасность зависит не только от действий государственных или правоохранительных органов и что она должна достигаться превентивными мерами и пользоваться поддержкой во всем обществе,

сознавая также, что кибербезопасность нельзя обеспечить с помощью одной только технологии и что приоритет должен отдаваться планированию кибербезопасности и управлению ее обеспечением во всем обществе,

признавая, что государственные органы, предприятия, другие организации и индивидуальные владельцы и пользователи информационных технологий должны, с учетом их соответствующей роли, знать о соответствующих факторах, угрожающих кибербезопасности, и о превентивных мерах и должны сознавать свою ответственность и принимать меры в отношении повышения безопасности этих информационных технологий,

признавая также, что несоответствия в уровне доступа различных государств к информационным технологиям и их использования могут снизить эффективность международного сотрудничества в борьбе с преступным использованием информационных технологий и в деле создания глобальной культуры кибербезопасности, и отмечая необходимость содействия передаче информационных технологий, в частности развивающимся странам,

признавая далее важное значение международного сотрудничества в целях достижения кибербезопасности посредством поддержки национальных усилий, направленных на укрепление человеческого потенциала, расширение возможностей в плане обучения и занятости, улучшение государственных ус-

луг и повышение качества жизни за счет использования передовых, надежных и безопасных информационно-коммуникационных технологий и сетей и содействия обеспечению всеобщего доступа,

отмечая, что в результате усиливающейся взаимосвязанности информационные системы и сети подвергаются сейчас все более многочисленным и разнообразным угрозам и факторам уязвимости, которые создают для всех новые проблемы в плане безопасности,

отмечая также работу соответствующих международных и региональных организаций над повышением кибербезопасности и безопасности информационных технологий,

1. *принимает к сведению* элементы, прилагаемые к настоящей резолюции, в интересах создания глобальной культуры кибербезопасности;

2. *предлагает* всем соответствующим международным организациям учитывать, в частности, эти элементы для создания такой культуры в любой будущей работе по вопросам кибербезопасности;

3. *предлагает* государствам-членам учитывать эти элементы, в частности, в рамках их усилий по развитию у себя в обществе культуры кибербезопасности при применении и использовании информационных технологий;

4. *предлагает* государствам-членам и всем соответствующим международным организациям учитывать, в частности, эти элементы и необходимость глобальной культуры кибербезопасности при подготовке к Всемирной встрече на высшем уровне по вопросам информационного общества, которая состоится в Женеве 10-12 декабря 2003 года и в Тунисе в 2005 году;

5. *подчеркивает* необходимость содействия передаче информационной технологии развивающимся странам и созданию в них потенциала в целях оказания им помощи в принятии мер в области кибербезопасности.

78-е пленарное заседание, 20 декабря 2002 года

Приложение
Элементы для создания глобальной культуры кибербезопасности

Стремительное развитие информационной технологии изменило то, как государственные органы, предприятия, другие организации и индивидуальные пользователи, которые разрабатывают эти информационные системы и сети, имеют, поставляют их, управляют ими, обслуживают и используют их («участники»), должны подходить к кибербезопасности. Глобальная культура кибербезопасности будет требовать от всех участников учета следующих девяти взаимодополняющих элементов:

а) осведомленность. Участники должны быть осведомлены о необходимости безопасности информационных систем и сетей и о том, что они могут сделать для повышения безопасности;

b) ответственность. Участники отвечают за безопасность информационных систем и сетей сообразно с ролью каждого из них. Участники должны подвергать свои политику, практику, меры и процедуры регулярному обзору и оценивать, соответствуют ли они среде их применения;

c) реагирование. Участники должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и реагированию на них. Они должны обмениваться в надлежащих случаях информацией об угрозах и факторах уязвимости и вводить процедуры, предусматривающие оперативное и эффективное сотрудничество в деле предупреждения таких инцидентов, их обнаружения и реагирования на них. Это может предполагать трансграничный информационный обмен и сотрудничество;

d) этика. Поскольку информационные системы и сети проникли во все уголки современного общества, участникам необходимо учитывать законные интересы других и признавать, что их действия или бездействие могут повредить другим;

e) демократия. Безопасность должна обеспечиваться так, чтобы это соответствовало ценностям, которые признаются демократическим обществом, включая свободу обмена мыслями и идеями, свободный поток информации, конфиденциальность информации и коммуникации, надлежащая защита информации личного характера, открытость и гласность;

f) оценка риска. Все участники должны выполнять периодическую оценку риска, которая: позволяет выявлять угрозы и факторы уязвимости; имеет достаточно широкую базу, чтобы охватить такие ключевые внутренние и внешние факторы, как технология, физические и человеческие факторы, применяемая методика и услуги третьих лиц, сказывающиеся на безопасности; дает возможность определить допустимую степень риска; и помогает выбрать надлежащие инструменты контроля, позволяющие регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации;

g) проектирование и внедрение средств обеспечения безопасности. Участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;

h) управление обеспечением безопасности. Участники должны принять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций;

i) *переоценка.* Участники должны подвергать вопросы безопасности информационных систем и сетей обзору и повторной оценке и вносить надлежащие изменения в политику, практику, меры и процедуры обеспечения безопасности, учитывая при этом появление новых и изменение прежних угроз и факторов уязвимости.

Пятьдесят шестая сессия
Пункт 110 повестки дня
Резолюция, принятая Генеральной Ассамблеей
[по докладу Третьего комитета (A/56/574)]

56/121. Борьба с преступным использованием информационных технологий

Генеральная Ассамблея,

ссылаясь на Декларацию тысячелетия Организации Объединенных Наций, в которой государства-члены провозгласили решимость обеспечить, чтобы благами новых технологий, особенно информационно-коммуникационных технологий, в соответствии с рекомендациями, содержащимися в декларации министров, принятой на этапе заседаний высокого уровня основной сессии Экономического и Социального Совета 2000 года, могли пользоваться все, и на свою резолюцию 55/63 от 4 декабря 2000 года, в которой она призвала государства-члены учитывать меры по борьбе с преступным использованием информационных технологий,

признавая, что свободное движение информации может способствовать экономическому и социальному развитию, образованию и демократическому управлению,

отмечая значительный прогресс в разработке и внедрении информационных технологий и телекоммуникационных средств,

выражая обеспокоенность в связи с тем, что технический прогресс создал новые возможности для преступной деятельности, и в частности для преступного использования информационных технологий,

отмечая, что повсеместное распространение информационных технологий, масштабы использования которых в разных государствах могут быть различными, привело к значительному росту глобального сотрудничества и координации, в результате чего преступное использование информационных технологий может иметь серьезные последствия для всех государств,

признавая, что несоответствия в уровне доступа различных государств к информационным технологиям и их использования могут снизить эффективность международного сотрудничество в борьбе с преступным использованием информационных технологий, и признавая также необходимость содействия передаче информационных технологий, в частности развивающимся странам,

отмечая необходимость предупреждения преступного использования информационных технологий,

признавая необходимость сотрудничества между государствами и частным сектором в борьбе с преступным использованием информационных технологий,

подчеркивая необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием

информационных технологий и отмечая в этом контексте ту роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации,

приветствуя работу десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями,

признавая с признательностью работу Комиссии по предупреждению преступности и уголовному правосудию на ее девятой и десятой сессиях и последующую подготовку плана действий по борьбе с высокотехнологичной и компьютерной преступностью, в котором признается, в частности, необходимость эффективного обеспечения законности и необходимость эффективной защиты конфиденциальности и других связанных с этим основных прав, а также необходимость учета проводимой ныне работы на других форумах,

отмечая работу международных и региональных организаций по борьбе с высокотехнологичной преступностью, включая работу Совета Европы по разработке конвенции о кибернетической преступности, а также работу этих организаций по содействию диалогу между правительствами и частным сектором о безопасности и доверии в киберпространстве,

1. призывает государства-члены при разработке национальных законов, политики и практики в деле борьбы с преступным использованием информационных технологий надлежащим образом учитывать работу и достижения Комиссии по предупреждению преступности и уголовному правосудию и других международных и региональных организаций;

2. отмечает значение мер, изложенных в ее резолюции 55/63, и вновь призывает государства-члены учитывать их в своих усилиях по борьбе с преступным использованием информационных технологий;

3. постановляет отложить рассмотрение этого вопроса до выполнения работы, предусмотренной в плане действий Комиссии по предупреждению преступности и уголовному правосудию по борьбе с высокотехнологичной и компьютерной преступностью.

Пятьдесят третья сессия Пункт 66 повестки дня

Резолюция, принятая Генеральной Ассамблеей

[по докладу Первого комитета (A/53/579)]

53/73. **Роль науки и техники в контексте международной безопасности и разоружения**

Генеральная Ассамблея,

признавая возможность применения достижений науки и техники как в гражданских, так и в военных целях, а также необходимость поддерживать и поощрять развитие науки и техники для использования в гражданских целях, будучи обеспокоена тем, что применение достижений науки и техники в воен-

ных целях может в значительной мере способствовать совершенствованию и модернизации современных систем оружия, в частности оружия массового уничтожения,

признавая необходимость внимательно следить за достижениями науки и техники, способными оказать негативное воздействие на международную безопасность и процесс разоружения, а также целенаправленно использовать достижения науки и техники в созидательных целях,

сознавая, что международная передача изделий, услуг и "ноу-хау" двойного назначения, а также высокотехнологичных изделий, услуг и "ноу-хау" для их использования в мирных целях имеет важное значение для экономического и социального развития государств,

сознавая также необходимость регулирования такой передачи изделий и технологий двойного назначения и высоких технологий, имеющих военное применение, с помощью согласованных на многосторонней основе, общеприемлемых, недискриминационных руководящих принципов,

выражая обеспокоенность по поводу все более широкого распространения специальных и особых режимов и механизмов регулирования экспорта изделий и технологий двойного назначения, способных помешать экономическому и социальному развитию развивающихся стран,

напоминая, что в Заключительном документе двенадцатой Конференции глав государств и правительств неприсоединившиеся стран, состоявшейся в Дурбане, Южная Африка, 29 августа - 3 сентября 1998 года, было с обеспокоенностью отмечено, что до сих пор сохраняются чрезмерные ограничения на экспорт в развивающиеся страны материалов, оборудования и технологий для их использования в мирных целях,

подчеркивая, что международно согласованные руководящие принципы, касающиеся передачи высоких технологий, имеющие военное применение, должны учитывать законные оборонные потребности всех государств и потребности в поддержании международного мира и безопасности, не закрывая при этом доступа к высокотехнологичным изделиям, услугам и "ноу-хау" для их использования в мирных целях,

1. *заявляет*, что научно-технический прогресс следует использовать на благо всего человечества с тем, чтобы способствовать устойчивому экономическому и социальному развитию всех государств и гарантировать международную безопасность, и что необходимо содействовать развитию международного сотрудничества в деле использования достижений науки и техники на основе передачи технических знаний и обмена ими в мирных целях;

2. *предлагает* государствам-членам предпринять дополнительные усилия по применению достижений науки и техники в целях, связанных с разоружением, и предоставлять технологии, связанные с разоружением, заинтересованным государствам;

3. *настоятельно призывает* государства-члены провести многосторонние переговоры с участием всех заинтересованных государств для выра-

ботки общеприемлемых, недискриминационных руководящих принципов, касающихся международной передачи изделий и технологий двойного назначения и высоких технологий, имеющих военное применение;

4. *принимает к сведению* доклад Генерального секретаря о роли науки и техники в контексте международной безопасности и разоружения и просит Генерального секретаря запросить мнения государств-членов в отношении этого доклада и высказать рекомендации относительно возможных подходов к выработке согласованных на многосторонней основе, общеприемлемых, недискриминационных руководящих принципов, касающихся международной передачи изделий и технологий двойного назначения и высоких технологий, имеющих военное применение, в докладе, который должен быть представлен Генеральным секретарем Генеральной Ассамблее не позднее чем на ее пятьдесят четвертой сессии;

5. *призывает* органы Организации Объединенных Наций в рамках существующих мандатов содействовать применению достижений науки и техники в мирных целях;

6. *постановляет* включить в предварительную повестку дня своей пятьдесят четвертой сессии пункт, озаглавленный "Роль науки и техники в контексте международной безопасности и разоружения".

79-е пленарное заседание, 4 декабря 1998 года

Пятьдесят третья сессия

Резолюция, принятая Генеральной Ассамблеей

[по докладу Первого комитета (A/53/576)]

53/70. **Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности**

Генеральная Ассамблея,

ссылаясь на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительний прогресс в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе,

напоминая в этой связи о подходах и принципах, которые были намечены на конференции "Информационное сообщество и развитие", состоявшейся в Мидранде, Южная Африка, 13-15 мая 1996 года,

принимая к сведению итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 года, а также принятые на нем рекомендации,

отмечая, что распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности, выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств,

считая необходимым предотвратить неправомерное использование или использование информационных ресурсов или технологий в преступных или террористических целях,

1. *призывает* государства-члены содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности;

2. *просит* все государства-члены информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов;

c) целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом;

3. *просит* Генерального секретаря представить доклад Генеральной Ассамблее на ее пятьдесят четвертой сессии;

4. *постановляет* включить в предварительную повестку дня своей пятьдесят четвертой сессии пункт, озаглавленный "Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности".

79-е пленарное заседание, 4 декабря 1998 года

Пятьдесят седьмая сессия

Пункт 160 повестки дня

Резолюция, принятая Генеральной Ассамблеей

[по докладу Шестого комитета (A/57/567)]

57/27. **Меры по ликвидации международного терроризма**

Генеральная Ассамблея,

руководствуясь целями и принципами Устава Организации Объединенных Наций,

ссылаясь на Декларацию по случаю пятидесятой годовщины Организации Объединенных Наций,

ссылаясь также на Декларацию тысячелетия Организации Объединенных Наций,

ссылаясь далее на все резолюции Генеральной Ассамблеи и Совета Безопасности о мерах по ликвидации международного терроризма,

будучи убеждена в важности рассмотрения Генеральной Ассамблеей мер по ликвидации международного терроризма в качестве универсального органа, компетентного делать это,

будучи глубоко озабочена непрекращающимися террористическими актами, совершаемыми во всем мире,

подтверждая свое решительное осуждение отвратительных актов терроризма, которые повлекли за собой гибель огромного числа людей, громадные разрушения и ущерб, что побудило к принятию резолюции 56/1 Генеральной Ассамблеи от 12 сентября 2001 года, а также резолюции Совета Безопасности 1368 (2001) от 12 сентября 2001 года, 1373 (2001) от 28 сентября 2001 года и 1377 (2001) от 12 ноября 2001 года, а также тех актов, которые были совершены после принятия резолюции 56/88 Генеральной Ассамблеи от 12 декабря 2001 года, в том числе последних таких актов, которые были совершены на Бали и в Москве, что побудило к принятию резолюции Сонета Безопасности 1438 (2002) от 14 октября 2002 года и 1440 (2002) от 24 октября 2001 года, соответственно,

подчеркивая необходимость дальнейшего укрепления международного сотрудничества между государствами и между международными организациями и учреждениями, региональными организациями и механизмами и Организацией Объединенных Наций в целях предотвращения терроризма, борьбы с ним и его ликвидации во всех его формах и проявлениях, где бы и кем бы он ни осуществлялся, как того требуют принципы Устава, нормы международного права и соответствующие международные конвенции,

отмечая роль Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, в наблюдении за осуществлением этой резолюции, включая принятие государствами необходимых финансовых, правовых и технических мер и ратификацию или принятие соответствующих международных конвенции и протоколов,

учитывая необходимость усиления роли Организации Объединенных Наций и соответствующих специализированных учреждений в борьбе с международным терроризмом и предложения Генерального секретаря по усилению роли Организации в этом отношении,

учитывая также настоятельную необходимость укрепления международного, регионального и субрегионального сотрудничества, направленного на увеличение национальных возможностей государств по эффективному предотвращению и пресечению международного терроризма во всех его формах и проявлениях,

ссылаясь на Декларацию о мерах по ликвидации международного терроризма, содержащуюся в приложении к резолюции 49/60 Генеральной Ассамблеи от 9 декабря 1994 года, в которой Ассамблея предложила государствам в срочном порядке провести обзор сферы применения существующих международно-правовых положений о предупреждении, пресечении и ликвидации терроризма во всех его формах и проявлениях с целью обеспечить наличие всеобъемлющих правовых рамок, включающих все аспекты этого вопроса,

принимая к сведению заключительный документ тринадцатой Конференции на уровне министров Движения неприсоединившихся стран, состоявшейся в Картахене, Колумбия, 8 и 9 апреля 2000 года, в котором была вновь заявлена коллективная позиция Движения неприсоединившихся стран в отношении терроризма и подтверждена предыдущая инициатива, выдвинутая на двенадцатой Конференции глав государств и правительств неприсоединившихся стран, проходившей в Дурбане, Южная Африка, 29 августа-3 сентября 1998 года, обратиться с призывом созвать под эгидой Организации Объединенных Наций международную конференцию на высшем уровне для разработки международным сообществом совместной стратегии борьбы с терроризмом во всех его формах и проявлениях, и другие соответствующие инициативы,

учитывая недавние события, а также инициативы на международном, региональном и субрегиональном уровнях по предотвращению и пресечению международного терроризма,

ссылаясь на свое решение, содержащееся в резолюциях 54/110 от 9 декабря 1999 года, 55/158 от 12 декабря 2000 года и 56/88 о том, что Специальный комитет, учрежденный резолюцией 51/210 Генеральной Ассамблеи от 17 декабря 1996 года, рассмотрит и сохранит в своей повестке дня вопрос о созыве под эгидой Организации Объединенных Наций конференции высокого уровня для разработки совместных организованных действий международного сообщества для борьбы с терроризмом во всех его формах и проявлениях,

отмечая региональные усилия по предупреждению, пресечению и ликвидации терроризма во всех его формах и проявлениях, где бы и кем бы он ни осуществлялся, в том числе посредством разработки и соблюдения региональных конвенций,

рассмотрев доклад Генерального секретаря, доклад Специального комитета, учрежденного резолюцией 51/210 Генеральной Ассамблеи от 17 декабря 1996 года, и доклад Рабочей группы Шестого комитета, учрежденной в соответствии с резолюцией 36/88,

1. *решительно осуждает* как преступные и не имеющие оправдания все акты, методы, и практику терроризма, где бы и кем бы они ни осуществлялись;
2. вновь подтверждает, что преступные акты, направленные или рассчитанные на создание обстановки террора среди широкой общественнос-

ти, группы лиц или отдельных лиц в политических целях, ни при каких обстоятельствах не могут быть оправданы, какими бы ни были соображения политического, философского, идеологического, расового, этнического, религиозного или другого характера, которые могут приводиться в их оправдание;

3. вновь призывает все государства принимать согласно Уставу Организации Объединенных Наций и соответствующим нормам международного права, включая международные стандарты в области прав человека, дальнейшие меры по предотвращению терроризма и укреплению международного сотрудничества в борьбе с терроризмом и с этой целью рассмотреть, в частности, вопрос об осуществлении мер, изложенных в подпунктах /пунктах 3 резолюции 51/210;
4. вновь призывает также все государства в целях повышения эффективности осуществления соответствующих правовых документов активизировать, должным образом и где это уместно, обмен информацией о фактах, связанных с терроризмом, не допуская при этом распространения неточной или непроверенной информации;
5. вновь призывает государства воздерживаться от финансирования, поощрения, подготовки или оказания какой-либо иной поддержки террористической деятельности;
6. подтверждает, что международное сотрудничество, как и действия государств по борьбе с терроризмом, должно осуществляться в соответствии с принципами Устава, нормами международного права и соответствующими международными конвенциями;
7. настоятельно призываем все государства, которые еще не сделали этого, в первоочередном порядке и в соответствии с резолюцией 1373 (2001) Совета Безопасности рассмотреть вопрос о том, чтобы стать участниками соответствующих конвенции и протоколов, указанных в пункте 6 резолюции 51/210 Генеральной Ассамблеи, а также Международной конвенции о борьбе с бомбовым терроризмом и Международной конвенции о борьбе с финансированием терроризма, и призывает все государства принять, в надлежащем порядке, внутренние законодательные акты, необходимые для осуществления положений этих конвенции и протоколов, обеспечения того, чтобы юрисдикция их судов позволяла им привлекать к ответственности лиц, совершивших террористические акты, и осуществления сотрудничества с другими государствами и соответствующими международными и региональными организациями и оказания им поддержки и помощи в этих целях;
8. настоятельно призывает государства сотрудничать с Генеральным секретарем, друг с другом, а также с заинтересованными межправительственными организациями в целях обеспечения, где это уместно в рамках существующих мандатов, того, чтобы технические и другие консультации экспертов предоставлялись тем государствам, которые нуждаются

в помощи при присоединении к конвенциям и протоколам, упомянутым в пункте 7, выше, и просят о ней;

9. отмечает с признательностью и удовлетворением, что в ответ на призыв, содержащийся в пункте 7 резолюции 56/88, несколько государств стали сторонами соответствующих конвенции и протоколов, упомянутых в нем, обеспечивая тем самым достижение цели, заключающейся в более широком принятии и осуществлении этих конвенции;

10. вновь подтверждает Декларацию о мерах по ликвидации международного терроризма, содержащуюся в приложении к резолюции 49/60, и Декларацию, дополняющую Декларацию о мерах по ликвидации международного терроризма 1994 года, содержащуюся в приложении к резолюции 51/210, и призывает все государства осуществить их;

11. настоятельно призывает все государства и Генерального секретаря в своих усилиях по предотвращению международного терроризма наиболее эффективным образом использовать существующие институты Организации Объединенных Наций;

12. приветствует усилия Сектора по предупреждению терроризма Центра по международному предупреждению преступности в Вене, после анализа имеющихся возможностей в системе Организации Объединенных Наций, по укреплению на основе его мандата способности Организации Объединенных Наций предупреждать терроризм и в этом контексте с признательностью принимает к сведению доклад Генерального секретаря об укреплении Сектора по предупреждению терроризма Секретариата в соответствии с просьбой Генеральной Ассамблеи, содержащейся в ее резолюции 56/253 от 24 декабря 2001 года;

13. приветствует также издание Секретариатом в Сборнике законодательных актов Организации Объединенных Наций тома, озаглавленного «Национальные законы и постановления о предотвращении и пресечении международного терроризма», подготовленного Отделом кодификации Управления по правовым вопросам Секретариата во исполнение пункта 10 Декларации о мерах по ликвидации международного терроризма;

14. предлагает государствам, которые еще не сделали этого, представить Генеральному секретарю информацию о своих национальных законах и постановлениях, касающихся предупреждения и пресечения актов международного терроризма, и принимает к сведению в этой связи доклады государств-членов Комитету Совета Безопасности, учрежденному резолюцией 1373 (2001);

15. предлагает региональным межправительственным организациям представить Генеральному секретарю информацию о принятых ими на региональном уровне мерах по ликвидации международного терроризма;

16. приветствует существенный прогресс, достигнутый в разработке проекта всеобъемлющей конвенции о международном терроризме в ходе

заседаний Специального комитета, учрежденного резолюцией 51/210 Генеральной Ассамблеи от 17 декабря 1996 года, и Рабочей группы Шестого комитета, учрежденной в соответствии с резолюцией 56/88 Генеральной Ассамблеи;

17. постановляет, что Специальный комитет будет продолжать разрабатывать проект всеобъемлющей конвенции о международном терроризме в срочном порядке и предпринимать усилия в целях решения сохраняющихся вопросов, касающихся разработки проекта международной конвенции о борьбе с актами ядерного терроризма в качестве средства дальнейшего развития всеобъемлющего правового механизма конвенции, посвященных борьбе с международным терроризмом, и что он сохранит в своей повестке дня вопрос о созыве под эгидой Организации Объединенных Наций конференции высокого уровня для разработки совместных организованных действий международного сообщества по борьбе с терроризмом во всех его формах и проявлениях;

18. постановляет также, что Специальный комитет проведет 31 марта-2 апреля 2003 года сессию для продолжения разработки проекта всеобъемлющей конвенции о международном терроризме, на которой он посвятит достаточно времени продолжению рассмотрения нерешенных вопросов в связи с разработкой проекта международной конвенции о борьбе с актами ядерного терроризма, что он сохранит в своей повестке дня вопрос о созыве под эгидой Организации Объединенных Наций конференции высокого уровня для разработки совместных организованных действий международного сообщества по борьбе с терроризмом во всех его формах и проявлениях и что эта работа будет продолжена, при необходимости, в ходе пятьдесят восьмой сессии Генеральной Ассамблеи в рамках рабочей группы Шестого комитета;

19. просит Генерального секретаря продолжать обеспечивать Специальному комитету необходимые условия для выполнения им своей работы;

20. просит Специальный комитет в случае завершения разработки проекта всеобъемлющей конвенции о международном терроризме или проекта международной конвенции о борьбе с актами ядерного терроризма представить Генеральной Ассамблее на ее пятьдесят седьмой сессии соответствующий доклад;

21. просит также Специальный комитет представить Генеральной Ассамблее на ее пятьдесят восьмой сессии доклад о ходе выполнения свого мандата;

22. постановляет включить в предварительную повестку дня своей пятьдесят восьмой сессии пункт, озаглавленный «Меры по ликвидации международного терроризма».

52-е пленарное заседание, 19 ноября 2002 года

РЕЗОЛЮЦІЯ РАДИ
Про законне перехоплення телекомунікацій (96/С 329/01)*

Від 17 січня 1995р. *(Витяг)*

Офіційний переклад

РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про створення Європейського Союзу та, зокрема, статті К.1 (9) та К.2 (2) Договору;

Підтверджуючи знову необхідність дотримання при здійсненні заходів перехоплення права осіб на недоторканність їхнього приватного життя, яке закріплене в національному законодавстві, що застосовується на відповідних територіях;

Усвідомлюючи той факт, що дотримання цього права наштовхується на певні правові та технічні труднощі через розвиток технологій;

Будучи сповненою рішучості визначити та подолати ці труднощі при виконанні вимог, викладених в Додатку, в той же час дотримуючись прав людини та принципів захисту даних;

Враховуючи, що в законах держав-членів передбачено можливості обмеження таємниці передачі даних та, за певних обставин, перехоплення телекомунікацій;

Враховуючи, що дозволені законом перехоплення телекомунікацій є важливим засобом для захисту державних інтересів і, передусім, державної безпеки та розслідування тяжких злочинів;

Враховуючи, що перехоплення може здійснюватися лише після передбачення всіх технічних аспектів;

Враховуючи, що, згідно з рішенням міністрів групи Треві, прийнятим в грудні 1991 року, слід провести вивчення впливу правового, технічного та ринкового розвитку в межах телекомунікаційного сектора на різні можливості перехоплення, а також того, яких заходів слід вжити для вирішення проблем, що вже стали очевидними,

ПРИЙНЯЛА ТАКУ РЕЗОЛЮЦІЮ:

1. Рада відзначає, що вимоги держав-членів для забезпечення їхньої можливості проведення законного перехоплення телекомунікацій, які додаються до цієї Резолюції («вимоги»), є важливим стислим викладенням потреб компетентних органів для технічної реалізації санкціонованого законом перехоплення в сучасних телекомунікаційних системах.

2. Рада вважає, що вищезгадані вимоги повинні бути взяті до уваги при визначенні та проведенні заходів, що можуть мати вплив на санкціоноване за-

* Інформаційне законодавство: Збірник законодавчих актів: У 6 т. / За заг. ред. Ю. С. Шемшученка, І. С. Чижа. –Т. 5. Міжнародно-правові акти в інформаційній сфері. –К.: ТОВ «Видавництво «Юридична думка», 2005. – 328 с.

коном перехоплення телекомунікацій, та просить держав-членів закликати міністрів, відповідальних за телекомунікації, підтримати цю точку зору та співпрацювати з міністрами юстиції і внутрішніх справ з метою виконання вимог щодо операторів мереж та постачальників послуг.

ДОДАТОК

ВИМОГИ

В цьому розділі представлено вимоги правоохоронних органів щодо законного перехоплення телекомунікацій. Ці вимоги підпорядковуються національному законодавству та повинні тлумачитися згідно із відповідною національною політикою.

1. Правоохоронні органи вимагають доступу до всіх телекомунікацій, які передаються чи про передачу яких було прийнято розпорядження, до та від номера або іншого ідентифікатора цільової служби, який використовується суб'єктом перехоплення. Правоохоронні органи вимагають також доступу до інформації про зв'язок, які видаються для його обробки.

1.1. Правоохоронні органи вимагають доступу до всіх суб'єктів перехоплення, які функціонують тимчасово або постійно в межах телекомунікаційної системи.

1.2. Правоохоронні органи вимагають доступу у випадках, коли суб'єкт перехоплення може використовувати функції для переведення дзвінків на інші телекомунікаційні послуги чи термінальне обладнання, включаючи дзвінки, що перетинають більш ніж одну мережу або обробляються більш ніж одним оператором мережі/постачальником послуг до свого завершення.

1.3. Правоохоронні органи вимагають, щоб Надавалися телекомунікації з та до цільової служби, за винятком будь-яких телекомунікацій, які не входять до сфери дії дозволу на перехоплення.

1.4. Правоохоронні органи вимагають доступу до інформації про зв'язок, такої, як:

1.4.1. сигнал про стан готовності доступу;

1.4.2. для вихідного з'єднання – номер сторони, з якою зв'язуються, навіть якщо зв'язок не було встановлено;

1.4.3. для вхідного з'єднання – номер сторони, яка зв'язується, навіть якщо зв'язок не було встановлено;

1.4.4. усі сигнали, що були видані об'єктом цілі, включаючи сигнали після з'єднання, видані для активації функцій, таких як конференц-зв'язок та передача зв'язку;

1.4.5. початок, кінець та тривалість з'єднання;

1.4.6. фактичне місце призначення та проміжний абонентський номер у разі, якщо зв'язок був переадресований;

1.5. Правоохоронні органи вимагають інформацію щодо якомога точнішого географічного місцезнаходження, відомого для мережі для мобільних абонентів.

1.6. Правоохоронні органи вимагають дані щодо особливих послуг, які використовуються суб'єктом перехоплювання, та технічних параметрів для тих видів зв'язку.

2. Правоохоронні органи вимагають можливість постійного моніторингу перехоплення телекомунікація в реальному масштабі часу. Інформація щодо зв'язку також має передаватися в реальному масштабі часу. У випадку, якщо інформація щодо зв'язку не може бути доступною в реальному масштабі часу, правоохоронні органи вимагають, щоб ця інформація була доступна якомога швидше після завершення дзвінка.

3. Правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг надавали один або декілька інтерфейсів, звідки зв'язок, що перехоплюється, може бути переданий на контрольні пункти правоохоронних органів. Ці інтерфейси повинні бути погоджені органами перехоплення та операторами мережі/постачальниками послуг. Інші питання, пов'язані з цими інтерфейсами, будуть вирішуватись згідно із усталеною практикою в окремих країнах.

3.1.Правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг надавали інформацію щодо зв'язку та зміст зв'язку з цільової служби у спосіб, який передбачає точну кореляцію інформації щодо зв'язку із змістом зв'язку.

3.2. Правоохоронні органи вимагають, щоб формат для передачі повідомлень, які перехоплюються, на контрольні пункти був загальнодоступний. Цей формат остаточно буде узгоджений окремо в кожній країні.

3.3. У разі, якщо оператори мережі/постачальники послуг ініціюють кодування, стиснення чи шифрування телекомунікаційного трафіку, правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг надавали зв'язок, що перехоплюється, в незашифрованому вигляді.

3.4. Правоохоронні органи вимагають, щоб оператори мереж/постачальники послуг мали змогу передавати повідомлення, що перехоплюються, на контрольні пункти правоохоронних органів через фіксовані або комутовані з'єднання.

3.5. Правоохоронні органи вимагають, щоб передача перехоплених повідомлень на контрольні пункти правоохоронних органів відповідала застосовуваним вимогам безпеки.

4. Правоохоронні органи вимагають, щоб перехоплення здійснювалось так, щоб ані об'єкт перехоплення, ані будь-яка інша неуповноважена людина не знала про жодні зміни, зроблені для того, щоб виконати наказ про перехоплення. В першу чергу, функціонування цільової служби повинно здаватися незмінним суб'єкту перехоплення.

5. Правоохоронні органи вимагають, щоб перехоплення розроблялося та виконувалось так, щоб запобігти несанкціонованому та неналежному використанню та захистити інформацію, яка має відношення до перехоплення.

5.1.Правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг захищали інформацію про те, які і скільки перехоплень здійснюються чи були здійснені, та не розголошували інформацію про те, яким чином проводяться перехоплення.

5.2. Правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг забезпечували передачу зв'язку, що перехоплюється, лише наглядовому органу, визначеному в дозволі на перехоплення.

5.3. Згідно з національними нормативними актами, оператори мережі/постачальники послуг можуть бути зобов'язані вести захищений належним чином реєстр активацій перехоплень.

6. Базуючись на законному запиті та перед виконанням перехоплення, правоохоронні органи вимагають повідомити: (1) особу суб'єктів перехоплення, сервісний номер чи інший розпізнавальний ідентифікатор; (2) інформацію щодо послуг та функцій телекомунікаційної системи, що використовуються суб'єктом перехоплення та постачаються операторами мережі/постачальниками послуг; (3) інформацію щодо технічних параметрів передачі на контрольні пункти правоохоронних органів.

7. Під час перехоплення правоохоронні органи можуть вимагати інформацію та/чи допомогу від операторів мережі/постачальників послуг для того, щоб переконатись, що зв'язок, отриманий на інтерфейсі перехоплення, є зв'язком, що має відношення до цільової служби. Види інформації/допомоги, яка потрібна, будуть варіюватись згідно з усталеною практикою в окремих країнах.

8. Правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг забезпечували виконання декількох одночасних перехоплень. Множинні перехоплення для одної цільової служби можуть вимагатися для забезпечення можливості проведення нагляду більш ніж одним правоохоронним органом. У цьому випадку оператори мережі/постачальники послуг повинні вживати застережних заходів для захисту від розкриття інформації про те, які органи здійснюють нагляд, та для гарантування конфіденційності розслідувань. Максимальна кількість одночасних перехоплень для даної сукупності абонентів відповідатиме національним вимогам.

9. Правоохоронні органи вимагають, щоб оператори мережі/постачальники послуг виконували перехоплення якомога швидше (у термінових випадках протягом декількох годин або хвилин). Вимоги правоохоронних органів щодо швидкості реакції будуть варіюватись залежно від країни та від виду цільової послуги, яка має перехоплюватись.

10. Правоохоронні органи вимагають, щоб на час перехоплення надійність послуг, які підтримують перехоплення, принаймні дорівнювала надійності цільових послуг, які надаються суб'єкту перехоплення. Правоохоронні органи вимагають, щоб якість обслуговування передач, що перехоплюються і направляються на контрольні пункти, відповідала стандартам якості функціонування, визнаних операторами мереж/постачальниками послуг.

Офіційний журнал С 329, 04/11/1996, стор. 0001 — 0006 Переклад здійснено Центром перекладів актів Європейського права при Міністерстві юстиції України.

РЕЗОЛЮЦІЯ РАДИ

від 18 лютого 2003 року

про Європейський підхід до культури мережі та інформаційної безпеки

(2003/С 48/01) Офіційний вісник С 048, 28/02/2003

РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ

ЗГАДУЄ:

1. Повідомлення Комісії Раді, Європейському Парламенту, Європейському Економічно-соціальному комітету та Комітету регіонів - безпека мережі та інформації: пропозицію для підходу Європейської політики;

2. Резолюцію Ради від 30 травня 2001 року про "План Дій е-Європа: Безпека мережі та інформації";

3. Резолюцію Ради від 28 січня 2002 року про єдиний підхід та спеціальні дії у галузі безпеки мережі та інформації;

4. що, Севільська Європейська Рада у червні 2002 року підтримала План дій е-Європа 2005;

5. Висновок Європейського Парламенту та Європейської Комісії про безпеку мережі та інформації: Пропозиція для підходу Європейської політики;

НАГОЛОШУЄ, ЩО:

1. одночасно з розвитком послуг з забезпечення громадськості інформацією, підвищення рівня безпеки мережі та інформації залишається відкритим питання стосовно повсякденного життя громадян, діяльності підприємств та державного адміністрування, необхідного для належного функціонування внутрішнього ринку;

2. держави-члени та Європейські інституції, в подальшому, повинні розвивати відповідну Європейську стратегію безпеки мережі та інформації та намагатися досягти культури безпеки, беручи до уваги вагомість міжнародного співробітництва;

3. вказівки ОБСЄ щодо Безпеки інформаційних систем та мереж являються цінною моделлю розвитку політики, яка має на меті досягнення належної культури безпеки, з одночасним дотриманням відповідних демократичних цінностей та забезпеченням захисту персональних даних;

4. відповідна увага повинна приділятися особистим правам. Громадяни та підприємства повинні бути переконані, що інформація зберігається належним чином, конфіденційно і надійно;

5. розвиваючи культуру безпеки, важливо визначити відповідальність за безпеку мереж та інформаційних систем для всіх зацікавлених сторін;

6. Європа потребує гарантій розвитку та розповсюдження належної бази навиків у галузі безпеки мереж та інформації;

7. існує гостра необхідність у прозорості, обміні інформацією та співпраці між Європейськими інституціями та приватним сектором;

8. розвиток політики безпеки на Європейському рівні вимагає прозорості та співпраці ділових кіл;

9. поточна робота для виконання завдань, визначених у Резолюції Ради від 28 січня 2002 року про єдиний підхід та спеціальні дії у галузі безпеки мережі та інформації повинна продовжуватися.

ПРОПОНУЄ ДЕРЖАВАМ-ЧЛЕНАМ:

1. сприяти забезпеченню безпеки, як суттєвому аспекту в управлінні як на державному так і приватному рівні, а саме через розподіл відповідальностей;

2. надавати належну освіту та професійне навчання, а також підвищувати рівень обізнаності щодо питань безпеки, особливо серед молоді;

3. вживати адекватних заходів з метою запобігання та усунення випадків порушення безпеки, а саме через:

a) безперервне вдосконалення ідентифікації і оцінки проблем безпеки та застосування відповідних способів управління;

b) визначення ефективних способів повідомлення всіх зацікавле-них сторін про необхідність у діях через покращення діалогу на Європейському і національному рівнях та, якщо необхідно, на міжнародних рівнях, особливо, серед тих, хто забезпечує технологіями інфо-рмаційне суспільство та надає послуги;

c) забезпечувати належний обмін інформацією залежно від потреб суспільства у поінформованості щодо належних практик у сфері безпеки;

4. заохочувати до співпраці і партнерства наукових з діловими колами з метою розробки технологій безпеки і розробки та затвердження загальновизнаних стандартів.

ВІТАЄ НАМІРИ КОМІСІЇ СТОСОВНО:

1. застосування відкритого методу узгодження поточних дій держав-членів та визначення їх впливу на безпеку;

2. створення тимчасової міжвідомчої робочої групи у тісній співпраці та скликаної з представників держав-членів з метою застосування попередніх дій з огляду на заснування Спеціальної комісії з питань кібербезпеки, як зазначено у Резолюції Ради від 28 січня 2002 року;

3. подальшого розвитку діалогу з промисловим середовищем, у співпраці з державами-членами, з метою вдосконалення комп'ютерного та програмного забезпечення та забезпечення доступності послуг і даних;

4. встановлення контактів з відповідними міжнародними партнерами та організаціями, з огляду на співпрацю та обмін інформацією в цій галузі і звітування перед Радою на постійній основі;

5. заснування Спеціальної комісії з питань кібербезпеки, як зазначено в пункті 2.

ЗАКЛИКАЄ:

1. промислове середовище інтегрувати управління ризиками, пов'язаними з безпекою в основне поняття управління та ділову діяльність;

2. всіх користувачів звернути увагу на ризики, пов'язані з інформаційними системами та загрози, які виникають з фізичних чинників, людського фактору а також звернути увагу на технічну вразливість і сторонні атаки;

3. промислове середовище та всіх користувачів вступити у діалог з органами управління з метою розвитку культури безпеки.

ДИРЕКТИВА 95/46/ЄС ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ

Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних?

від 24 жовтня 1995р.

(Витяг)

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ і РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ, беручи до уваги Договір про заснування Європейського Співтовариства і, зокрема, його статтю 100a,

беручи до уваги пропозицію Комісії (1),

беручи до уваги висновок Економічного і Соціального Комітету,

діючи відповідно до процедури, викладеної в статті 189b Договору,

1. Враховуючи, що цілі Співтовариства, викладені в Договорі, з поправками, внесеними Договором про Європейський Союз, полягають в створенні дедалі тіснішого союзу серед народів Європи, заохоченні більш тісних відносин між державами, що входять до Співтовариства, забезпеченні економічного і соціального прогресу шляхом спільних дій, спрямованих на усунення бар'єрів, що розділяють Європу, підтримку постійного поліпшення умов життя його народів, збереження і зміцнення миру та свободи, а також на розвиток демократії, яка базується на основних правах, визнаних конституціями і законами держав-членів та Європейською конвенцією про захист прав людини і основних свобод;

2. Враховуючи, що системи обробки даних створені для служіння людині; враховуючи, що вони, незалежно від національності чи місця проживання фізичних осіб, повинні поважати їхні основні права і свободи, особливо право на невтручання в особисте життя, і сприяти економічному і соціальному прогресу, розширенню торгівлі і добробуту людей;

3. Враховуючи, що створення і функціонування внутрішнього ринку, у якому згідно зі статтею 7a Договору гарантується вільне пересування товарів,

осіб, послуг і капіталів, вимагає не тільки можливості вільного переміщення персональних даних з однієї держави-члена в іншу, але й захисту основних прав людей;

4. Враховуючи дедалі частіше застосування обробки персональних даних у Співтоваристві в різних сферах соціальної та економічної діяльності; враховуючи, що прогрес, досягнутий у сфері інформаційних технологій, значно полегшує обробку та обмін такими даними;

5. Враховуючи, що економічна і соціальна інтеграція, досягнута в результаті створення і функціонування внутрішнього ринку в розумінні статті 7а Договору, неминуче призведе до істотного збільшення транскордонних потоків персональних даних між усіма тими, хто бере участь в економічному і соціальному житті держав-членів, як в приватному, так і в державному статусі; враховуючи, що обмін персональними даними між підприємствами різних держав-членів має розвиватися; враховуючи, що відповідно до права Співтовариства державні органи різних держав-членів повинні співпрацювати й обмінюватися персональними даними для того, щоб могти виконувати свої обов'язки і завдання від імені органів влади в іншій державі-члені в контексті простору без внутрішніх кордонів, який створюється внутрішнім ринком;

6. Враховуючи, крім того, що збільшення науково-технічного співробітництва і узгоджене введення нових телекомунікаційних мереж у Співтоваристві роблять необхідним і полегшують здійснення транскордонних потоків персональних даних;

7. Враховуючи, що розходження в рівні захисту прав і свобод фізичних осіб, що надають держави-члени, в особливості права на невтручання в особисте життя, при обробці персональних даних, може перешкоджати передачі таких даних з території однієї держави-члена на територію іншої держави-члена; враховуючи, що такі розходження до того ж можуть стати перешкодою в здійсненні певних видів економічної діяльності на рівні Співтовариства, негативно відбитися на конкуренції, перешкоджати владі у виконанні її зобов'язань згідно з правом Співтовариства; враховуючи, що такі розходження в рівні захисту викликані існуванням великої різноманітності національних законів, постанов і адміністративних положень;

8. Враховуючи, що для усунення перешкод на шляху передачі персональних даних рівень захисту прав і свобод фізичних осіб при обробці цих даних повинен бути однаковим у всіх державах-членах; враховуючи, що ця мета, будучи життєво необхідною для внутрішнього ринку, не може бути досягнута державами-членами поодинці, особливо з урахуванням ступеня існуючих у даний час розходжень між відповідним законодавством держав-членів і необхідністю узгодження законів держав-членів для забезпечення єдиного підходу до регулювання транскордонних потоків персональних даних, тобто, дотримуючись цілей внутрішнього ринку, передбачених статтею 7а Договору; враховуючи, що в зв'язку з цим необхідні дії Співтовариства, спрямовані на зближення такого законодавства;

9. Враховуючи, що при рівному рівні захисту внаслідок зближення національних законодавств держави-члени більше не зможуть перешкоджати вільному пересуванню персональних даних між собою, посилаючись на обмеження, пов'язані із захистом прав і свобод фізичних осіб, а особливо права на невтручання в особисте життя; враховуючи, що державам-членам буде наданий певний ступінь свободи маневрування, який в контексті виконання Директиви може також використовуватись діловими і соціальними партнерами; враховуючи, що держави-члени в такий спосіб зможуть уточнити у своєму національному законодавстві загальні умови, що регулюють законність обробки даних; враховуючи, що при цьому держави-члени будуть прагнути поліпшити систему захисту, передбачену в їхньому законодавстві в даний час; враховуючи, що в межах певного ступеня свободи маневрування та відповідно до права Співтовариства можуть виникнути розбіжності в процесі здійснення Директиви, і це може вплинути на пересування даних як у державі-члені, так і в Співтоваристві;

10. Враховуючи, що метою національного законодавства про обробку персональних даних є захист основних прав і свобод, а особливо права на невтручання в особисте життя, що визнається як статтею 8 Європейської конвенції про захист прав людини й основних свобод, так і загальними принципами права Співтовариства; враховуючи, що з цієї причини зближення згаданих законодавств не повинне призвести до зниження рівня наданого ними захисту, а навпаки, повинне прагнути забезпечити високий рівень захисту в Співтоваристві;

11. Враховуючи, що принципи захисту прав і свобод фізичних осіб, а особливо права на невтручання в приватне життя, викладені в даній Директиві, уточнюють і посилюють принципи, викладені в Конвенції Ради Європи від 28 січня 1981 року про захист фізичних осіб при автоматизованій обробці персональних даних;

12. Враховуючи, що принципи захисту повинні застосовуватися до усіх випадків обробки персональних даних, здійснюваних будь-якою особою, чия діяльність регулюється правом Співтовариства; враховуючи, що ці принципи не поширюються на обробку даних, створених фізичною особою в процесі діяльності винятково особистого чи домашнього характеру, такої як переписування і ведення адресних книг;

13. Враховуючи, що діяльність, згадана в Розділах V і VI Договору про Європейський Союз, щодо суспільного порядку, оборони, державної безпеки чи діяльності держави в сфері кримінального законодавства, не входить до сфери дії права Співтовариства, без шкоди для зобов'язань, покладених на держави-члени згідно з параграфом 2 статті 56, статті 57 чи статті 100 Договору, що засновує Європейське Співтовариство; враховуючи, що обробка персональних даних, необхідна для захисту економічного добробуту держави, не входить до сфери дії даної Директиви, у випадках, коли така обробка пов'язана з питаннями державної безпеки;

14. Враховуючи, що з урахуванням важливості розвитку технологій, використовуваних для прийому, передачі, маніпуляцій, реєстрації, збереженні чи повідомленні звукових і візуальних даних, які стосуються фізичних осіб, який відбувається в інформаційному суспільстві, дана Директива повинна застосовуватися до обробки, що використовує такі дані;

15. Враховуючи, що обробка таких даних підпадає під дію даної Директиви лише в тих випадках, коли обробка є автоматизованою або коли оброблені дані розміщуються чи призначені для розміщення в картотеках, структурованих за визначеними критеріями, що стосуються фізичних осіб, таким чином, щоб забезпечити легкий доступ до відповідних персональних даних;

16. Враховуючи, що обробка звукових і візуальних даних, таких як, наприклад, відеоспостереження, не відноситься до сфери дії даної Директиви, якщо вона проводиться з метою суспільного порядку, оборони, державної безпеки чи в ході державної діяльності, що відноситься до сфери кримінального права, чи іншої діяльності, що не відноситься до сфери дії права Співтовариства;

17. Враховуючи, що до випадків, коли обробка звукових і візуальних даних провадиться з метою журналістики чи з метою літературної або художньої творчості, зокрема в аудіовізуальній області, принципи Директиви повинні застосовуватися з обмеженнями відповідно до положень, викладених в статті 9;

18. Враховуючи, що для того, щоб уникнути втрати фізичною особою захисту, на який вона має право згідно з даною Директивою, будь-яка обробка персональних даних у Співтоваристві повинна відбуватися відповідно до законодавства однієї з держав-членів; враховуючи, що в зв'язку з цим обробка, здійснена в межах юрисдикції контролера, створеного в державі-члені, повинна регулюватися законодавством цієї держави;

19. Враховуючи, що створення такого органу на території держави-члена передбачає ефективне і реальне ведення діяльності на основі постійних домовленостей; враховуючи, що правова форма такої установи, незалежно від того є воно простою філією чи представництвом — суб'єктом права, не є вирішальним чинником у цьому відношенні; враховуючи, що при створенні єдиного контролера на території декількох держав-членів, зокрема шляхом створення представництв, для запобігання порушення національних правил, він повинен забезпечити виконання своїми установами зобов'язань, накладених на них національним законодавством, що застосовується до його діяльності;

20. Враховуючи, що той факт, що обробка даних проводиться особою, яка перебуває в третій країні, не повинен перешкоджати захисту фізичних осіб, передбаченому даною Директивою; враховуючи, що в таких випадках обробка даних повинна регулюватися законами держави-члена, у якому розташовані використовувані засоби, і повинні існувати гарантії для забезпечення дотримання на практиці прав і обов'язків, передбачених даною Директивою;

21. Враховуючи, що дана Директива не завдає шкоди правилам територіальності, застосовуваним у кримінальних справах;

22. Враховуючи, що держави-члени більш точно визначають у законах, що приймаються, а також при здійсненні заходів на виконання даної Директиви, загальні умови, при яких обробка даних є законною; враховуючи, що, зокрема, стаття 5 у сполученні зі статтями 7 і 8 дозволяє державам-членам незалежно від загальних правил передбачати особливі умови обробки даних для певних секторі» і для різних категорій даних, зазначених у статті 8;

23. Враховуючи, що держави-члени уповноважені забезпечити здійснення захисту фізичних осіб шляхом прийняття як загального закону про захист фізичних і осіб при обробці персональних даних, такі галузевих законів, таких як ті, що стосуються, наприклад, статистичних установ;

24. Враховуючи, що законодавство про захист юридичних осіб при обробці даних, які їх стосуються, не зачіпається даною Директивою;

25. Враховуючи, що принципи захисту повинні бути відображені, з одного боку, у зобов'язаннях, що накладаються на осіб, на державні органи влади, підприємства, агентства чи інші органи, які відповідають за обробку, зокрема в тому, що стосується якості даних, технічної безпеки, повідомлення наглядових органів, і обставин, при яких може проводитися обробка, та, з іншого боку, у праві, яким наділені фізичні особи, чиї дані підлягають обробці, знати, що обробка дійсно проводиться, звертатися до даних, вимагати внесення змін і навіть заперечувати проти обробки за певних обставин;

26. Враховуючи, що принципи захисту повинні застосовуватися до будь-якої інформації, яка стосується встановленої особи чи особи, яку можна встановити; враховуючи, що для визначення того, чи можна особу встановити, повинні враховуватися всі засоби, використання яких контролером чи якою-небудь іншою особою імовірно очікувати для встановлення вищезгаданої особи; враховуючи, що принципи захисту не застосовуються до даних, що надані анонімно таким чином, що суб'єкт даних не може бути встановлений; враховуючи, що кодекси поведінки в значенні статті 27 можуть бути корисним знаряддям для забезпечення керівництва щодо способів анонімного надання даних і їхнього збереження у формі, що забезпечує неможливість встановлення особи суб'єкта даних;

27. Враховуючи, що захист фізичних осіб повинен застосовуватися як до автоматизованої обробки даних, так і до ручної обробки; враховуючи, що масштаби такого захисту не повинні залежати від використовуваних методів, бо інакше це створить серйозну загрозу обходу закону; враховуючи, що, незважаючи на це, у тому що стосується ручної обробки, дана Директива охоплює тільки картотеки даних, але не неструктуровані справи; враховуючи, що, зокрема, вміст картотеки даних повинен бути структурований відповідно до визначених критеріїв щодо фізичних осіб, що забезпечувало б легкий доступ до персональних даних; враховуючи, що, відповідно до визначення в статті 2 (с), різні критерії визначення складових частин структурованої сукупності персо-

нальних даних і різні критерії управління доступом до такої сукупності можуть бути встановлені кожною державою-членом; враховуючи, що справи чи зібрання справ, як і їхні титульні аркуші, що не розроблені відповідно до визначених критеріїв, за жодних обставин не входять до сфери дії даної Директиви;

28. Враховуючи, що будь-яка обробка персональних даних повинна бути законною і справедливою по відношенню до фізичних осіб, яких вона безпосередньо стосується; враховуючи, що, зокрема, дані повинні бути достовірними, відповідними і не надмірними з точки зору цілей, заради яких проводиться їхня обробка; враховуючи, що ці цілі повинні бути чіткими і законними і повинні бути визначені на час збору даних; враховуючи, що цілі обробки даних, яка проводиться після збору даних, не повинні бути несумісними із цілями, визначеними спочатку;

29. Враховуючи, що подальша обробка персональних даних в історичних, статистичних чи наукових цілях не повинна розглядатися як несумісна з цілями, заради яких дані були зібрані раніше, за умови, що держави-члени забезпечать відповідні гарантії; враховуючи, що ці гарантії повинні, зокрема, виключати використання даних на підтримку заходів чи рішень відносно будь-якої конкретної особи;

30. Враховуючи, що для забезпечення законності обробки персональних даних, вона повинна, крім іншого, проводитися з дозволу суб'єкта даних чи бути необхідною для укладання чи виконання договору, обов'язкового для суб'єкта даних, або в якості правової вимоги, або для виконання завдання, яке здійснюється в інтересах суспільства чи при виконанні офіційних повноважень, або в законних інтересах фізичної чи юридичної особи, за умови, що враховуються інтереси чи права і свободи суб'єкта даних; враховуючи, що, зокрема, для того, щоб зберегти рівновагу між інтересами, які зачіпаються, водночас гарантуючи ефективну конкуренцію, держави-члени можуть визначити обставини, при яких персональні дані можуть використовуватися чи надаватися третій стороні в контексті законної звичайної ділової діяльності компаній і інших органів; враховуючи, що держави-члени можуть аналогічним чином визначити умови, за яких персональні дані можуть надаватися третій стороні з метою маркетингу, здійснюваного або в комерційних цілях, або благодійною організацією чи будь-якою іншою асоціацією чи фондом, наприклад, політичного характеру, за умови дотримання положень, що дозволяють суб'єкту даних безкоштовно і без зазначення причин заперечувати проти обробки даних, які його стосуються;

31. Враховуючи, що обробка персональних даних повинна розглядатися також як законна, якщо вона проводиться з метою захисту інтересу, який є надзвичайно важливим для життя суб'єкта даних;

32. Враховуючи, що питання про те, чи повинен контролер, який виконує завдання в інтересах суспільства чи при виконанні офіційних повноважень, бути державним органом або іншою фізичною чи юридичною особою,

що регулюється публічним правом чи приватним правом, такою, як професійне об'єднання, повинне визначатися національними законодавствами;

33. Враховуючи, що дані, які за своєю природою можуть порушити основні свободи і таємницю приватного життя, не повинні оброблятися доти, доки суб'єкт даних не дасть своєї згоди; враховуючи, що, незважаючи на це, відступ від даної заборони повинен бути чітко викладений з огляду на особливі потреби, зокрема, якщо обробка цих даних проводиться у певних цілях, пов'язаних із здоров'ям, особами, які зв'язані правовим зобов'язанням зберігати професійну таємницю, або під час законної діяльності певних асоціацій чи фондів, метою яких є дозволити здійснення основних свобод;

34. Враховуючи, що держави-члени повинні бути також уповноважені, якщо це виправдовується важливим суспільним інтересом, відступати від заборони обробляти конфіденційні категорії даних, якщо це пов'язано із суспільними інтересами в таких сферах, як охорона суспільного здоров'я і соціальний захист, особливо з метою гарантування якості і рентабельності процедур, що використовуються під час врегулювання позовів про виплату допомоги і надання послуг у системі страхування здоров'я, а також у сфері наукових досліджень і урядової статистики; враховуючи, що, незважаючи на це, вони зобов'язані забезпечувати особливі і відповідні гарантії, спрямовані на захист основних прав і приватного життя людей;

35. Враховуючи, що, крім того, обробка персональних даних, яка здійснюється офіційними органами для досягнення цілей, встановлених у конституційному праві чи в міжнародному публічному праві, офіційно визнаних релігійних об'єднань здійснюється на важливих підставах суспільного інтересу;

36. Враховуючи, що якщо в ході виборчої діяльності функціонування демократичної системи в деяких державах-членах вимагає від політичних партій збору даних про політичні погляди людей, обробка таких даних може бути дозволенна на важливих підставах суспільного інтересу, за умови створення відповідних гарантій;

37. Враховуючи, що обробка персональних даних для цілей журналістики чи художньої або літературної творчості, зокрема в аудіовізуальному секторі, повинна підлягати звільненню від вимог, викладених у деяких положеннях даної Директиви, у тій мірі, у якій це необхідно для узгодження основних прав людини зі свободою інформації і особливо з правом одержувати і передавати інформацію, яке гарантується, передусім, статтею 10 Європейської конвенції про захист прав людини й основних свобод; враховуючи, що, виходячи з цього, держави-члени повинні визначити винятки і відступи, необхідні для досягнення балансу між основними правами в тому, що стосується загальних заходів щодо законності обробки даних, заходів для передачі даних третім країнам і повноважень наглядового органу; враховуючи, однак, що це не повинно призвести до того, що держави-члени встановлять винятки відносно заходів із забезпечення безпеки обробки; враховуючи, що, принаймні, наглядо-

вий орган, відповідальний за цю галузь, повинен також бути наділений певними апостеріорними повноваженнями, наприклад, видавати регулярний звіт чи передавати справи судовим органам;

38. Враховуючи, що для того, щоб обробка даних була справедливою, суб'єкт даних повинен могти дізнатися про існування факту обробки і, якщо дані отримані від нього, повинен одержати точну і повну інформацію з урахуванням обставин збору даних;

39. Враховуючи, що деякі випадки обробки стосуються даних, які контролер одержав не від суб'єкта даних безпосередньо; враховуючи, крім того, що дані можуть бути відкриті законним шляхом третій стороні, навіть якщо це не було передбачено під час збору даних у суб'єкта даних; враховуючи, що у всіх цих випадках суб'єкт даних повинен бути проінформований про це тоді, коли дані записуються, чи пізніше, коли вони вперше розкриваються третій стороні;

40. Враховуючи, однак, що дане зобов'язання не обов'язково накладати, якщо суб'єкт даних вже має необхідну інформацію; враховуючи, що, крім того, дане зобов'язання не накладається, якщо запис чи розкриття третій стороні будуть чітко передбачені законом або якщо надання інформації суб'єкту даних виявиться неможливим чи зажадає непропорційних зусиль, що може відбутися у випадку, коли обробка даних проводиться в історичних, статистичних чи наукових цілях; враховуючи, що при цьому може враховуватися число суб'єктів даних, вік даних і будь-які затверджені компенсаційні заходи;

41. Враховуючи, що будь-яка особа повинна мати можливість використати право доступу до даних, які стосуються її і перебувають в обробці, з метою їхньої перевірки, особливо перевірки точності і законності обробки; враховуючи, що з тих же причин кожен суб'єкт даних повинен також мати право знати логіку, застосовувану при автоматизованій обробці даних, які його стосуються, принаймні у випадку з автоматизованими рішеннями, про які йде мова в пункті 1 статті 15; враховуючи, що це право не повинне негативно впливати на торгові секрети чи інтелектуальну власність і, зокрема, на авторське право, що захищає програмне забезпечення; враховуючи, що, незважаючи на це, врахування цих факторів не повинне призвести до відмови суб'єкту даних у наданні всієї інформації;

42. Враховуючи, що держави-члени можуть в інтересах суб'єкта даних чи з метою захисту прав і свобод інших осіб обмежити права на доступ і на інформування; враховуючи, що вони, наприклад, можуть прийняти рішення, що доступ до медичних даних може бути отриманий тільки через медичного працівника;

43. Враховуючи, що обмеження прав на доступ і інформування та обмеження деяких інших зобов'язань контролера можуть подібним чином бути встановлені державами-членами в тій мірі, у якій вони необхідні для захисту, наприклад, національної безпеки, оборони, суспільної безпеки чи важливих економічних і фінансових інтересів держави-члена чи Союзу, а також у карних

розслідуваннях, переслідуваннях і діях у зв'язку з порушенням етики встановлених професій; враховуючи, що перелік винятків і обмежень повинен включати задачі моніторингу, інспекції чи регулювання, що необхідні в трьох останніх із згаданих сфер відносно суспільної безпеки, економічних чи фінансових інтересів і попередження злочинності; враховуючи, що перерахування задач у цих трьох сферах не впливає на законність винятків чи обмежень, встановлених із причин державної безпеки чи оборони;

44. Враховуючи, що держави-члени можуть бути змушені, на підставі положень права Співтовариства, відступати від положень даної Директиви в тому, що стосується права доступу, зобов'язання інформувати фізичних осіб, якості даних; з метою виконання деяких із вищезгаданих цілей;

45. Враховуючи, що у випадках, коли дані можуть оброблятися законним шляхом на підставі суспільного інтересу, офіційних повноважень чи законних інтересів фізичної або юридичної особи, будь-який суб'єкт даних повинен, незважаючи на це, мати право на законних і незаперечних підставах, що стосуються його конкретної ситуації, опротестувати обробку будь-яких даних, які його стосуються; враховуючи, що, незважаючи на це, держави-члени можуть передбачити протилежні національні положення;

46. Враховуючи, що захист прав і свобод суб'єктів даних при обробці персональних даних вимагає прийняття відповідних технічних й організаційних заходів як при розробці системи обробки, так і під час самої обробки, зокрема для забезпечення безпеки і, таким чином, запобігання будь-якій незаконній обробці; враховуючи, що держави-члени повинні забезпечити дотримання контролерами таких заходів; враховуючи, що ці заходи повинні забезпечити відповідний рівень безпеки, з огляду на існуюче положення речей і вартість їхньої реалізації з врахуванням пов'язаного з обробкою ризику і характеру даних, що підлягають захисту;

47. Враховуючи, що, якщо повідомлення, що містить персональні дані, передається за допомогою телекомунікацій чи електронної пошти, єдиною метою яких є передача таких повідомлень, контролером у відношенні персональних даних, які містяться в повідомленні, буде вважатися особа, від якої виходить це повідомлення, а не особа, що надає послуги з передачі повідомлень; враховуючи, що, незважаючи на це, особи, що надають ці послуги, будуть, як правило, вважатися контролерами стосовно обробки додаткових персональних даних, необхідних для надання цієї послуги;

48. Враховуючи, що процедури повідомлення наглядового органу покликані забезпечити розкриття цілей і основних принципів будь-якого процесу обробки для перевірки того, що процес здійснюється відповідно до національних заходів, прийнятих відповідно до даної Директиви;

49. Враховуючи, що для того, щоб уникнути непотрібних адміністративних формальностей, звільнення від зобов'язання повідомляти і спрощення необхідного повідомлення можуть бути передбачені державами-членами у випадках, коли обробка навряд чи може завдати шкоди правам і свободам

суб'єктів даних, і за умови, що вона проводиться відповідно до прийнятої державою-членом міри, що визначає її рамки; враховуючи, що звільнення чи спрощення можуть бути передбачені державами-членами за умови, що особа, призначена контролером, гарантує, що здійснена обробка даних навряд чи може завдати шкоди правам і свободам суб'єктів даних; враховуючи, що такий службовець із захисту даних незалежно від того, чи є він співробітником інституту контролера чи ні, повинен мати можливість виконувати свої функції абсолютно незалежно;

50. Враховуючи, що звільнення чи спрощення може бути передбачене у випадках із процесами обробки, єдиною метою яких є ведення реєстру, що відповідно до національного законодавства, призначений для надання інформації населенню і є відкритим для звертань населення чи будь-якої особи, що демонструє законний інтерес;

51. Враховуючи, що, незважаючи на це, спрощення чи звільнення від зобов'язання повідомляти не звільняє контролера від жодних інших зобов'язань, що випливають з даної Директиви;

52. Враховуючи, що в цьому контексті апостеріорна перевірка компетентними органами в цілому повинна розглядатися як достатній захід;

53. Враховуючи, що, незважаючи на це, при деяких процесах обробки існує імовірність певних ризиків для прав і свобод суб'єктів даних в силу їхньої природи, їхнього обсягу чи їхніх цілей, як, наприклад, позбавлення фізичних осіб права, допомоги чи контракту, або через особливе використання нових технологій; враховуючи, що держави-члени за власним бажанням визначають ці ризики у своєму законодавстві;

54. Враховуючи, що з врахуванням всіх процесів обробки, які здійснюються в суспільстві, кількість процесів, які створюють такий особливий ризик, повинна бути обмеженою; враховуючи, що держави-члени повинні передбачити, що наглядовий орган чи службовець із захисту даних разом з органом перевіряють таку обробку до її виконання; враховуючи, що після проведення такої попередньої перевірки наглядовий орган у відповідності із своїм національним законодавством дає свій висновок чи дозвіл на здійснення обробки; враховуючи, що така перевірка може в однаковій мірі відбуватися в ході підготовки або законодавчого заходу національного парламенту, або заходу, що базується на такому законодавчому заході, що визначає природу обробки і встановлює відповідні гарантії;

55. Враховуючи, що у випадку порушення контролером прав суб'єктів даних, національне законодавство повинне передбачити судовий спосіб захисту; враховуючи, що будь-яка шкода, що може бути завдана людині в результаті незаконної обробки даних, повинна відшкодовуватися контролером, який може бути звільнений від відповідальності, якщо доведе, що він не є відповідальним за цю шкоду, зокрема у випадках, коли він встановлює наявність провини суб'єкта даних чи за форс-мажорних обставин; враховуючи, що санкції повинні застосовуватися до будь-якої особи, незалежно від того,

керуються вони приватним чи публічним правом, якщо вона не виконує національних заходів, прийнятих відповідно до даної Директиви;

56. Враховуючи, що транскордонні потоки персональних даних необхідні для розширення міжнародної торгівлі; враховуючи, що захист фізичних осіб, гарантований у Співтоваристві даною Директивою, не перешкоджає передачі персональних даних третім країнам, що забезпечують адекватний рівень захисту; враховуючи, що адекватність рівня захисту, наданого третіми країнами, повинна оцінюватися у світлі всіх обставин, пов'язаних із процесом передачі чи сукупністю процесів передачі;

57. Враховуючи, що, з одного боку, передача персональних даних третій країні, що не забезпечує адекватний рівень захисту, повинна бути заборонена;

58. Враховуючи, що повинні бути прийняті положення, які передбачають винятки з такої заборони при визначених обставинах: коли суб'єкт даних дав свою згоду; коли передача даних необхідна для контракту чи права вимоги; коли того вимагає захист важливого суспільного інтересу, наприклад, у випадках міжнародної передачі даних між податковими і митними органами чи між службами, що відповідають за питання соціального забезпечення, або коли передача даних здійснюється з реєстру, що створений відповідно до закону і призначений для консультацій населення чи осіб, що мають законний інтерес; враховуючи, що в цьому випадку така передача даних не повинна включати всі дані чи всі категорії даних, що містяться в реєстрі, і оскільки реєстр призначений для звертання осіб, що мають законний інтерес, передача даних повинна здійснюватися тільки на прохання цих осіб чи у випадку, якщо вони будуть одержувачами даних;

59. Враховуючи, що можуть бути застосовані особливі заходи, спрямовані на компенсацію відсутності захисту в третій країні, у випадках, коли контролер пропонує відповідні гарантії; враховуючи, що, крім того, повинні бути передбачені положення відносно порядку переговорів між Співтовариством і такими третіми країнами;

60. Враховуючи, що, в будь-якому випадку, передача даних третій країні може здійснюватися тільки в повній відповідності до положень, прийнятих державами-членами відповідно до даної Директиви, зокрема її статті 8;

61. Враховуючи, що держави-члени і Комісія в межах своїх повноважень повинні заохочувати профспілкові об'єднання та інші зацікавлені представницькі організації до складання кодексів поведінки для того, щоб сприяти в застосуванні даної Директиви, беручи до уваги особливі характеристики обробки даних, що проводиться у визначених галузях, і дотримуючись національних положень, прийнятих з метою виконання даної Директиви;

62. Враховуючи, що створення в державах-членах наглядових органів, що наділені повною незалежністю у виконанні своїх функцій, є істотним елементом захисту фізичних осіб при обробці персональних даних;

63. Враховуючи, що такі органи повинні мати необхідні засоби для виконання своїх обов'язків, включаючи повноваження із розслідування і втру-

чання, зокрема у випадках скарг фізичних осіб, і повноваження брати участь у судових розглядах; враховуючи, що такі органи повинні сприяти забезпеченню прозорості обробки в державах-членах, до юрисдикції яких вони належать;

64. Враховуючи, що органи влади різних держав-членів повинні допомагати одна одній у виконанні своїх обов'язків для того, щоб забезпечити дотримання правил захисту на належному рівні на всій території Європейського Союзу;

68. Враховуючи, що викладені в даній Директиві принципи щодо захисту прав і свобод фізичних осіб, особливо, їхнього права на невтручання в приватне життя, при обробці персональних даних, можуть бути доповнені чи уточнені, зокрема це стосується певних галузей, визначених правилами, що базуються на цих принципах;

69. Враховуючи, що державам-членам повинен надаватися період часу, що не перевищує трьох років з моменту набуття чинності національними заходами, що впроваджують дану Директиву, для послідовного застосування таких нових національних правил до всіх процесів обробки, що уже ведуться; враховуючи, що для полегшення їхньої рентабельної реалізації державам-членам надаватиметься подальший період, що закінчується через 12 років з дати прийняття даної Директиви, для забезпечення відповідності існуючих неавтоматизованих картотек до деяких положень Директиви; враховуючи, що, якщо дані, що містяться в таких картотеках, обробляються вручну в період цього подовженого перехідного періоду, ці картотеки повинні приводитись у відповідність до цих положень під час такої обробки;

70. Враховуючи, що суб'єкту даних не потрібно повторно давати свою згоду для того, щоб дозволити контролеру після набуття чинності національними положеннями, прийнятими відповідно до даної Директиви, продовжити обробку будь-яких чутливих даних, необхідних для виконання контракту, укладеного на основі вільної та поінформованої згоди до набуття чинності такими положеннями;

71. Враховуючи, що дана Директива не перешкоджає державам-членам у регулюванні маркетингової діяльності, орієнтованої на споживачів, що проживають на їхній території, у тій мірі, в якій таке регулювання не стосується захисту фізичних осіб при обробці персональних даних;

72. Враховуючи, що дана Директива дозволяє враховувати принцип громадського доступу до офіційних документів при здійсненні принципів, викладених у цій Директиві,

ПРИЙНЯЛИ ЦЮ ДИРЕКТИВУ:

Глава I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1
Мета Директиви

Відповідно до цієї Директиви, держави-члени захищають основні права і свободи фізичних осіб і, особливо, їхнє право на невтручання в особисте життя при обробці персональних даних.

Держави-члени не обмежують і не забороняють вільну передачу персональних даних між державами-членами на підставах, пов'язаних із захистом, що надається згідно з п.1.

Стаття 2
Визначення

В цілях даної Директиви:

(a) «персональні дані» означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити («суб'єкт даних»); особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості;

(b) «обробка персональних даних» («обробка») означає будь-яку операцію чи сукупність операцій, здійснюваних з персональними даними (за допомогою чи без допомоги автоматизованих засобів), таких, як збір, реєстрація, організація, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття за допомогою передачі, поширення чи іншого надання, упорядкування чи комбінування, блокування, стирання чи знищення;

(c) «картотека персональних даних» («картотека») означає будь-який структурований масив персональних даних, що є доступним за визначеними критеріями, незалежно від того, чи є такий масив централізованим, децентралізованим або розділеним на функціональних або географічних засадах;

(d) «контролер» означає фізичну чи юридичну особу, державний орган, агентство або будь-який інший орган, що, окремо чи разом з іншими, визначає цілі і засоби обробки персональних даних; якщо цілі і засоби обробки визначені законодавчими чи нормативними положеннями держави чи Співтовариства, контролер або особливі критерії його призначення можуть визначатися правом держави чи Співтовариства;

(e) «оператор обробки даних» означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, що обробляє персональні дані від імені контролера;

(f) «третя сторона» означає будь-яку фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, інший ніж суб'єкт даних, контролер, оператор обробки даних і особи, що, будучи безпосередньо підпо-

рядкованими контролеру чи оператору обробки даних, уповноважені обробляти дані;

(g) «одержувач» означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, якому надаються дані, незалежно до того, третя особа це чи ні; однак органи, що можуть одержувати дані в рамках окремого запиту, не розглядаються як одержувачі;

(h) «згода суб'єкта даних» означає будь-яке вільно виражене спеціальне і поінформоване зазначення його бажань, за допомогою якого суб'єкт даних дає свою згоду на обробку персональних даних, які його стосуються.

Стаття 3

Сфера застосування

1. Дана Директива застосовується до обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів, а також до обробки неавтоматичними засобами персональних даних, що є частиною картотеки чи призначені для внесення в картотеку.

2. Дана Директива не застосовується до обробки персональних даних:

— протягом діяльності, що не входить у сферу дії права Співтовариства, такої, як діяльність, передбачена Розділами V і VI Договору про Європейський Союз і, будь-якому випадку, до операцій із обробки даних, що стосуються суспільної безпеки, оборони, державної безпеки (включаючи економічний добробут державі, якщо процес обробки стосується питань державної безпеки) і діяльності держави в сфері кримінального права;

— якщо вона проводиться фізичною особою під час діяльності виключно особистого чи побутового характеру.

Стаття 4

Застосовуване національне законодавство

1. Кожна держава-член застосовує національні положення, які вона приймає відповідно до даної Директиви, до обробки персональних даних, якщо:

(a) обробка здійснюється в контексті діяльності установи контролера на території держави-члена якщо ж один і той самий контролер заснований на території декількох держав-членів, він повинен вжити всіх необхідних заходів для забезпечення того, що кожна з цих установ дотримується зобов'язань, передбачених відповідним національним законодавством;

(b) контролер заснований не на території держави-члена, а у місці, де його національне законодавство застосовується відповідно до міжнародного публічного права;

(c) контролер не заснований на території Співтовариства, але з метою обробки персональних даних використовує автоматизоване чи будь-яке інше устаткування, розташоване на території згаданої держави-члена, за умови, що таке устаткування не використовується винятково з метою транзиту через територію Співтовариства.

2. За обставин, передбачених у підпункті (c) пункту 1, контролер повинен призначити представника на території цієї держави-члена, без шкоди для судових позовів, що можуть бути подані проти самого контролера.

Глава II
ЗАГАЛЬНІ ПРАВИЛА ЗАКОННОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 5

Держави-члени в рамках положень цієї Глави більш точно визначають умови, за яких обробка персональних даних є законною.

Розділ I
Принципи, які стосуються якості даних

Стаття 6

1. Держави-члени передбачають, що персональні дані повинні:

(a) оброблятися чесно і законно;

(b) збиратися для встановлених, чітких і законних цілей і надалі не оброблятися у спосіб, несумісний з цими цілями. Подальша обробка даних в історичних, статистичних чи наукових цілях не розглядається як несумісна, якщо держави-члени забезпечують відповідні гарантії;

(c) бути достовірними, відповідними і не надлишковими відносно цілей, заради яких вони збираються і/або надалі обробляються;

(d) бути точними і, якщо необхідно, обновлятися; слід вжити всіх розумних заходів, щоб гарантувати, що дані, які є неточними чи неповними, з урахуванням цілей, заради яких вони були зібрані чи заради яких вони надалі обробляються, стиралися чи виправлялися;

(e) зберігатися у формі, що дозволяє встановлювати особу суб'єктів даних не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються. Держави-члени встановлюють відповідні гарантії для персональних даних, що зберігаються протягом більш тривалих періодів з метою історичного, статистичного чи наукового використання.

2. Забезпечення дотримання пункту 1 покладається на контролера.

Розділ II
Критерії законності обробки даних

Стаття 7

1. Держави-члени передбачають, що персональні дані можуть оброблятися тільки за умови, що:

(a) суб'єкт даних недвозначно дав свою згоду; чи

(b) обробка необхідна для виконання контракту, стороною якого є суб'єкт даних, чи для вживання заходів на прохання суб'єкта даних до підписання контракту; чи

(c) обробка необхідна для дотримання правового зобов'язання, яким зв'язаний контролер; чи

(d) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних; чи

(e) обробка необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані; чи

(f) обробка необхідна в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних, що вимагають захисту згідно з пунктом 1 статті 1.

Розділ III
Особливі категорії обробки

Стаття 8 Обробка особливих категорій даних

1. Держави-члени забороняють обробку персональних даних, що вказують на расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, профспілкове членство, і обробку даних, що стосуються здоров'я чи статевого життя людини.

2. Пункт 1 не застосовується, якщо:

(a) суб'єкт даних дав свою недвозначну згоду на обробку цих даних, крім випадків, коли законодавство держав-членів передбачає, що заборона, згадана в пункті 1, не може бути знята при наданні згоди з боку суб'єкта даних; чи

(b) обробка необхідна з метою виконання зобов'язань і особливих прав контролера в області законодавства про працевлаштування, у тій мірі, у якій це Дозволено національним законодавством, що передбачає адекватні гарантії; чи

(c) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних чи іншої особи, якщо суб'єкт даних не може дати свою згоду через свою недієздатність чи неправоздатність; чи

(d) обробка проводиться в ході законної діяльності з відповідними гарантіями Установою, асоціацією чи будь-яким іншим некомерційним органом у політичних, філософських, релігійних чи профспілкових цілях і за умови, що обробка стосується винятково членів цього органу чи людей, що у зв'язку з цими цілями перебувають у постійному контакті з ним, і що дані не надаються третій особі без згоди суб'єктів даних; чи

(e) обробка стосується даних, що явно оприлюднені суб'єктами даних, чи необхідна для порушення, виконання чи захисту судових позовів.

3. Пункт 1 не застосовується, якщо обробка даних необхідна з метою профілактичної медицини, медичної діагностики, надання медичних послуг чи лікування або для керування служб охорони здоров'я, і якщо ці дані обробляються медичним працівником, що, відповідно до національного законодавства чи правил, встановлених національними компетентними органами, зв'язаний зобов'язанням збереження професійної таємниці, чи іншою особою, що зв'язана подібним зобов'язанням збереження таємниці.

4. За умови надання відповідних гарантій, держави-члени можуть на важливій підставі суспільного інтересу встановлювати винятки на додачу до

тих, що передбачені в пункті 2, за допомогою або національного закону, або рішення наглядового органу.

5. Обробка даних, що стосуються правопорушень, обвинувачення у кримінальних справах чи засобів безпеки, може проводитися тільки під контролем офіційного органу або якщо національне законодавство передбачає відповідні спеціальні гарантії, з винятками, що можуть бути надані державою-членом відповідно до національних положень, що передбачають відповідні спеціальні гарантії. Однак повний реєстр обвинувачень у кримінальних справах може вестися лише під контролем офіційного органу.

Держави-члени можуть передбачити, що дані про адміністративні санкції чи про судові рішення в цивільних справах також повинні оброблятися під контролем офіційного органу.

6. Відступи від пункту 1, передбачені у пунктах 4 і 5, доводяться до відома Комісії.

7. Держави-члени визначають умови, за яких може оброблятися національний ідентифікаційний код чи будь-який інший ідентифікатор загального застосування.

Розділ IV

Інформація, що надається суб'єкту даних

Стаття 10 Інформація у разі збору даних від суб'єкта даних

Держави-члени передбачають, що контролер чи його представник повинні надати суб'єкту даних, у якого збираються дані щодо нього самого, принаймні таку інформацію, крім тих випадків, коли в нього вже є ця інформація:

(a) особа контролера і мого представника, якщо такий є;

(b) цілі обробки, для якої призначені дані;

(c) будь-яка додаткова інформація, як наприклад:

— одержувачі чи категорії одержувачів даних,

— обов'язковість чи добровільність відповіді на питання, а також можливі наслідки за ненадання відповіді,

— існування права доступу і права на виправлення даних, які його стосуються у тій мірі, у якій така додаткова інформація необхідна, з огляду на особливі обставини, за яких дані збираються, для гарантії справедливої обробки у відношенні суб'єкта даних обробки.

Стаття 11

Інформація у разі, якщо дані не були отримані від суб'єкта даних

1. У випадку, якщо дані не були отримані від суб'єкта даних, держави-члени передбачають, що контролер чи його представник повинні під час реєстрації персональних даних чи, якщо передбачене розголошення даних третій особі, не і пізніше того часу, коли дані вперше розголошуються, надати суб'єкту даних таку і інформацію, крім тих випадків, коли в нього вже є ця інформація:

(a) особа контролера і його представника, якщо такий є;

(b) цілі обробки;

(c) будь-яка додаткова інформація, як, наприклад:

– категорії використовуваних даних,

– одержувачі чи категорії одержувачів,

– існування права доступу і права на виправлення даних, які його стосуються у тій мірі, у якій така додаткова інформація необхідна, з огляду на особливі обставини, за яких дані обробляються, для гарантії справедливої обробки у відношенні суб'єкта даних обробки.

2. Пункт 1 не застосовується в певних випадках, зокрема при обробці даних у статистичних цілях чи з метою історичних чи наукових досліджень, коли надання такої інформації виявляється неможливим чи може спричинити непропорційні зусилля або коли реєстрація чи надання даних чітко передбачене законодавством. У цих випадках держави-члени надають відповідні гарантії.

Розділ V
Право суб'єкта даних на доступ до даних

Стаття 12
Право доступу

Держави-члени гарантують кожному суб'єкту даних право отримати від контролера:

(a) без обмежень через розумні інтервали часу і без надмірної затримки або витрат:

– підтвердження того, обробляються чи ні дані, які його стосуються, і інформацію, принаймні про цілі обробки, категорії розглянутих даних і про одержувачів чи категорії одержувачів, яким надаються дані;

– повідомлення йому в зрозумілій формі про те, що дані знаходяться в процесі обробки, і будь-яку іншу доступну інформацію щодо їхнього джерела;

– інформацію про логіку, використовувану під час автоматизованої обробки даних, що його стосуються, принаймні у випадку автоматизованих рішень, згаданих у статті 15;

(b) залежно від випадку, виправлення, стирання чи блокування даних, обробка яких не відповідає положенням даної Директиви, зокрема через неповноту чи неточність даних;

(c) повідомлення третім сторонам, яким були надані дані, про будь-яке виправлення, стирання чи блокування, виконане відповідно до підпункту (b), якщо це можливо чи не вимагає непропорційних зусиль.

Розділ VI
Винятки та обмеження

Стаття 13
Винятки та обмеження

1. Держави-члени можуть вживати законодавчих заходів для обмеження обсягів обов'язків і прав, передбачених у статтях 6, 10, 11, 12 і 21, якщо таке обмеження є необхідним, щоб гарантувати:

(a) національну безпеку;

(b) оборону;

(c) суспільну безпеку;

(d) запобігання, розслідування, виявлення і судове переслідування кримінальних злочинів чи порушень етики визначених професій;

(e) важливий економічний чи фінансовий інтерес держави-члена чи Європейського Союзу, включаючи монетарні, бюджетні і податкові питання;

(f) моніторинг, перевірку чи регулятивну функцію, пов'язану, навіть зрідка, з виконанням офіційних повноважень у випадках, вказаних у підпунктах (c), (d) і (e);

(g) захист суб'єкта даних чи прав і свобод інших осіб.

2. За умови виконання відповідних правових гарантій, зокрема того, що дані не використовуються для вживання заходів чи прийняття рішень щодо будь-якої конкретної людини, держави-члени можуть, за явної відсутності якого-небудь ризику втручання в особисте життя, обмежити шляхом законодавчого заходу права, передбачені в статті 12, якщо дані обробляються виключно з метою наукових досліджень чи зберігаються в особовій формі протягом періоду, що не перевищує період часу, необхідного лише для цілі створення статистики.

Розділ VII
Право суб'єкта даних на заперечення

Стаття 14

Право суб'єкта даних на заперечення

Держави-члени надають суб'єкту даних право:

(a) принаймні у випадках, передбачених у підпунктах (e) і (f) статті 7, заперечувати в будь-який час на безсумнівних законних підставах, пов'язаних з його конкретною ситуацією, проти обробки даних, які його стосуються, за винятком випадків, коли інше передбачено національним законодавством. За наявності обґрунтованого заперечення в розпочатій контролером обробці більше не можуть використовуватися такі дані;

(b) заперечувати, за вимогою і безкоштовно, проти обробки персональних даних, що його стосуються і які контролер має намір обробити з метою прямого маркетингу, чи бути проінформованим до того, як персональні дані будуть вперше надаватися третім особам чи використовуватися від їхнього імені з метою прямого маркетингу, при цьому йому чітко пропонується право на безкоштовне заперечення проти такого надання чи використання даних.

Держави-члени вживають необхідних заходів для забезпечення того, щоб суб'єкти даних були інформовані про існування права, про яке йдеться в першій частині підпункту (b).

Стаття 15

Автоматизовані індивідуальні рішення

1. Держави-члени надають кожній особі право на те, щоб стосовно неї не приймалося рішення, що має для неї правові наслідки чи значною мірою зачіпає її і яке ґрунтується виняткова на автоматизованій обробці даних, призначеній для оцінки деяких його особистісних характеристик, як, наприклад, виконання нею професійних обов'язків, кредитоспроможності, надійності, поведінки і т.д.

2. Відповідно до інших статей даної Директиви, держави-члени передбачають, що стосовно особи може бути прийняте рішення, про яке йдеться в пункті 1, якщо це рішення:

(a) прийняте в ході укладання чи виконання контракту, за умови, що прохання про укладання чи виконання контракту, подане суб'єктом даних, було задоволене або існують відповідні заходи для захисту його законних інтересів, як, наприклад, заходи, що дозволяють йому виразити свою точку зору; чи

(b) санкціоноване законом, що також передбачає заходи для захисту законних інтересів суб'єкта даних.

Розділ VIII
Конфіденційність і безпека обробки

Стаття 16

Конфіденційність обробки

Будь-яка особа, яка діє у підпорядкуванні контролеру чи оператору обробки, включаючи самого оператора обробки, який має доступ до персональних даних, не повинні обробляти їх інакше, як за вказівкою контролера, за винятком тих випадків, коли це вимагається законом.

Стаття 17

Безпека обробки

1. Держави-члени передбачають, що контролер повинен здійснювати відповідні технічні й організаційні заходи для захисту персональних даних від випадкового або незаконного знищення чи випадкової втрати, зміни, несанкціонованого розкриття чи доступу, зокрема, якщо обробка включає передачу даних через мережу, і від усіх інших незаконних форм обробки.

Такі заходи, із врахуванням нинішнього стану речей і вартості їхнього здійснення, повинні забезпечувати рівень безпеки, співвідносний з ризиком, що супроводжує обробку, і з природою даних, що захищаються.

2. Держави-члени передбачають, що контролер повинен, у випадку обробки від свого імені, вибрати оператора обробки, що надає достатні гарантії щодо технічних заходів безпеки і організаційних заходів, що регулюють обробку, яка має проводитись, і повинен забезпечити виконання цих заходів.

3. Здійснення обробки за допомогою оператора обробки даних повинне регулюватися договором чи правовим актом, яким оператор обробки даних підпорядковується контролеру і який передбачає, зокрема, таке:

– оператор обробки даних повинен діяти тільки за вказівками контролера;

– зобов'язання, викладені в пункті 1 і визначені законодавством держави-члена, у якому призначений оператор обробки даних, повинні також застосовуватися до оператора обробки.

4. З метою збереження доказів, розділи договору чи юридичного акта про захист даних і вимоги про заходи, згадані у пункті 1, повинні бути викладені в письмовій формі чи в іншій рівносильній формі.

Розділ IX
Повідомлення

Стаття 18

Зобов'язання повідомляти наглядовий орган

1. Держави-члени передбачають, що контролер чи його представник, якщо такий існує, повинні повідомити наглядовий орган, згаданий у статті 28, про обробку до проведення будь-якої повної чи часткової автоматизованої операції з обробки даних чи сукупності таких операцій, призначених служити єдиній цілі чи декільком взаємозалежним цілям.

2. Держави-члени можуть передбачити спрощення чи звільнення від повідомлення тільки у таких випадках і за таких умов:

– якщо для категорій операцій з обробки, які, беручи до уваги дані, що будуть оброблятися, навряд чи можуть завдати шкоди правам і свободам суб'єктів даних, вони визначають цілі обробки даних, дані чи категорії даних, які проходять обробку, категорію чи категорії суб'єктів даних, одержувачів чи категорії одержувачів, яким будуть надані дані, і період часу, протягом якого дані будуть зберігатися, і/чи

– якщо контролер відповідно до національного права, яким він керується, призначає посадову особу із захисту персональних даних, що, серед іншого, відповідає за таке:

– забезпечення у незалежний спосіб внутрішнього застосування національних положень, прийнятих на виконання цієї Директиви;

– ведення реєстру операцій із обробки, що проводиться контролером і містить інформацію, згадану в пункті 2 статті 21, у такий спосіб забезпечуючи те, що операції із обробки навряд чи завдадуть шкоди правам і свободам суб'єктів даних.

3. Держави-члени можуть передбачити, що пункт 1 не застосовується до обробки, єдиною метою якої є ведення реєстру, що, відповідно до законодавчих чи нормативних положень, призначений для надання інформації громадськості і відкритий для консультування або населення в цілому, або будь-якої особи, що проявляє законний інтерес.

4. Держави-члени можуть передбачити звільнення від зобов'язання щодо повідомлення чи спрощення системи повідомлення у випадку здійснення операцій із обробки, про які йдеться в підпункті (d) пункту 2 статті 8.

5. Держави-члени можуть передбачити повідомлення про деякі чи всі неавтоматизовані операції з персональними даними або передбачити спрощений порядок повідомлення про ці операції із обробки.

Стаття 19

Зміст повідомлення

1. Держави-члени визначають інформацію, що повинна міститися в повідомленні. Вона повинна включати принаймні таке:

(a) ім'я та адресу контролера і його представника, якщо такий є;

(b) ціль чи цілі обробки;

(c) опис категорії чи категорій суб'єктів даних або категорій їхніх персональних даних;

(d) одержувачів чи категорії одержувачів, яким можуть надаватися дані;

(e) передачі даних, що передбачаються, третім країнам;

(f) загальний опис, що дозволяє зробити попередню оцінку відповідності заходів, прийнятих згідно із статтею 17, для забезпечення безпеки обробки.

2. Держави-члени встановлюють процедури, згідно з якими наглядовий орган повинен бути сповіщений про будь-яку зміну, що зачіпає інформацію, згадану в пункті 1.

Стаття 20

Попередня перевірка

1. Держави-члени визначають операції із обробки, що можуть мати певний ризик для прав і свобод суб'єктів даних, і перевіряють, щоб ці операції із обробки вивчалися до початку обробки.

2. Такі попередні перевірки здійснюються наглядовим органом після одержання повідомлення від контролера чи посадової особи з питань захисту даних, що при виникненні сумнівів повинні радитися з наглядовим органом.

3. Держави-члени можуть також проводити такі перевірки у зв'язку з підготовкою законодавчого заходу національного парламенту або заходу, що базується на такому законодавчому заході і визначає характер обробки та встановлює відповідні гарантії.

Стаття 21

Оголошення операцій із обробки

1. Держави-члени вживають заходів для забезпечення того, що операції із обробки оголошуються.

2. Держави-члени передбачають, що наглядовий орган повинен вести реєстр операцій із обробки, повідомлення про які відбувається згідно із статтею 18.

Реєстр повинен містити принаймні інформацію, перераховану в підпунктах (a) – (e) пункту 1 статті 19. Будь-яка особа може перевірити такий реєстр.

3. Держави-члени передбачають у відношенні операцій із обробки, повідомлення про які не передбачаються, що контролери чи інші органи, призначені державами-членами, надають після запиту будь-якої особи у

відповідній формі принаймні інформацію, перераховану в підпунктах (a) – (e) пункту 1 статті 19.

Держави-члени можуть передбачити, що це положення не застосовується до обробки, єдиною метою якої є ведення реєстру, що згідно із законодавчим чи нормативним положенням передбачає надання інформації населенню і який відкритий для консультування або для населення в цілому, або для будь-якої особи, що може довести свій законний інтерес.

Глава III
ЗАСОБИ СУДОВОГО ЗАХИСТУ, ВІДПОВІДАЛЬНІСТЬ ТА САНКЦІЇ

Стаття 22
Засоби захисту

Без шкоди для будь-якого адміністративного засобу захисту, що може бути передбачений, у тому числі захисту наглядовим органом, згаданому в статті 28, до звертання в судовий орган, держави-члени передбачають право кожної людини на засоби судового захисту від будь-якого порушення прав, гарантованих їй національним законодавством, що застосовується до відповідної обробки.

Стаття 23
Відповідальність

1. Держави-члени передбачають, що будь-яка особа, якій завдано шкоди в результаті незаконної операції із обробки чи будь-якої дії, несумісної із національними положеннями, прийнятими відповідно до цієї Директиви, має право на одержання компенсації від контролера за завдану шкоду.

2. Контролер може бути звільнений від цієї відповідальності цілком чи частково, якщо він доведе, що не є відповідальним за випадок, що став причиною завданої шкоди.

Стаття 24
Санкції

Держави-члени вживають відповідних заходів для забезпечення повного виконання положень даної Директиви і, зокрема, встановлюють санкції, що повинні накладатися у випадку порушення положень, прийнятих відповідно до даної Директиви.

Глава IV
ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІМ КРАЇНАМ

Стаття 25
Принципи

1. Держави-члени передбачають, що передача третій країні персональних даних, що проходять обробку чи призначені для проходження обробки після передачі, може відбуватися за умови, що розглянута третя країна гарантує адекватний рівень захисту, без шкоди для виконання національних положень, прийнятих відповідно до інших положень даної Директиви.

2. Адекватність рівня захисту, наданого третьою країною, розглядається у світлі всіх обставин операції з передачі даних чи сукупності операцій з передачі даних; особливу увагу варто звернути на характер даних, ціль і тривалість запропонованої операції чи операцій із обробки, країну походження даних і країну кінцевого призначення даних, загальні і галузеві норми права, що діють у розглянутій третій країні, і професійні правила та заходи безпеки, що виконуються в цій країні.

3. Держави-члени і Комісія інформують одні одного про випадки, коли вони вважають, що третя країна не забезпечує адекватного рівня захисту, передбаченого пунктом 2.

4. Якщо Комісія дійде висновку, відповідно до процедури, передбаченої в статті 31, що третя країна не забезпечує адекватного рівня захисту, передбаченого пунктом 2 даної статті, держави-члени вживають заходів, необхідних для запобігання будь-якій передачі даних цього ж виду відповідній третій країні.

5. У належний час Комісія проводить переговори з метою виправлення ситуації, що склалася в результаті виявлення фактів згідно з пунктом 4.

6. Комісія може дійти висновку, згідно з процедурою, згаданою в пункті 2 статті 31, що третя країна забезпечує адекватний рівень захисту, передбаченого пунктом 2 даної статті, керуючись своїм внутрішнім законодавством чи міжнародними зобов'язаннями, які вона взяла на себе, особливо після завершення переговорів, передбачених у пункті 5, щодо захисту особистого життя та основних свобод і прав фізичних осіб. Держави-члени вживають заходів, необхідних для виконання рішення Комісії.

Стаття 26

Відступи

1. Шляхом відступу від статті 25 і крім випадків, коли інше передбачено національним законодавством, що регулює особливі випадки, держави-члени передбачають, що передача чи сукупність передач персональних даних третій країні, яка не забезпечує адекватний рівень захисту, згаданий в пункті 2 статті 25, може відбуватися за умови, що:

(a) суб'єкт даних дав свою недвозначну згоду на пропоновану передачу даних; або

(b) передача даних необхідна для виконання контракту між суб'єктом даних і контролером чи для виконання заходів, що передують договору і прийняті у відповідь на прохання суб'єкта даних; або

(c) передача даних необхідна для укладення чи виконання контракту, укладеного в інтересах суб'єкта даних між контролером і третьою стороною; або

(d) передача даних необхідна чи юридично обов'язкова на важливих підставах суспільних інтересів або для встановлення, виконання чи захисту правових вимог; або

(e) передача даних необхідна для захисту життєво важливих інтересів суб'єкта даних; або

(f) передача даних зроблена з реєстру, метою якого, відповідно до законів або положень, є надання інформації населенню і який відкритий для консультацій або населення в цілому, або будь-якої людини, що може продемонструвати законний інтерес, у тому обсязі, за якого умови, передбачені в законодавстві про консультацію, виконуються в особливому випадку.

2. Без шкоди для пункту 1, держава-член може дозволити передачу чи сукупність передач персональних даних третій країні, що не забезпечує адекватного рівня захисту, передбаченого в пункті 2 статті 25, якщо контролер надає відповідні гарантії із захисту невтручання в особисте життя та основних прав і свобод фізичних осіб і в тому, що стосується здійснення відповідних прав; такі гарантії можуть, зокрема, стати результатом відповідних умов договору.

3. Держава-член повідомляє Комісію й інші держави-члени про дозволи, які вона дає відповідно до пункту 2.

Якщо член чи Комісія заперечують проти цього на обґрунтованих підставах, що стосуються захисту невтручання в особисте життя й основних прав і свобод фізичних осіб, Комісія вживає відповідних заходів згідно з процедурою, передбаченою в пункті 2 статті 31. Держави-члени вживають необхідних заходів для виконання рішення Комісії.

4. Якщо Комісія відповідно до процедури, передбаченої в пункті 2 статті 31, вирішує, що деякі стандартні умови договору пропонують достатні гарантії, як того вимагає пункт 2, держави-члени вживають необхідних заходів для виконання рішення Комісії.

Глава VI
НАГЛЯДОВИЙ ОРГАН ТА РОБОЧА ГРУПА ІЗ ЗАХИСТУ ФІЗИЧНИХ ОСІБ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 28
Наглядовий орган

1. Кожна держава-член передбачає, що один чи більше державних органів відповідають за моніторинг застосування в межах її території положень, прийнятих державами-членами відповідно до даної Директиви.

Ці органи діють у повній незалежності при здійсненні функцій, якими вони наділені.

2. Кожна держава-член передбачає, що при розробці адміністративних заходів чи положень, що стосуються захисту прав і свобод фізичних осіб при обробці персональних даних, проводяться консультації з наглядовими органами.

Кожен орган, зокрема, наділений:

– такими слідчими повноваженнями, як право доступу до даних, що є предметом операцій із обробки, і право збирати всю інформацію, необхідну для виконання його обов'язків із здійснення нагляду;

– ефективними повноваженнями на втручання, як то надання висновків до здійснення операцій із обробки відповідно до статті 20, і забезпечення

відповідного опублікування таких висновків, видання розпоряджень про блокування, стирання чи знищення даних, накладення тимчасової чи остаточної заборони на обробку даних, попередження чи винесення догани контролеру, або повноваження звертатися до національних парламентів чи інших політичних інститутів,

– право брати участь у судочинстві, якщо були порушені національні положення, прийняті відповідно до даної Директиви, чи довести ці порушення до відома судових органів.

Рішення наглядового органу, що викликали скарги, можуть бути оскаржені в суді.

4. Кожен наглядовий орган розглядає запити, зроблені будь-якою особою чи об'єднанням, що представляє інтереси цієї особи, про захист її прав і свобод при обробці персональних даних. Особа, якої це стосується, повинна бути поінформована про результати розгляду запиту.

Кожен наглядовий орган, зокрема, розглядає запити про перевірки законності обробки даних, зроблені будь-якою особою, у випадках, коли застосовуються національні положення, прийняті у відповідності до статті 13 даної Директиви. Така особа повинна в будь-якому випадку бути поінформована про те, що перевірка мала місце.

5. Кожен наглядовий орган регулярно складає звіт про свою діяльність. Звіт повинен оприлюднюватись.

6. Кожен наглядовий орган має право, незалежно від того, яке національне законодавство застосовується до відповідної обробки, виконувати на території власної держави-члена повноваження, якими він наділений відповідно до пункту 3. Кожен орган може отримати прохання про виконання його повноважень від органу іншої держави-члена. Наглядові органи співпрацюють один з одним у тій мірі, наскільки це необхідно для виконання їхніх обов'язків, зокрема, шляхом обміну всією корисною інформацією.

7. Держави-члени передбачають, що навіть після звільнення на посадових осіб і персонал наглядового органу поширюється обов'язок зберігати професійну таємницю відносно конфіденційної інформації, до якої вони мають доступ.

Стаття 29

Робоча група із захисту фізичних осіб при обробці персональних даних

1. Цим створюється Робоча група із захисту фізичних осіб при обробці персональних даних, надалі – «Робоча група». Вона має консультативний статус і незалежна у своїй діяльності. Робоча група складається з представника наглядового органу чи органів, призначеного кожною державою-членом, і представника від органа чи органів, створених для установ і органів Співтовариства, а також представника Комісії.

2. Кожен член Робочої групи призначається установою, органом чи органами, які він представляє. Якщо держава-член створила більш ніж один наглядовий орган, вони призначають спільного представника. Ті ж самі поло-

ження повинні застосовуватися до органів, створених для установ і органів Співтовариства.

3. Робоча група приймає рішення простою більшістю представників наглядових органів.

4. Робоча група вибирає свого голову. Термін повноважень голови складає два роки. Він може вибиратися повторно.

5. Секретаріат Робочої групи забезпечується Комісією.

6. Робоча група приймає свій власний регламент.

7. Робоча група розглядає питання, винесені на порядок денний головою або за його власною ініціативою, або на прохання представника наглядового органу чи органів, або на прохання Комісії.

Стаття 30

Робоча група:

(a) розглядає будь-яке питання, що стосується застосування національних заходів, прийнятих відповідно до даної Директиви, з метою сприяння загальному застосуванню таких заходів;

(b) представляє Комісії висновки щодо рівня захисту в Співтоваристві та в третіх країнах;

(c) повідомляє Комісію про будь-яку запропоновану поправку до даної Директиви, про будь-які додаткові чи особливі заходи із захисту прав і свобод фізичних осіб при обробці персональних даних і про будь-які інші запропоновані заходи Співтовариства, що стосуються цих прав і свобод;

(d) виносить висновок про кодекси, складені на рівні Співтовариства.

2. Якщо Робоча група виявляє, що між законами чи практикою держав-членів виникають розбіжності, що можуть порушити рівень захисту осіб при обробці персональних даних у Співтоваристві, вона відповідним чином сповіщає про це Комісію.

3. Робоча група може за власною ініціативою давати рекомендації з усіх питань, які стосуються захисту осіб при обробці персональних даних у Співтоваристві.

4. Висновки і рекомендації Робочої групи передаються Комісії і комітету, передбаченому статтею 31.

5. Комісія повідомляє Робочу групу про дії, розпочаті у відповідь на її висновки і рекомендації. Повідомлення робиться у вигляді доповіді, що також подається Європейському Парламенту і Раді. Доповідь повинна бути оприлюднена.

6. Робоча група складає щорічний звіт про ситуацію відносно захисту фізичних осіб при обробці персональних даних у Співтоваристві та в третіх країнах, яку вона надає Комісії, Європейському Парламенту і Раді. Звіт повинен бути оприлюднений.

ДИРЕКТИВА 97/66/ЄС ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ

Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі?

від 15 грудня 1997 р.

(Витяг)

Офіційний переклад

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

беручи до уваги Договір про заснування Європейського Співтовариства і, зокрема, його статтю 100 а,

беручи до уваги пропозицію Комісії (1),

беручи до уваги висновок Економічного і соціального комітету (2),

діючи відповідно до процедури, викладеної в статті 189Ь Договору (3), в світлі спільного тексту, затвердженого Узгоджувальним комітетом 6 листопада 1997 року,

(1) Враховуючи, що Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних вимагає, щоб держави-члени забезпечували права та свободи фізичних осіб при обробці персональних даних і, зокрема, їхнє право на невтручання в особисте життя, з метою забезпечення вільного потоку персональних даних в Співтоваристві;

(2) Враховуючи, що конфіденційність зв'язку гарантується відповідно до міжнародних документів, що стосуються прав людини (зокрема Європейської конвенції про захист прав людини і основних свобод, а також конституцій держав-членів;

(3) Враховуючи, що зараз в Співтоваристві в телекомунікаційних мережах загального користування запроваджуються нові передові цифрові технології, які зумовлюють певні вимоги щодо захисту персональних даних та невтручання в особисте життя користувача; враховуючи, що розвиток інформаційного суспільства характеризується запровадженням нових телекомунікаційних послуг; враховуючи, що успішний транскордонний розвиток таких послуг, як, наприклад, відео на вимогу, інтерактивного телебачення, частково залежить від віри користувачів в те, що загрози втручання в їхнє особисте життя немає;

(4) Враховуючи, що це стосується, зокрема, випадку із запровадженням цифрової мережі зв'язку з комплексними послугами (ISDN) та цифрових мобільних мереж;

(6) Враховуючи, що Європейський Парламент підкреслив важливість захисту персональних даних та невтручання в особисте життя в телекомунікаційних мережах, зокрема з огляду на запровадження цифрової мережі зв'язку з комплексними послугами (ISDN);

(7) Враховуючи, що у випадку телекомунікаційних мереж загального користування слід розробити спеціальні правові, регулятивні та технічні положення з метою захисту основних прав і свобод фізичних осіб та законних інтересів юридичних осіб, зокрема з огляду на зростання ризику, пов'язаного з автоматичним зберіганням та обробкою даних, що стосуються абонентів і користувачів;

(8) Враховуючи, що правові, регулятивні та технічні положення, прийняті державами-членами стосовно захисту персональних даних, невтручання в особисте життя та законних інтересів юридичних осіб в телекомунікаційному секторі, повинні бути гармонізовані для того, щоб уникнути перешкод на внутрішньому ринку телекомунікацій, відповідно до мети, встановленої в статті 7а Договору; враховуючи, що така гармонізація обмежується вимогами, які необхідні для гарантування того, що не буде створено перешкод на шляху сприяння поширенню і розвитку нових телекомунікаційних послуг і мереж між державами-членами;

(9) Враховуючи, що держави-члени, відповідні постачальники та користувачі, разом з компетентними органами Співтовариства повинні співпрацювати у запровадженні і розробці відповідних технологій, якщо це необхідно для застосування гарантій, передбачених положеннями цієї Директиви;

(10) Враховуючи, що такі нові послуги включають інтерактивне телебачення та відео на вимогу;

(11) Враховуючи, що в телекомунікаційному секторі, зокрема в усіх питаннях, що стосуються захисту основних прав і свобод, які окремо не охоплюються положеннями цієї Директиви, включаючи зобов'язання, які покладаються на контролерів, і права осіб, застосовується Директива 95/46/ЄС; враховуючи, що Директива 95/46/ЄС застосовується до телекомунікаційних послуг, які не є загальнодоступними;

(12) Враховуючи, що ця Директива, подібно до того, що передбачається в статті 3 Директиви 95/46/ЄС, не розглядає питань захисту основних прав і свобод, пов'язаних із діяльністю, що не регулюється правом Співтовариства; враховуючи, що держави-члени самі мають вживати заходів, які вони вважають необхідними для захисту громадського порядку, оборони, державної безпеки (включаючи економічний добробут держави, коли діяльність стосується питань безпеки держави), а також застосування кримінального права; враховуючи, що ця Директива не впливає на здатність держав-членів здійснювати законне перехоплення телекомунікацій для будь-яких із перелічених цілей;

(13) Враховуючи, що абоненти загальнодоступної телекомунікаційної послуги можуть бути фізичними чи юридичними особами; враховуючи, що положення цієї Директиви спрямовані на захист, шляхом доповнення Директиви 95/46/ЄС, основних прав фізичних осіб і, зокрема, їхнього права на невтручання в особисте життя, а також законних інтересів юридичних осіб; враховуючи, що ці положення в жодному разі не можуть накласти на держав-членів зобов'язання поширювати застосування Директиви 95/46/ЄС на захист за-

конних інтересів юридичних осіб; враховуючи, що такий захист забезпечується в рамках відповідного законодавства Співтовариства і держав-членів;

(14) Враховуючи, що застосування певних вимог, пов'язаних з показуванням та обмеженням визначення лінії, з якої робиться з'єднання і з якою з'єднуються, та з автоматичною переадресацією дзвінка на лінії абонентів, підключених до аналогових АТС, не повинне бути обов'язковим в окремих випадках, коли таке застосування виявилося б технічно неможливим чи вимагало б непропорційних економічних зусиль; враховуючи, що для зацікавлених сторін важливо бути поінформованими про такі випадки і що тому держави-члени повинні доводити їх до відома Комісії;

(15) Враховуючи, що постачальники послуг повинні вживати необхідних заходів для гарантування безпеки своїх послуг, якщо необхідно — спільно з оператором мережі, а також інформувати абонентів про особливі загрози порушення безпеки мережі; враховуючи, що безпека оцінюється в світлі положення статті 17 Директиви 95/46/ЄС;

(16) Враховуючи, що слід вжити заходів для запобігання несанкціонованому доступу до зв'язку, щоб захистити конфіденційність зв'язку через телекомунікаційні мережі загального користування та за допомогою загальнодоступних телекомунікаційних послуг; враховуючи, що національне законодавство в деяких державах-членах забороняє навмисний несанкціонований доступ до зв'язку;

(17) Враховуючи, що дані, які стосуються абонентів і які обробляються для встановлення дзвінків, містять інформацію про особисте життя фізичних осіб і пов'язані з правом на поважання таємниці їхнього листування чи пов'язані із законними інтересами юридичних осіб; враховуючи, що такі дані можуть зберігатися тільки тоді, коли це необхідно при наданні послуги для цілей виставляння рахунків чи розрахунків за сполучення, і тільки протягом обмеженого часу; враховуючи, що будь-яка подальша обробка, яку може захотіти здійснити постачальник загальнодоступних телекомунікаційних послуг для цілей просування на ринку власних телекомунікаційних послуг, може дозволятися лише у разі, коли абонент надає на це згоду відповідно до точної та повної інформації, наданої постачальником загальнодоступних телекомунікаційних послуг щодо видів подальшої обробки, яку він має намір здійснити;

(18) Враховуючи, що запровадження деталізованих рахунків покращило можливості перевірки абонентом правильності платежів, які стягуються постачальником послуги; враховуючи, що, водночас, воно може загрожувати таємниці особистого життя користувачів загальнодоступних телекомунікаційних послуг; враховуючи, що, таким чином, для збереження таємниці особистого життя користувача держави-члени повинні заохочувати розвиток таких варіантів телекомунікаційних послуг, як альтернативні механізми платежів, що уможливлюють анонімний та цілком конфіденційний доступ до загальнодоступних телекомунікаційних послуг, наприклад, телефонні картки чи механізми оплати кредитною карткою; враховуючи, що в якості альтернативи держави-члени можуть з тією ж метою вимагати вилучення певної кількості

цифр з номерів, на які здійснюється дзвінок і які вказуються в деталізованих рахунках;

(19) Враховуючи, що в тому, що стосується визначення лінії, з якої здійснюється дзвінок, необхідно захистити право сторони, яка здійснює дзвінок, приховувати показування визначення лінії, з якої робиться дзвінок, і права сторони, якій дзвонять, відхиляти дзвінки з невизначених ліній; враховуючи, що справедливо відхилити показування визначення лінії, з якої робиться дзвінок, в окремих випадках; враховуючи, що деякі абоненти, зокрема лінії допомоги і тому подібні організації, зацікавлені в збереженні анонімності осіб, які їм дзвонять; враховуючи, що в тому, що стосується визначення лінії, необхідно захистити право і законний інтерес сторони, якій дзвонять, приховувати показування визначення лінії, до якої сторона, якій дзвонять, підключена, зокрема у разі переадресованих дзвінків; враховуючи, що постачальники загальнодоступних телекомунікаційних послуг повинні інформувати своїх абонентів про існування визначення ліній, з яких і на які робляться дзвінки в мережі, а також про всі послуги, які пропонуються на базі визначення ліній, з яких і на які робляться дзвінки, і про наявні варіанти таємності; враховуючи, що це дозволить абонентам зробити поінформований вибір про механізми таємності, які вони хочуть використовувати; враховуючи, що варіанти таємності, які надаються окремо по кожній лінії, не обов'язково повинні існувати у вигляді автоматичної мережевої послуги, а можуть бути доступними також і на просте прохання до постачальника загальнодоступної телекомунікаційної послуги;

(20) Враховуючи, що слід передбачити захист абонентів від незручностей, які може створити автоматична переадресація дзвінків іншими особами; враховуючи, що в таких випадках повинна існувати можливість для абонентів припинити переключення переадресованих дзвінків на їхні термінали шляхом простого звертання з проханням про це до постачальника загальнодоступної телекомунікаційної послуги;

(21) Враховуючи, що телефонні довідники широко розповсюджуються і є загальнодоступними; враховуючи, що право на невтручання в особисте життя фізичних осіб та законні інтереси юридичних осіб вимагають, щоб абоненти мали змогу визначати те, якою мірою їхні персональні дані публікуватимуться в телефонному довіднику; враховуючи, що держави-члени можуть обмежувати цю можливість для абонентів, які є фізичними особами;

(22) Враховуючи, що слід передбачити заходи охорони абонентів від втручання в їхнє особисте життя через незапитувані дзвінки чи телефакси; враховуючи, що держави-члени можуть обмежити такі заходи для абонентів, які є фізичними особами;

(24) Враховуючи, що, зокрема, аналогічно до того, що передбачено в статті 13 Директиви 95/46/ЄС, держави-члени можуть обмежити за певних обставин обсяги прав і обов'язків абонентів, наприклад, шляхом забезпечення можливості постачальника загальнодоступної телекомунікаційної послуги

не брати до уваги скасування показування визначення лінії, з якої робиться дзвінок, відповідно до національного законодавства для цілей запобігання і виявлення кримінальних злочинів чи державної безпеки;

(25) Враховуючи, що у разі недотримання прав користувачів та абонентів, національне законодавство має передбачати засіб судового захисту; враховуючи, що санкції повинні накладатися на будь-яку особу, яка не дотримується національних заходів, вжитих відповідно до цієї Директиви, незалежно від того, є така особа суб'єктом приватного чи публічного права;

(28) Враховуючи, що для сприяння дотриманню положень, цієї Директиви потрібні певні спеціальні домовленості щодо обробки даних, яка триває на день набуття чинності національним імплементаційним законодавством відповідно до цієї Директиви,

ПРИЙНЯЛИ ТАКУ ДИРЕКТИВУ:

Стаття 1

Мета та сфера дії

3. Ця Директива не застосовується до діяльності, що виходить за межі права Співтовариства, такої як та, що передбачена в Розділах V і VI Договору про Європейський Союз, і, в жодному разі, до діяльності, що стосується громадського порядку, оборони, державної безпеки (включаючи економічний добробут держави, коли діяльність стосується питань безпеки держави), а також діяльності держави в сфері кримінального права.

Стаття 2

Визначення

На додачу до визначень, наведених в Директиві 95/46/ЄС, для цілей цієї Директиви:

(a) «абонент» означає будь-яку фізичну чи юридичну особу, яка є стороною в контракті з постачальником загальнодоступних телекомунікаційних послуг стосовно надання таких послуг;

(b) «користувач» означає будь-яку фізичну особу, яка користується загальнодоступною телекомунікаційною послугою для особистих чи ділових цілей, при цьому передплата цієї послуги не є обов'язковою;

(c) «телекомунікаційна мережа загального користування» означає системи передавання і, у відповідних випадках, комутаційне обладнання та інші ресурси, що дозволяють передавати сигнали між визначеними кінцевими пунктами за допомогою телеграфу, радіо, оптичних чи інших електромагнітних засобів, які використовуються, повністю чи частково, для надання загальнодоступних телекомунікаційних послуг;

(d) «телекомунікаційна послуга» означає послуги, надання яких повністю чи частково полягає в передачі та маршрутизації сигналів в телекомунікаційних мережах, за винятком радіо- та телевізійного мовлення.

Стаття 3

Послуги, до яких застосовується Директива

1. Ця Директива застосовується до обробки персональних даних у зв'язку з наданням загальнодоступних телекомунікаційних послуг в телекомунікаційних мережах загального користування в Співтоваристві, зокрема через цифрову мережу зв'язку з комплексними послугами (ISDN) та цифрові мобільні мережі загального користування.

2. Статті 8, 9 і 10 застосовуються до абонентських ліній, підключених до цифрових АТС, і, якщо це технічно можливо і не вимагає несумірних економічних зусиль, – до абонентських ліній, підключених до аналогових АТС.

3. Держави-члени повідомляють Комісію про випадки, коли виконати вимоги статей 8, 9 і 10 технічно неможливо або ж це вимагає несумірних інвестицій.

Стаття 4

Безпека

1. Постачальник загальнодоступної телекомунікаційної послуги повинен вживати відповідних технічних та організаційних заходів для гарантування безпеки своїх послуг, якщо потрібно, спільно з оператором телекомунікаційної мережі загального користування в тому, що стосується безпеки мережі.

З врахуванням сучасного стану науки і техніки, а також вартості їхньої реалізації, такі заходи забезпечують рівень безпеки, що відповідає представленому ризику.

2. Уразі особливого ризику порушення безпеки мережі постачальник загальнодоступної телекомунікаційної послуги повинен повідомити абонентів про такий ризик та будь-які можливі засоби захисту, включаючи пов'язані з цим витрати.

Стаття 5

Конфіденційність зв'язку

1. Держави-члени забезпечують в національних положеннях конфіденційність зв'язку за допомогою телекомунікаційної мережі загального користування та загальнодоступних телекомунікаційних послуг. Зокрема, вони забороняють прослуховування, перехоплення, зберігання та інші види перехоплювання і нагляду за зв'язком, окрім того, що здійснюється користувачами, без згоди відповідних користувачів, за винятком випадків, коли на це існує законний дозвіл відповідно до статті 14 (1).

2. Параграф 1 не зачіпає жодного законно санкціонованого записування зв'язку вході законної економічної діяльності з метою надання доказів комерційної транзакції чи будь-якого іншого економічного зв'язку.

Стаття 6

Дані щодо потоку обміну і рахунків

1. Дані щодо потоку обміну, які стосуються абонентів та користувачів і які обробляються для встановлення дзвінка і зберігаються оператором телекомунікаційної мережі загального користування та/чи постачальником за-

гальнодоступної телекомунікаційної послуги, повинні стиратися чи перетворюватися на анонімні після завершення дзвінка без шкоди для положень параграфів 2, 3 і 4.

2. Для цілей виставляння рахунків абонентам і здійснення оплати за сполучення можуть оброблятися вказані в Додатку дані. Така обробка дозволяється тільки до завершення періоду, протягом якого рахунок може законно бути оскаржений чи протягом якого платіж може вимагатися в судовому порядку.

3. Для цілей просування на ринку власних телекомунікаційних послуг постачальник загальнодоступної телекомунікаційної послуги може обробляти дані, про які йдеться в параграфі 2, якщо абонент дав на це свою згоду.

4. Обробка даних щодо потоку обміну та рахунків має обмежуватися особами, які діють в рамках повноважень операторів телекомунікаційних мереж загального користування та/чи постачальників загальнодоступних телекомунікаційних послуг, які займаються виставлянням рахунків чи управлінням потоками обміну, запитами клієнтів, виявленням обману та збутом власних телекомунікаційних послуг постачальника, і ця обробка не повинна виходити за межі того, що необхідно для цілей такої діяльності.

5. Параграфи 1, 2, 3 і 4 застосовуються без шкоди для можливості інформування компетентних органів про дані щодо рахунків та потоків обміну відповідно до застосовуваного законодавства з мстою вирішення спорів, зокрема спорів щодо сполучення чи рахунків.

Стаття 7

Деталізовані рахунки

1. Абоненти мають право на отримання недеталізованих рахунків.

2. Держави-члени застосовують національні положення для узгодження прав абонентів, які отримують деталізовані рахунки, з правом на невтручання в особисте життя користувачів, які з'єднуються, і абонентів, з якими з'єднуються, наприклад, шляхом забезпечення того, що для таких користувачів і абонентів існують достатні альтернативні модальності.

Стаття 8

Показування і обмеження визначення ліній,
з яких і на які здійснюється дзвінок

1. Якщо пропонується показування лінії, з якої робиться дзвінок, користувач, який робить дзвінок, повинен мати можливість за допомогою простих засобів безкоштовно скасовувати показування лінії, з якої робиться дзвінок, окремо для кожного дзвінка. Абонент, який здійснює дзвінок, повинен мати таку можливість окремо для кожної лінії.

2. Якщо пропонується показування лінії, з якої робиться дзвінок, абонент, якому дзвонять, повинен мати можливість за допомогою простих засобів безкоштовно для розумного користування цією функцією запобігати показуванню визначення лінії, з якої робиться дзвінок, для вхідних дзвінків.

3. Якщо пропонується показування лінії, з якої робиться дзвінок, і якщо лінія, з якої робиться дзвінок, визначається до встановлення дзвінка, абонент,

якому дзвонять, повинен мати можливість за допомогою простих засобів відхиляти вхідні дзвінки, коли показування визначення лінії, з якої робиться дзвінок, було скасоване користувачем чи абонентом, які дзвонять.

4. Якщо пропонується показування лінії, з якою існує з'єднання, абонент, якому дзвонять, повинен мати можливість за допомогою простих засобів безплатне скасовувати показування визначення лінії, з якою існує з'єднання, для користувача, який дзвонить.

5. Положення, викладені в параграфі 1, також застосовуються по відношенню до дзвінків із Співтовариства в треті країни; положення, встановлені в параграфах 2, 3 і 4 також застосовуються до вхідних дзвінків з третіх країн.

6. Держави-члени забезпечують, щоб у разі надання показування лінії, з якої робиться дзвінок чи з якою існує з'єднання, постачальники загальнодоступних телекомунікаційних послуг інформували громадськість про це та про можливості, встановлені в параграфах 1, 2, 3 і 4.

Стаття 9

Винятки

Держави-члени забезпечують існування прозорих процедур, якими б регулювався спосіб, у який оператор телекомунікаційної мережі загального користування та/чи постачальник загальнодоступної телекомунікаційної послуги може відхилити скасування показування визначення лінії, з якої робиться дзвінок:

(a) тимчасово – після подання абонентом заяви з проханням прослідкувати зловмисні дзвінки чи дзвінки, які порушують спокій; в такому разі, відповідно до національного законодавства, дані, які містять визначення абонента, який дзвонить, зберігатимуться і оприлюднюватимуться оператором телекомунікаційної мережі загального користування та/чи постачальником загальнодоступної телекомунікаційної послуги;

(b) окремо для певних ліній – для організацій, які займаються екстреними викликами і визнані такими державою-членом, включаючи правоохоронні органи, службу швидкої допомоги та пожежні бригади, з метою відповіді на такі дзвінки.

Стаття 12

Не запитувані дзвінки

1. Використання автоматичних викличних систем без людського втручання (пристрій автоматичного виклику) чи факсимільних пристроїв (факсу) для цілей прямого маркетингу може дозволятися тільки у відношенні абонентів, які дали на це свою попередню згоду.

2. Держави-члени вживають необхідних заходів для забезпечення того, що без стягнення плати за це незапитувані дзвінки для цілей прямого маркетингу за допомогою засобів, інших ніж ті, про які йдеться у параграфі 1, не дозволяються або у разі відсутності згоди відповідних абонентів, або стосовно абонентів, які не бажають отримувати такі дзвінки, при цьому вибір між цими варіантами визначається національним законодавством.

3. Права, які надаються параграфами 1 і 2, застосовуються до абонентів, які є фізичними особами. Держави-члени також гарантують, в рамках законодавства Співтовариства і застосовуваного національного законодавства, що законні інтереси абонентів, інших ніж фізичні особи, також достатньо захищені в тому, що стосується незапитуваних дзвінків.

Стаття 13

Технічні параметри та стандартизація

1. При застосуванні положень цієї Директиви держави-члени забезпечують, за умови виконання параграфів 2 і 3, що стосовно термінального чи іншого телекомунікаційного обладнання не встановлюється жодних обов'язкових вимог щодо технічних параметрів, які могли б перешкодити розміщенню обладнання на ринку та вільному обігу такого обладнання в державах-членах та між ними.

2. Якщо положення цієї Директиви можуть бути виконані тільки шляхом встановлення вимоги щодо технічних параметрів, держави-члени інформують Комісію відповідно до порядку, передбаченого Директивою 83/189/ЄЕС (7), якою встановлюється порядок надання інформації в сфері технічних стандартів та правил.

3. Якщо необхідно, Комісія забезпечуватиме складання спільних європейських стандартів для запровадження певних технічних параметрів, відповідно до законодавства Співтовариства про наближення законів держав-членів щодо телекомунікаційного термінального обладнання, включаючи взаємне визнання їхньої узгодженості, а також Рішення Ради 87/95/ЄЕС від 22 грудня 1986 року про стандартизацію в сфері інформаційних технологій і телекомунікацій.

Стаття 16

Адресати

Ця Директива адресована державам-членам. Вчинено в Брюсселі, 15 грудня 1997 року.

РЕЗОЛЮЦІЯ РАДИ
Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL)
Брюссель, 20 червня 2001 р.

(Витяг)

Офіційний переклад

РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Нагадуючи про цілі Договору про Європейський Союз;

Беручи до уваги Резолюцію Ради від 17 січня 1995 року про законне перехоплення телекомунікацій;

Підтверджуючи потребу дотримуватись права осіб на таємницю при вживанні заходів щодо перехоплення телекомунікацій;

Беручи до уваги використання злочинцями, як і будь-ким іншим, телекомунікацій з метою досягнення своїх цілей та використання ними переваг, наданих можливостями телекомунікаційних систем, як з метою уникнення затримання, так і для скоєння злочинів;

Будучи переконаними, що законний доступ до цих телекомунікацій є життєво важливим для розкриття серйозних злочинів та переслідування злочинців;

Усвідомлюючи вплив новітніх телекомунікаційних технологій на законне перехоплення;

Беручи до уваги те, що метою Резолюції від 17 січня 1995 року було забезпечення платформи для обговорень із постачальниками телекомунікацій оперативних запитів правоохоронних органів, а не накладання на них правових зобов'язань;

Беручи до уваги триваючу роботу правоохоронних органів з метою співробітництва із представниками телекомунікаційної індустрії при обговоренні оперативних запитів та засобів їх задоволення;

Усвідомлюючи той факт, що, хоча Резолюція від 17 січня 1995 року і описала оперативні запити правоохоронних органів, розвиток новітніх технологій зумовлює необхідність подальших роз'яснень;

Відзначаючи вимоги держав-членів продовжувати і підтримувати можливості перехоплення;

Беручи до уваги, що Додаток до цієї Резолюції є важливим підсумком та роз'ясненням оперативних запитів правоохоронних органів у світлі розвитку новітніх технологій,

ПРИЙМАЄ ЦЮ РЕЗОЛЮЦІЮ:

Рада закликає держав-членів забезпечити належне врахування оперативних запитів правоохоронних органів при розвитку та запровадженні у співробітництві із постачальниками послуг зв'язку будь-яких заходів, що можуть мати вплив на здійснення законних форм перехоплення телекомунікацій.

ДОДАТОК ОПЕРАТИВНІ ЗАПИТИ ПРАВООХОРОННИХ ОРГАНІВ

Загальні положення

Відповідно до внутрішнього законодавства усі види телекомунікацій можуть підлягати перехопленню та/чи пошуку під час ведення розслідування. Цей документ пов'язаний із оперативними запитами правоохоронних органів по відношенню до телекомунікаційних мереж загального користування та послуг. Він не містить рекомендацій щодо технічних вимог чи рішень, а є лише викладом настанов для обговорень з технічних питань, необхідних для імплементації.

Сфера застосування послуг

Цей документ застосовується до всіх телекомунікаційних послуг, комутації каналів та пакетів, мереж стаціонарного та мобільного зв'язку і послуг.

Для стаціонарних мереж це включає в себе, наприклад, PSTN та ISDN (цифрова мережа інтегрованих послуг). Щодо мереж та послуг комутації пакетів це включає в себе, наприклад, GPRS, UMTS (Універсальну систему мобільних телекомунікацій), xDSL, TETRA (Транс'європейський стандарт радіозв'язку з автоматичним розподілом каналів), послуги електронної пошти та інші послуги Інтернет-зв'язку. Щодо PLMN, це включає в себе, наприклад, C5M (Глобальну систему для мобільного зв'язку), CDMA, IS41, AMPS, GPRS, UMTS, TETRA. Це також застосовується до S-PCS (персональної супутникової системи зв'язку).

Оперативні запити правоохоронних органів

Загальні спостереження

Міжнародні вимоги до користувача (МВК) були написані у той час, коли в телекомунікаціях переважала комутація каналів. І хоча це й могло вплинути на термінологію МВК, запити правоохоронних органів виражаються в нейтральній термінології.

Доступ до телекомунікацій

[МВК 1] Правоохоронні органи вимагають доступу до всіх переданих телекомунікацій чи тих, що будуть передані, до і від номера чи іншого ідентифікатора цільової служби, який використовується суб'єктом перехоплення. Правоохоронні органи також вимагають надання їм доступу до інформації про зв'язок, яка використовується з метою обробки дзвінка.

«Зв'язок» у цьому контексті означає усі передані телекомунікації чи такі, що будуть передані, до та від об'єкта, що асоціюється із номером чи іншим ідентифікатором, передбаченим в законному документі про санкціонування.

«Номер» чи «ідентифікатор» є засобами, за допомогою яких засоби телекомунікацій визначають особливі зв'язки. Ідентифікатори можуть стосуватись фізичних чи логічних об'єктів (наприклад, адреса користувача, розпізнавальні ознаки обладнання, імені/пароля користувача, розпізнавальні ознаки порту, електронної пошти тощо) та можуть відрізнятись відповідно до виду телекомунікаційних систем.

Типовими, але не виключними прикладами для деяких послуг є: для PLMN – IMSI, MS-ISDN, IMEI; для PSTN/ISDN — абонентські номери, визначення порту, номер замовлення; для Інтернет-пòслуг (доступу) — IP адреси, номер рахунку, логін ID/пароль, PIN-код та електронна адреса.

Правоохоронні органи вимагають постачання переданих та отриманих компонентів перехоплених телекомунікацій у такий спосіб, щоб ці компоненти могли передаватись окремо. (Наприклад, це застосовується в телефонних мережах до звичайного зв'язку між пунктами А і Б, конференц-зв'язку тощо).

Одночасні телекомунікації мають передаватись таким чином, щоб між ними була чітка різниця. (Деякими прикладами телефонних мереж є довідкові дзвінки, одночасні дзвінки, що переадресовуються, тощо).

Правоохоронні органи вимагають представлення будь-яких телекомунікацій, що асоціюються із ідентифікацією суб'єкта перехоплення.

В цьому документі під «інформацією про зв'язок» розуміються дані, що отримуються про зв'язок (див. більш детальні пояснення в пункті 1.4).

[МВК 1.1] Правоохоронні органи вимагають доступу до усіх суб'єктів перехоплення, які постійно чи тимчасово користуються телекомунікаційною системою.

Правоохоронні органи вимагають доступу до телекомунікацій, навіть якщо суб'єкт перехоплення є тимчасовим користувачем мережі чи телекомунікаційних засобів. (*Деякими яскравими прикладами* можуть бути: в PLMN — роумінг; в телефонних системах — UPT та телефонні картки; в Інтернет-послугах — віддалений доступ через *інших постачальників* послуг тощо).

[МВК 1.2] Правоохоронні органи вимагають доступу у випадках, коли суб'єкт перехоплення може використовувати певні особливості з метою спрямувати зв'язок до інших телекомунікаційних послуг чи обладнання, включаючи зв'язок, який до свого завершення проходить через більш ніж одного оператора мережі/постачальника послуг.

Як зазначено вище, «зв'язок» має трактуватись як «телекомунікації». Правоохоронні органи вимагають надання будь-яких телекомунікацій, що пов'язуються із ідентифікацією суб'єкта перехоплення. (Прикладами для телефонних систем є ухилення від зв'язку чи пряме повідомлення у скриньку, де зберігається голосова пошта).

Пункт 3.1 містить вимогу про відслідковування взаємозв'язку. Він може бути достовірним при деяких технологіях, коли інформація про зв'язок подається разом із змістом телекомунікацій. Однак, в іншому випадку, має бути використаний надійний метод прослідковування взаємозв'язку. (Наприклад, посилання на час є неприйнятним, оскільки вони можуть мати подвійне трактування: наприклад, стандартний час, літній час; а також якщо одночасний зв'язок може розвиватись). [МВК 3.2] *Правоохоронні органи вимагають*, щоб формат передачі перехопленого зв'язку до контрольного пункту був загальнодоступним. Цей формат буде узгоджений окремо кожною державою. Пункт 3.2 не потребує роз'яснень.

[МВК 3.4] Правоохоронні органи вимагають від операторів мережі/постачальників послуг передання перехопленого зв'язку на правоохоронний контрольний пункт через стаціонарне чи комутоване з'єднання.

Пункт 3.4 не потребує роз'яснень, але варто відзначити, що термін «постачальник послуг» застосовується до всіх постачальників телекомунікацій. «Комутоване з'єднання» включає в себе як комутацію каналів, так і комутацію пакетів. [МВК 3.5] Правоохоронні органи вимагають відповідності передачі перехопленого зв'язку до контрольного пункту вимогам безпеки.

Пункт 3.5 вимагає, щоб передача перехоплених телекомунікацій здійснювалась таким чином, щоб підтримувалась конфіденційність та цілісність продукту. Продукт може використовуватись як доказ цілей захисту та переслідування; конфіденційність має забезпечуватись як з міркувань права на таємницю, так і з причин розслідування.

[МВК 5.2] Правоохоронні органи вимагають від операторів мережі/постачальників послуг забезпечити передавання перехопленого зв'язку виключно до органу відслідковування, зазначеного в санкції на перехоплення.

Пункт 5.2 не потребує роз'яснень та застосовується до всіх постачальників телекомунікацій.

Безпека засобів перехоплення

[МВК 4] Правоохоронні органи вимагають здійснення перехоплення таким чином, щоб ні об'єкт перехоплення, ні будь-яка інша не уповноважена особа не дізналася про будь-які зміни, внесені з метою виконання розпорядження по перехопленню. Зокрема, діяльність цільової служби для суб'єкта перехоплення повинна залишитись незмінною.

Пункт 4 не потребує роз'яснень, але варто відзначити, що служби телекомунікацій та мереж повинні бути здатні здійснювати перехоплення таємно від інших служб чи мереж.

[МВК 5] Правоохоронні органи вимагають здійснення перехоплення таким чином, щоб перешкодити несанкціонованому чи неналежному використанню та сприяти захисту інформації про перехоплення.

Пункт 5 не потребує роз'яснень, але варто відзначити, що міркування безпеки охоплюють такі аспекти як несанкціонований доступ до безпеки засобів, місця та персоналу.

[МВК 5.3] Відповідно до постанов національного законодавства, оператор мережі/постачальник послуг може/зобов'язаний підтримувати адекватно захищений запис активації перехоплень.

Пункт 5.3 не потребує роз'яснень, але варто відзначити, що той самий рівень безпеки, що застосовується до засобів перехоплення, застосовується і до записів активації. Термін «активація» також охоплює припинення та розширення.

[МВК 5.11 Правоохоронні органи вимагають від операторів мережі/постачальників послуг захисту інформації щодо змісту та обсягу перехоплених телекомунікацій, а також нерозкриття інформації про те, як здійснювалось перехоплення.

Пункт 5.1 не потребує роз'яснення, але варто відзначити, що він застосовується до всіх постачальників телекомунікацій.

Доступ до інформації про суб'єкт перехоплення

[МВК 6] На підставі запиту та перед здійсненням перехоплення правоохоронні органи вимагають:

1) встановлення особи суб'єкта перехоплення, номер служби та інші відмінні ознаки;

2) надання інформації про служби та особливості телекомунікаційних систем, що використовуються суб'єктом перехоплення та постачаються операторами мережі/постачальниками послуг та

3) надання інформації про технічні параметри передачі інформації до контрольного пункту.

Пункти 6 (1) та (2) виражають потребу в інформації, яка буде підтримувати вимоги правоохоронних органів щодо перехоплення. Типова інформація про предмет перехоплення, що вимагається, включає в себе: технічний ідентифікатор; повне ім'я особи (чи компанії), яка є абонентом послуг; постійну адресу абонента (або зареєстровану службову адресу компанії); поштову адресу, на яку надсилаються рахунки; дані про кредитну картку, достатні для ідентифікації рахунку; ім'я в каталозі абонентів, якщо необхідно (варто відзначити, що воно відрізняється від імені абонента); адресу, що вказана в довіднику, якщо необхідно (варто відзначити, що вона може відрізнятись від постійної чи поштової адреси).

Пункт 6 (3) безпосередньо не стосується суб'єкта перехоплення, але є необхідним для загальної підтримки перехоплень.

Інша допомога

[МВК 7] Під час перехоплення правоохоронні органи можуть вимагати надання інформації та/чи допомоги від операторів мереж/постачальників послуг з метою забезпечення того, що зміст зв'язку, отриманий на інтерфейсі перехоплення, є змістом зв'язку, пов'язаного із цільовою службою. Вид інформації та/чи допомоги, що вимагається, буде варіюватися відповідно до прийнятої практики окремих держав.

Пункт 7 не потребує роз'яснень.

[МВК 9] Правоохоронні органи вимагають від операторів мережі/постачальників послуг здійснювати перехоплення якомога оперативніше (в термінових випадках протягом декількох годин чи хвилин). Зворотні вимоги правоохоронних органів будуть варіюватись в кожній окремій країні та за типом цільової служби, що є об'єктом перехоплення.

Пункт 9 виражає потребу у адміністративних засобах та технічних проектах, які дають постачальникам можливість ефективно здійснювати перехоплення.

Доступ до багаторазового та одночасного перехоплення

[МВК 8] Правоохоронні органи вимагають від операторів мережі/постачальників послуг забезпечити здійснення ряду одночасних перехоплень. Багаторазові перехоплення можуть вимагатись по відношенню до однієї цільової служби з метою надання можливості відслідковування більш ніж одному правоохоронному органу. В цьому випадку оператори мережі/постачальники послуг мають вживати заходів попередження з метою захисту ідентичності органів відслідковування та забезпечення конфіденційності розслідувань. Максимальна кількість одночасних перехоплень зв'язку визначеної групи абонентів буде узгоджуватись відповідно до вимог національного законодавства.

Пункт 8 не потребує роз'яснень і застосовується до всіх постачальників телекомунікацій.

Надійність місця перехоплення

[МВК 10] Протягом здійснення перехоплення правоохоронні органи вимагають, щоб надійність служб, які підтримують перехоплення, принаймні

була такою ж, як і надійність цільових служб, що надають послуги суб'єкту перехоплення. Правоохоронні органи вимагають відповідності якості послуг по переданню перехоплень до контрольного пункту стандартам роботи оператора мережі/постачальника послуг.

Пункт 10 не потребує роз'яснень (див. також МВК 2).

Послуги щодо шифрування

[МВК 3.3] У випадку, якщо оператори мережі/постачальники послуг використовують код, скорочення чи шифрування трафіку телекомунікацій, правоохоронні органи вимагають від операторів мережі/постачальників послуг забезпечити представлення перехопленого змісту зв'язку відкритим текстом.

Глосарій

Доступ – технічна здатність працювати із засобами зв'язку, такими, як лінія зв'язку чи комутатор, таким чином, щоб правоохоронний орган міг мати доступ та відслідковувати зв'язок та інформацію про зв'язок, що здійснюється за допомогою засобів.

Автентичність – встановлення дійсності стверджуваної особи користувача, пристрою чи юридичної особи в інформаційній системі чи системі зв'язку.

Уповноважена особа (особи) – особа (особи), уповноважена (уповноважені) здійснювати обов'язки в сфері законного перехоплення інформації.

Доступність – характеристика, за якою система чи служба зв'язку можуть відповідним чином регулярно використовуватися.

Зв'язок – будь-яке з'єднання (стаціонарне чи тимчасове), яким може передаватися інформація між двома чи більше користувачами системи передачі даних.

Примітка: як правило, технологічно нейтральним терміном є «телекомунікації».

Інформація про зв'язок – інформація про передачу даних між пунктом призначення та мережею чи іншим користувачем. Включає в себе інформацію про передачу, що використовується для встановлення зв'язку та контролю за його розвитком (наприклад, утримання запиту, передача запиту). Інформація про зв'язок також включає в себе інформацію, доступну для постачальника послуг/оператора мережі (наприклад, тривалість зв'язку).

Дані (інформація) – представлення інформації відповідним чином для зв'язку, тлумачення, зберігання і обробки.

Перехоплення – в даному випадку законна дія, що передбачає доступ та постачання телекомунікацій, що здійснюються суб'єктом, правоохоронним органам.

Інтерфейс-перехоплення – фізичне місце розташування в межах засобів телекомунікації, що обслуговуються постачальником послуг/оператором мережі, де надається доступ до перехопленої передачі даних. Інтерфейс-перехоплення не обов'язково є чимось єдиним, усталеним.

Розпорядження на перехоплення – розпорядження, що робиться постачальникові послуг мережі/операторові мережі з метою надання ними допомоги правоохоронному органу в сфері законного перехоплення телекомунікацій.

Суб'єкт перехоплення – особа чи особи, визнані законним чином як такі, що їх вхідний та вихідний зв'язок має бути перехопленим та відслідкованим.

Цілісність – властивість, яка передбачає незмінюваність даних чи інформації неналежним чином.

Міжнародні вимоги до користувача – загальний термін, що використовується у Міжнародних вимогах щодо перехоплення телекомунікацій (версія 1.0) та Резолюції Ради від 17 січня 1995 року про законне перехоплення телекомунікацій (опублікованої в Офіційному журналі Європейських Співтовариств С329, 4.11. 1996. - С. 1).

Правоохоронний орган – служба, уповноважена відповідно до закону здійснювати перехоплення передачі даних.

Примітка: це визначення застосовується до функцій правоохоронного органу виключно в межах цього документа.

Контрольний пункт правоохоронних органів – пункт правоохоронних органів, який є пунктом призначення перехопленого зв'язку та інформації про зв'язок певного суб'єкта перехоплення. Місце, де розташоване обладнання для моніторингу/запису.

Законний дозвіл – дозвіл, наданий за певних умов правоохоронному органу для перехоплення визначеної передачі даних. Як правило, це стосується розпорядження, виданого законно уповноваженим на те органом.

Оператор мережі/постачальник послуг – «Оператор мережі» – це оператор інфраструктури телекомунікацій загального користування, що дозволяє передачу сигналів між визначеними пунктами призначення всередині мережі за допомогою телефонного зв'язку, мікрохвиль, оптичних засобів чи інших електромагнітних засобів.

«Постачальник послуг мережі» – це фізична чи юридична особа, що займається наданням послуг у сфері телекомунікацій загального користування, забезпечення яких цілком або частково полягає в передачі сигналів всередині мережі зв'язку.

Якість послуг – визначення якості каналу зв'язку, системи, віртуального каналу, сеансу зв'язку тощо. Якість послуг може вимірюватися, наприклад, рівнем шумів у сигналі, кількістю помилок при передачі, пропускною спроможністю чи можливістю блокувати зв'язок.

Надійність – ймовірність того, що система чи служби будуть задовільно функціонувати протягом певного періоду часу при використанні їх в особливих умовах.

Роумінг – здатність абонентів мобільних служб зв'язку робити та отримувати дзвінки у випадку, якщо вони перебувають поза визначеною територією місця розташування оператора.

Цільова служба – служба, що пов'язана із суб'єктом перехоплення та, як правило, наділена законним правом перехоплення.

Телекомунікації – будь-яка передача знаків, сигналів, записів, образів, звуків, інформації чи свідчень будь-якого характеру, що передаються повністю або частково за допомогою телефонного зв'язку, радіо, електромагнітної, фотоелектронної чи фотооптичної системи.

Переклад здійснено Центром перекладів актів Європейського права при Міністерстві юстиції України.

Європейська Конвенція про кіберзлочинність
(офіційний випуск)

Преамбула

Держави-члени Ради Європи та інші Держави, які підписали цю Конвенцію,

Вважаючи, що метою Ради Європи є досягнення більшої єдності між її членами;

Визнаючи цінність налагодження співробітництва з іншими Державами, які є Сторонами цієї Конвенції;

Впевнені у першочерговій необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва;

Усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, яка продовжується;

Стурбовані ризиком того, що комп'ютерні мережі та електронна інформація може також використовуватися для вчинення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами;

Визнаючи необхідність співробітництва між Державами і приватними підприємствами для боротьби протии кіберзлочинності і необхідність захисту законних інтересів в ході використання і розвитку інформаційних технологій;

Вважаючи, що ефективна боротьба проти кіберзлочинності вимагає більшого, швидкого і ефективно функціонуючого міжнародного співробітництва у кримінальних питаннях;

Впевнені, що ця Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, і надання повноважень, достатніх для

ефективної боротьби з такими кримінальними правопорушеннями, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо надійного міжнародного співробітництва;

Пам'ятаючи про необхідність забезпечити належний баланс між правоохоронними інтересами і повагою до основних прав людини, як це передбачено Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною Хартією ООН про громадянські і політичні права 1966 р. і іншими відповідними міжнародними угодами з прав людини, які підтверджують право кожного безперешкодно дотримуватись поглядів, а також право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, а також права на повагу до приватного життя;

Також пам'ятаючи про захист особистої інформації, як це передбачено Конвенцією Ради Європи про захист осіб по відношенню до автоматичної обробки даних 1981 р.;

Посилаючись на Конвенцію ООН про права дитини 1989 р. і Конвенцію МОП про найгірші форми дитячої праці 1999 р.;

Беручи до уваги існуючі конвенції Ради Європи про співробітництво у кримінальній сфері і подібні угоди, що існують між Державами-членами Ради Європи та іншими Державами, і підкреслюючи, що ця Конвенція має на меті доповнення цих конвенцій для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі;

Вітаючи нещодавні події, які сприяють міжнародному порозумінню і співробітництву у боротьбі з кіберзлочинністю, включаючи заходи ООН, ОЕСР, ЄС і "Великої вісімки;

Посилаючись на Рекомендацію № R (85) 10, що стосується практичного застосування Європейської Конвенції про взаємодопомогу у кримінальних справах по відношенню до листів, які створюють необхідність перехоплення телекомунікацій, Рекомендацію № R (88) 2, про піратство у сфері авторських і суміжних прав, Рекомендацію № R (87) 15, яка регулює використання особистих даних у поліцейській галузі, Рекомендацію № R (95) 4 про захист особистих даних у сфері телекомунікаційних послуг, з особливим посиланням на телефонні послуги, а також на Рекомендацію № R (89) 9 про злочини, пов'язані з комп'ютерами, яка надає орієнтири для національного законодавства щодо визначення певних комп'ютерних злочинів і Рекомендацію № R (95) 13, що стосується проблем кримінально-процесуального права, пов'язаних з інформаційними технологіями;

Посилаючись на Резолюцію № 1, прийняту європейськими міністрами юстиції на своїй 21-й Конференції (Прага, червень 1997 р.), яка рекомендувала Комітету Міністрів підтримати роботу, що проводиться Європейським

комітетом з проблем злочинності (ЄКПЗ) щодо кіберзлочинності для зближення положень внутрішньодержавних положень кримінального права і створення можливостей для застосування ефективних заходів розслідування таких правопорушень, а також на Резолюцію № 3, прийняту на 23-й Конференції європейських міністрів юстиції (Лондон, червень 2000 р.), яка заохочувала сторони переговорів до пошуку відповідних рішень для надання можливості якомога більшій кількості Держав стати учасниками цієї Конвенції, і визнала необхідність швидкодіючої і ефективної системи міжнародного співробітництва, яка б належним чином враховувала специфічні вимоги боротьби проти кіберзлочинності.

Також посилаючись на План дій, прийнятий Головами Держав та Урядів Ради Європи з нагоди їх Другого Самміту (Страсбург, 10-11 жовтня 1997 р.), для пошуку спільних відповідей на розвиток нових інформаційних технологій, які базуються на стандартах і цінностях Ради Європи;

Погодились про таке:

Розділ I — Використання термінів

Стаття 1 — Визначення

Для цілей цієї Конвенції:

a. "комп'ютерна система" означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, у відповідності до певної програми, виконує автоматичну обробку даних;

b. "комп'ютерні дані" означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

c. "постачальник послуг" означає:

I. будь-яку державну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та

II. будь-яка інша установа, яка обробляє або зберігає комп'ютерні дані від імені такої послуги або користувачів такої послуги.

d. "дані про рух інформації" означає будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, яка складала частину ланцюгу комунікації, і які зазначають походження, кінцевий пункт, шлях, час, дату, розмір і тривалість інформації або тип основної послуги.

Розділ II – Заходи, які мають здійснюватися на національному рівні

Частина 1 – Матеріальне кримінальне право

Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Стаття 2 – Незаконний доступ

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб [для встановлення кримінальної відповідальності – прим. пер.] таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 3 – Нелегальне перехоплення

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб [для встановлення кримінальної відповідальності – прим. пер.] таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 4 – Втручання у дані

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це.

2. Сторона може залишити за собою право вимагати, щоб [для встановлення кримінальної відповідальності – прим. пер.] поведінка, описана у пункті 1, завдавала серйозну шкоду.

Стаття 5 – Втручання у систему

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

Стаття 6 – Зловживання пристроями

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисне вчинення, без права на це:

a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином:

1. пристроїв, включаючи комп'ютерні програми, створених або адаптованих для використання, в першу чергу, для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5;

2. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5; та

b. володіння предметом, перерахованим у параграфах (a)(1) або (2) вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів.

2. Ця стаття не тлумачиться як така, що встановлює кримінальну відповідальність у разі, якщо виготовлення, продаж, придбання для використання, розповсюдження чи надання для використання іншим чином або володіння, зазначені у пункті 1 цієї статті, не призначені для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 цієї Конвенції, такі як дозволене випробування або захист комп'ютерної системи.

3. Кожна Сторона може залишити за собою право не застосовувати частину 1 цієї статті, за умови, що таке застереження не стосується продажу, розповсюдження або надання для використання іншим чином предметів, перерахованих у параграфі 1(a)(2).

Правопорушення, пов'язані з комп'ютерами

Стаття 7 – Підробка, пов'язана з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або у відповідності до них проводилися б дії, як з дійсними, незалежно від того, чи можна такі дані прямо прочитати і зрозуміти, чи ні. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності.

Стаття 8 – Шахрайство, пов'язане з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у

відповідності до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних,

b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.

Правопорушення, пов'язані зі змістом [інформації – прим. пер.]

Стаття 9 – Правопорушення, пов'язані з дитячою порнографією

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій:

a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;

b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;

c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;

d. набуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;

e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

2. Для цілей пункту 1 вище "дитяча порнографія" включає в себе порнографічний матеріал, який візуально зображує:

a. неповнолітню особу, задіяну у явно сексуальній поведінці;

b. особу, яка виглядає як неповнолітня особа, задіяну у явно сексуальній поведінці;

c. реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці.

3. Для цілей пункту 2 вище термін "неповнолітня особа" включає в себе усіх осіб до 18 років. Сторона може, однак, передбачити нижчий віковий поріг, який має бути не меншим за 16 років.

4. Кожна Сторона може залишити за собою право не застосовувати, частково чи повністю, параграфи 1(d), 1(e), 2(b) та 2(c).

Правопорушення, пов'язані з порушенням авторських та суміжних прав

Стаття 10 – Правопорушення, пов'язані з порушенням авторських та суміжних прав

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у

відповідності до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони у відповідності до її зобов'язань за Паризьким Актом 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони у відповідності до її зобов'язань за Римською Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

3. Кожна Сторона може залишити за собою право не встановлювати кримінальну відповідальність у відповідності до пунктів 1 і 2 цієї статті у обмежених випадках, за умови існування інших ефективних засобів впливу, і за умови того, що таке застереження не порушує міжнародних зобов'язань Сторони у відповідності до міжнародних документів, на які містяться посилання у пунктах 1 і 2 цієї статті.

Додаткова відповідальність і санкції

Стаття 11 – Спроба і допомога або співучасть

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів, перерахованих у статтях 2-10 цієї Конвенції з метою вчинення такого злочину.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за навмисну спробу вчинити будь-який зі злочинів, перерахованих у статтях 3-5, 7, 8, 9 (1) а та 9 (1) с цієї Конвенції.

3. Кожна Сторона може залишити за собою право не застосовувати, повністю чи частково, пункт 2 цієї Статті.

Стаття 12 – Корпоративна відповідальність

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене у

відповідності до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи.

Така фізична особа має займати керівну посаду в рамках юридичної особи, в силу:

a. повноважень на представлення цієї юридичної особи;

b. повноважень приймати рішення від імені цієї юридичної особи;

c. повноважень здійснювати контроль в рамках цієї юридичної особи.

2. Окрім випадків, вже передбачених у пункті 1, кожна Сторона вживає заходів для забезпечення того, щоб юридична особа могла понести відповідальність у разі, коли недостатній нагляд чи контроль, який мав здійснюватися особою, вказаною у пункті 1, створив можливість вчинення кримінального правопорушення, встановленого у відповідності до цій Конвенції, на користь цієї юридичної особи фізичною особою, яка діяла під її контролем.

3. У відповідності до юридичних принципів Сторони, відповідальність юридичної особи може бути кримінальною, цивільною або адміністративною.

4. Така відповідальність не впливає на кримінальну відповідальність фізичних осіб, які вчинили правопорушення.

Стаття 13 – Санкції і заходи

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб кримінальні правопорушення, встановлені у відповідності до статей 2 – 11, каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі.

2. Кожна Сторона забезпечує, щоб юридичні особи, які несуть відповідальність відповідно до статті 12, каралися ефективними, пропорційними і переконливими кримінальними або некримінальними санкціями, включаючи грошові санкції.

Частина 2 – Процедурне право

Загальні положення

Стаття 14 – Сфера процедурних положень

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань.

2. За винятком обставин, конкретно передбачених статтею 21, кожна Сторона застосовує повноваження і процедури, передбачені у пункті 1, до:

a. кримінальних правопорушень, встановлених відповідно статей 2 – 11 цієї Конвенції;

b. інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем; та

c. збору доказів у електронній формі по кримінальному правопорушенню.

3. a. Кожна Сторона може залишити за собою право застосовувати заходи, які містяться у статті 20, тільки до правопорушень або до категорій правопорушень, зазначених у застереженні, за умови, що обсяг таких правопорушень або категорій правопорушень не менший за обсяг правопорушень, до яких вона застосовує заходи, які містяться у статті 21. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статті 20.

b. Якщо Сторона внаслідок обмежень, встановлених її чинним законодавством під час прийняття цієї Конвенції, не може застосовувати заходи, які містяться у статтях 20 і 21, до комунікацій, які передаються всередині комп'ютерної системи постачальника послуг, причому така система

i. використовується на користь закритої групи користувачів, та

ii. не використовує мережі зв'язку загального доступу, і не пов'язана з іншою комп'ютерною системою, відкритою для загального доступу чи приватною, то така Сторона може залишити за собою право не застосовувати ці заходи до таких комунікацій. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статтях 20 і 21.

Стаття 15 – Умови і запобіжні заходи

1. Кожна Сторона забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, які містяться у цій частині, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини, включаючи права, що випливають з зобов'язань за Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною Хартією ООН про громадянські і політичні права 1966 р. і іншими відповідними міжнародними угодами з прав людини, і які б включали в себе принцип пропорційності.

2. Такі умови і запобіжні заходи включатимуть, між іншим, як це є доречним з огляду на природу відповідного повноваження або процедури, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур.

3. У тій мірі, як це відповідає суспільним інтересам, зокрема, належному відправленню правосуддя, Сторони розглядають вплив повноважень і процедур, які містяться у цій частині, на права, відповідальність і законні інтереси третіх сторін.

Стаття 16 – Термінове збереження комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання можливості своїм компетентним органам видавати накази або іншим подібним шляхом спричиняти термінове збереження зазначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у разі, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації.

2. Якщо Сторона застосовує пункт 1 вище шляхом ордеру особі, яким така особа зобов'язується зберігати зазначені комп'ютерні дані, які зберігаються і знаходяться у власності або під контролем такої особи, то Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати таку особу зберігати і підтримувати цілісність таких комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їхнє розкриття, з максимальним терміном у 90 днів. Сторона може передбачити можливість наступного продовження терміну дії такого ордеру.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати особу, яка має зберігати комп'ютерні дані, зберігати конфіденційність факту проведення таких процедур протягом періоду, визначеного внутрішньодержавним законодавством.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Стаття 17 – Термінове збереження і часткове розкриття даних про рух інформації

1. Кожна Сторона вживає по відношенню до даних про рух інформації, які мають зберігатися відповідно статті 16, такі законодавчі та інші заходи, які можуть бути необхідними для

a. забезпечення того, щоб таке термінове збереження даних про рух інформації могло проводитися, незважаючи на те, один чи більше постачальників послуг було залучено до передачі такої інформації; та

b. забезпечити термінове розкриття компетентному органові Сторони або особі, призначеній таким органом, обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг і шлях, яким була передана інформація.

2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Порядок представлення

Стаття 18 – Порядок представлення

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати накази:

a. особі, яка знаходиться на її території – про надання зазначених комп'ютерних даних, якими така особа володіє або контролює, і які зберігаються у комп'ютерній системі або на комп'ютерному носії інформації; та

b. постачальнику послуг, який пропонує свої послуги на території Сторони – про надання інформації про користувача послуг, пов'язаної з такими послугами, яка знаходиться у власності або під контролем такого постачальника послуг.

2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

3. Для цілей цієї статті "інформація про користувача послуг" означає будь-яку інформацію, у формі комп'ютерних даних чи у іншій формі, яка знаходиться у постачальника послуг, відноситься до користувачів його послуг, і не є даними про рух даних або власне даними змісту інформації [з якою працювали користувачі послуг – прим. перекл.], за допомогою яких можна встановити:

a. тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;

b. особистість користувача послуг, поштову або географічну адресу, телефони та іншу інформацію про номер доступу, рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг;

c. будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про постачання послуг.

Обшук і арешт комп'ютерних даних, які зберігаються

Стаття 19 – Обшук і арешт комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам для обшуку або подібного доступу до:

a. комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній; та

b. комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані, на її території.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб у разі, коли її компетентні органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини відповідно до параграфу 1 (a), і мають підстави вважати, що дані, які розшукуються, зберігаються у іншій комп'ютерній системі чи її частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень арештовувати або вчиняти подібні дії щодо комп'ютерних даних, до яких був здійснений доступ відповідно параграфу 1 або [так у тексті – прим. перекл.] Такі заходи включатимуть повноваження на:

a. арешт або подібні дії щодо комп'ютерної системи або її частини або комп'ютерного носія інформації;

b. копіювання і збереження копії таких комп'ютерних даних;

c. збереження цілісності відповідних збережених комп'ютерних даних; та

d. заборону доступу або вилучення цих комп'ютерних даних з комп'ютерної системи, до якої здійснювався доступ.

4. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень вимагати від будь-якої особи, яка знає про функціонування комп'ютерної системи або про заходи, які були здійснені для захисту комп'ютерних даних, які містяться у ній, надавати відповідну необхідну інформацію для проведення дій, які містяться у параграфах 1 і 2.

5. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Збирання комп'ютерних даних у реальному масштабі часу

Стаття 20 – Збирання даних про рух інформації у реальному масштабі часу

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень:

a. збирати або записувати технічними засобами на території такої Сторони; та

b. зобов'язувати постачальника послуг, в межах його існуючих технічних повноважень:

i. збирати або записувати технічними засобами на території такої Сторони; або

ii. співробітничати і допомагати компетентним органам у зборі або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, яка передається за допомогою комп'ютерних систем.

2. Якщо Сторона, в силу встановлених принципів її юридичної системи, не може застосувати заходи, на які містяться посилання у параграфі 1 (a), вона замість цього може вжити такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення збору або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту і будь-якої інформації про використання будь-якого з повноважень, зазначених у цій статті.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Стаття 21 – Перехоплення даних змісту інформації

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними по відношенню до певних серйозних злочинів, які визначаються внутрішньодержавним законодавством, для надання повноважень своїм компетентним органам:

a. збирати або записувати технічними засобами на території такої Сторони; та

b. зобов'язувати постачальника послуг, в межах його існуючих технічних повноважень:

i. збирати або записувати технічними засобами на території такої Сторони; або

ii. співробітничати і допомагати компетентним органам у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється шляхом комп'ютерної системи.

2. Якщо Сторона, в силу встановлених принципів її юридичної системи, не може застосувати заходи, на які містяться посилання у параграфі 1 (a), вона замість цього може вжити такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення збору або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту і будь-якої інформації про використання будь-якого з повноважень, зазначених у цій статті.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Частина 3 – Юрисдикція

Стаття 22 – Юрисдикція

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, встановленого відповідно статтям 2-11 цієї Конвенції, у випадках, коли таке правопорушення вчинене:

a. на її території; або

b. на борту судна, яке плаває під прапором такої Сторони; або

c. на борту літака, зареєстрованого відповідно законів такої Сторони; або

d. одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

2. Кожна Держава може залишити за собою право не застосовувати або застосовувати лише у окремих випадках або за окремих умов правила юрисдикції, викладені у параграфах 1(b) – 1(d) цієї статті або у будь-якій їх частині.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення юрисдикції стосовно злочинів, встановлених відповідно пункту 1 статті 24 цієї Конвенції, у випадках, коли підозрюваний правопорушник знаходиться на її території і не передається іншій Стороні лише на підставі його громадянства після запиту про екстрадицію.

4. Ця Конвенція не виключає будь-якої кримінальної юрисдикції, здійсненої відповідно внутрішньодержавного законодавства.

5. Якщо більш ніж одна Сторона заявляє про юрисдикцію стосовно підозрюваного правопорушення, встановленого відповідно цієї Конвенції, зацікавлені Сторони, де це можливо, проводять консультації з метою визначення найбільш придатної для переслідування юрисдикції.

Розділ III – Міжнародне співробітництво

Частина 1 – Загальні принципи

Стаття 23 – Загальні принципи міжнародного співробітництва

Сторони співробітничають між собою у найширших обсягах відповідно принципів цього розділу шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються правопорушень.

Принципи екстрадиції

Стаття 24 – Екстрадиція

1. a. Ця стаття застосовується до екстрадиції, що має місце між Сторонами у зв'язку з кримінальними правопорушеннями, встановленими відповідно статтям 2 – 11 цієї Конвенції, за умови, що вони підлягають покаранню позбавленням волі, максимальний строк якого складає щонайменше один рік, або більш суворому покаранню, відповідно законодавству обох зацікавлених Сторін.

b. У випадках, коли відповідно домовленості, укладеної на основі єдиного чи взаємного законодавства, або договору про екстрадицію, включаючи Європейську Конвенцію про екстрадицію (ETS No.24), які застосовуються між двома або більше сторонами, має застосовуватися різне мінімальне покарання, застосовується мінімальне покарання відповідно такій домовленості чи угоді.

2. Кримінальні правопорушення, описані у пункті 1 цієї статті, вважаються такими, що включаються як правопорушення, які спричиняють екстрадицію, до будь-якої угоди про екстрадицію, яка існує між Сторонами. Сторони зобов'язуються включати такі правопорушення, як такі, що спричиняють екстрадицію, до будь-якого договору про екстрадицію, який буде укладено між ними.

3. Якщо Сторона, яка здійснює екстрадицію відповідно існуючого договору, отримує запит про екстрадицію від іншої Сторони, з якої в неї нема договору про екстрадицію, вона може вважати цю Конвенцію юридичною основою для екстрадиції відносно будь-якого кримінального правопорушення, на яке міститься посилання у пункті 1 цієї статті.

4. Сторони, які не здійснюють екстрадицію відповідно існуючого договору, визнають для себе кримінальні правопорушення, на які міститься посилання у пункті 1 цієї статті, такими, що спричиняють екстрадицію.

5. Екстрадиція підлягає умовам, які містяться у законодавстві Сторони, яку запитують про екстрадицію, або у відповідних договорах про екстрадицію, включаючи підстави, на яких Сторона, яку запитують, може відмовити у екстрадиції.

6. Якщо у екстрадиції стосовно кримінального правопорушення, на яке міститься посилання у пункті 1 цієї статті, відмовлено виключно на підставі громадянства особи, стосовно якої надходить запит про екстрадицію або тому, що Сторона, яку запитують, вважає, що вона має юрисдикцію стосовно такого правопорушення, то Сторона, яку запитують, на запит Сторони, яка запитує, надсилає справу своїм компетентним органам з метою переслідування правопорушення, і належним чином повідомляє його результат Стороні, яка запитує. Такі органи приймають свої рішення і проводять свої розслідування і переслідування таким же чином, як і у випадку будь-якого іншого правопорушення подібної природи відповідно законодавства такої Сторони.

7. a. Кожна Сторона під час підписання або передачі документу про ратифікацію, прийняття, затвердження чи приєднання повідомляє Генеральному Секретареві Ради Європи назви і адреси усіх компетентних органів, які відповідають за надсилання чи отримання запитів про екстрадицію або тимчасовий арешт у випадку відсутності договору.

b. Генеральний Секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно призначених Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

Загальні принципи взаємної допомоги

Стаття 25 — Загальні принципи взаємної допомоги

1. Сторони надають одна іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для виконання зобов'язань, що містяться у статтях 27-35.

3. Кожна Сторона за надзвичайних умов може зробити запит про взаємну допомогу або про повідомлення, пов'язані з такою допомогою, які здійснюються терміновими засобами комунікації, включаючи факс і електронну пошту, у тому обсязі, в якому такі засоби комунікацій можуть забезпечити належні форми безпеки і підтвердження достовірності (включаючи використання кодування, де це необхідно), за яким має слідувати формальне підтвердження, якщо таке вимагається Стороною, яку запитують. Сторона, яку запитують, приймає і відповідає на запит шляхом будь-якого з таких термінових засобів комунікації.

4. Якщо інше не передбачене статтями цього розділу, взаємна допомога надається відповідно законодавства Сторони, яку запитують або відповідних договорів про взаємну допомогу, включаючи підстави, на яких Сторона, яку запитують, може відмовити у співробітництві. Сторона, яку запитують, не використовує право відмовити у взаємній допомозі відносно правопорушень, які містяться у статтях 2-11 тільки на підставі того, що запит стосується правопорушення, яке вона вважає фіскальним правопорушенням.

5. Якщо відповідно положенням цього розділу Стороні, яку запитують, дозволяється надавати взаємну допомогу за умови існування подвійного визнання правопорушення, ця умова вважається виконаною, незалежно від того, чи відносить її законодавство таке правопорушення до тієї ж категорії правопорушень або визначає його тією ж термінологією, як і Сторона, яка запитує, у разі, якщо поведінка, яка визначає правопорушення, стосовно якого запитується допомога, є злочином відповідно законодавства Сторони, яку запитують.

Стаття 26 – Добровільно надана інформація

1. Сторона може в рамках свого законодавства без попереднього запиту надіслати іншій Стороні інформацію, отриману в ході її власного розслідування, якщо вона вважає, що розкриття такої інформації може допомогти Стороні, яка отримує інформацію, у відкритті або проведенні розслідування чи переслідування стосовно кримінальних злочинів, встановлених відповідно цієї Конвенції або може спричинити запит про співробітництво від такої Сторони відповідно цього розділу.

2. До надання такої інформації Сторона, яка надає інформацію, може вимагати, щоб вона залишалася конфіденційною або використовувалася за певних умов. Якщо Сторона, яка отримує інформацію, не може задовольнити вимоги такого запиту, вона повідомляє про це Сторону, яка надає інформацію, яка після цього визначає, чи надавати інформацію незважаючи на це. Якщо Сторона, яка отримує інформацію приймає її за певних умов, вона має їх дотримуватися.

Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод

Стаття 27 – Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод

1. У разі відсутності між Стороною, яка запитує, і Стороною, яку запитують, відповідних чинних договорів про взаємну допомогу чи угод на основі єдиного чи взаємного законодавства, застосовуються положення пунктів 2-10 цієї статті.

Положення цієї статті не застосовуються у разі наявності такого договору, угоди або законодавства, якщо тільки зацікавлені Сторони не погоджуються застосовувати замість них, частково або повністю, вищевикладені положення цієї статті.

2. а. Кожна Сторона призначає центральний уповноважений орган або органи, які відповідають за надсилання та відповідь на запити про взаємну

допомогу, виконання таких запитів або їх передачу уповноваженим органам, компетентним виконувати їх.

b. Ці центральні уповноважені органи здійснюють прямі зносини між собою.

c. Кожна Сторона під час підписання або передачі документу про ратифікацію, прийняття, затвердження чи приєднання повідомляє Генеральному Секретареві Ради Європи назви і адреси усіх компетентних органів, призначених відповідно цієї частини.

d. Генеральний Секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно призначених Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

3. Запити про взаємну допомогу відповідно цієї статті здійснюються згідно процедур, зазначених Стороною, яка запитує, якщо тільки вони не суперечать законодавству Сторони, яку запитують.

4. Сторона, яку запитують, може, на додаток до підстав відмови, передбачених у пункті 4 статті 25, відмовити у допомозі, якщо:

a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

b. вона вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

5. Сторона, яку запитують, може відкласти свої дії щодо запиту, якщо такі дії можуть зашкодити кримінальному розслідуванню чи переслідуванню, яке здійснюється її уповноваженими органами.

6. До відмови або відкладення допомоги Сторона, яку запитують, після консультацій з Стороною, яка запитує, розгляне, якщо це доречно, можливість часткового задоволення запиту або його задоволення за умов, які вона вважає доречними.

7. Сторона, яку запитують, терміново інформує Сторону, яка запитує, про висновок розгляду щодо можливості виконання запиту про допомогу. Якщо у допомозі відмовлено чи вона відкладена, то надаються причини відмови чи відкладення. Сторона, яку запитують, також інформує Сторону, яка запитує, про будь-які причини, які унеможливлюють виконання запиту або можуть значною мірою затримати його виконання.

8. Сторона, яка запитує, може запросити Сторону, яку запитують, зберігати конфіденційним факт і зміст будь-якого запиту, зробленого відповідно цього розділу, за винятком того обсягу, який є необхідним для виконання запиту. Якщо Сторона, яку запитують, не може виконати запит за умов його конфіденційності, вона терміново інформує про це Сторону, яка запитує.

Остання визначає, чи необхідно виконати запит, незважаючи на неможливість збереження конфіденційності.

9. a. У термінових випадках *запити про взаємну допомогу* або про повідомлення, пов'язані з нею, могуть надсилатися безпосередньо судовими органами Сторони, яка запитує, до відповідних уповноважених органів Сторони, яку запитують. В будь-якому такому разі копія одночасно надсилається центральному уповноваженому органу Сторони, яку запитують, через центральний уповноважений орган Сторони, яка запитує.

b. Будь-який запит або повідомлення відповідно цього пункту може здійснюватися через Міжнародну організацію кримінальної поліції (Інтерпол).

c. Якщо запит здійснено відповідно підпункту (a), і державний орган не має компетенції розглядати такий запит, то він має передати запит до компетентного державного органу, і безпосередньо повідомити Сторону, яка запитує, про це.

d. Запити або повідомлення відповідно цього пункту, які не включають в себе примусові дії, можуть передаватися безпосередньо компетентними органами Сторони, яка запитує, компетентним органам Сторони, яку запитують.

e. Кожна Сторона під час підписання або передачі документу про ратифікацію, прийняття, затвердження чи приєднання може повідомити Генерального Секретаря Ради Європи про те, що з метою ефективності усі запити відповідно цього пункту мають надсилатися її центральному органу.

Частина 2 – Конкретні принципи
Взаємна допомога щодо тимчасових заходів

Стаття 29 – Термінове збереження комп'ютерних даних, які зберігаються

1. Будь-яка Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

2. Запит про збереження відповідно пункту 1 зазначає:

a. назву компетентного органу, який робить запит про збереження;

b. правопорушення, яке підлягає кримінальному розслідуванню або переслідуванню, і короткий опис відповідних фактів;

c. комп'ютерні дані, які необхідно зберегти, та їх зв'язок з правопорушенням;

d. будь-яку доступну інформацію для ідентифікації особи, яка зберігає такі комп'ютерні дані або розташування комп'ютерної системи;

e. необхідність збереження; та

f. положення про те, що така Сторона має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких комп'ютерних даних, які зберігаються.

3. Після отримання запиту від іншої Сторони, Сторона, яку запитують, вживає усіх належних заходів для термінового збереження зазначених даних відповідно її внутрішньодержавному законодавству. Для цілей відповіді на запит, подвійне визнання правопорушення не вимагається як підстава проведення такого збереження.

4. Сторона, яка вимагає подвійне визнання правопорушення як умову виконання запиту про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних, може відносно правопорушень, які не є правопорушеннями, встановленими статтями 2-11 цієї Конвенції, зберегти за собою право відмовити у виконанні запиту про збереження відповідно цієї статті у випадках, коли вона має підстави вважати, що на час розголошення умову щодо подвійного визнання правопорушення не можна задовольнити.

5. На додаток до цього, у виконанні запиту про збереження можна відмовити лише у випадках, коли:

a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

b. Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

6. Якщо Сторона, яку запитують, вважає, що таке збереження не забезпечить майбутню доступність даних або загрожуватиме їх конфіденційності чи іншим чином зашкодить розслідуванню, яке проводить Сторона, яка запитує, вона терміново інформує про це Сторону, яка запитує. Після цього остання визначає, чи необхідно виконувати запит, незважаючи на це.

7. Будь-яке збереження, проведене у відповідь на запит відповідно пункту 1, проводиться не менше ніж 60 днів, для того, щоб надати можливість Стороні, яка запитує, надіслати запит щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних. Після отримання такого запиту, дані зберігаються до винесення рішення стосовно такого запиту.

Стаття 30 – Термінове розкриття збережених даних про рух інформації

1. Якщо в ході виконання запиту, зробленого відповідно статті 29, щодо збереження даних про рух інформації, які стосуються конкретної передачі інформації, Стороні, яку запитують, стає відомо, що постачальник послуг в іншій Державі був залучений до передачі такої інформації, Сторона, яку запитують, терміново повідомляє Стороні, яка запитує, обсяг інформації про рух даних, достатній для ідентифікації такого постачальника послуг і шляху передачі такої інформації.

2. У розкриття інформації про рух даних відповідно пункту 1 може бути відмовлено тільки якщо:

a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

b. Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

Взаємна допомога щодо повноважень на розслідування

Стаття 31 – Взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються

1. Будь-яка Сторона може запитати іншу Сторону провести обшук чи подібний доступ, арешт чи подібні дії або розголошення даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території Сторони, яку запитують, включаючи дані, збережені відповідно статті 29.

2. Сторона, яку запитують, відповідає на запит шляхом застосування відповідних міжнародних документів, угод і законодавства, на які містяться посилання у статті 23, а також відповідно іншим положенням цього розділу.

3. На запит надається термінова відповідь, якщо:

a. існують підстави вважати, що відповідні дані особливо вразливі для втрати або змін; або

b. міжнародні документи, угоди і законодавство, на які містяться посилання у пункті 2, передбачають термінове співробітництво.

Стаття 32 – Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними

Будь-яка Сторона може, не отримуючи дозвіл іншої Сторони:

a. здійснювати доступ до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або

b. здійснювати доступ або відновлювати шляхом комп'ютерної системи, яка знаходиться на її території, комп'ютерних даних, які зберігаються і знаходяться у іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи.

Стаття 33 – Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу

1. Сторони надають взаємну допомогу одна одній щодо збирання даних про рух інформації у реальному масштабі часу, пов'язаних із зазначеною передачею інформації на їх території, яка передається за допомогою комп'ютерної системи. Відповідно пункту 2, допомога регулюється умовами і процедурами, які передбачені внутрішньодержавним законодавством.

2. Кожна Сторона надає таку допомогу щонайменше відносно кримінальних правопорушень, стосовно яких проводиться збирання даних про рух інформації у реальному масштабі часу у випадку подібної внутрішньодержавної справи.

Стаття 34 – Взаємна допомога у перехопленні даних змісту інформації

Сторони надають взаємну допомогу одна одній щодо перехоплення даних змісту інформації у зазначених передачах інформації, які здійснюються за допомогою комп'ютерної системи, у обсягах, які дозволяються відповідними договорами між ними і внутрішньодержавним законодавством.

Цілодобова мережа

Стаття 35 – Цілодобова мережа

1. Кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме:

a. надання технічних порад;

b. збереження даних відповідно статтям 29 і 30; та

c. збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних.

2. a. Орган Сторони, визначений нею для здійснення контактів, має можливість терміново встановлювати контакт з органом іншої Сторони для здійснення контактів.

b. Якщо орган Сторони, визначений нею для здійснення контактів, не є частиною уповноваженого органу або органів такої Сторони, які відповідають за міжнародну взаємну допомогу або екстрадицію, то орган, визначений для здійснення контактів, забезпечує свою здатність проводити термінову координацію з таким уповноваженим органом або органами.

c. Кожна Сторона забезпечує кваліфікований персонал і відповідне обладнання для сприяння роботі мережі.

Розділ IV – Прикінцеві положення

Стаття 36 – Підписання та набуття чинності

1. Ця Конвенція відкрита для підписання державами-членами Ради Європи та державами, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції.

2. Ця Конвенція підлягає ратифікації, прийняттю або схваленню. Ратифікаційні грамоти або документи про прийняття або схвалення здаються на зберігання Генеральному секретареві Ради Європи.

3. Ця Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати, на яку п'ять держав, серед яких принаймні три держави-члена Ради Європи, висловлять свою згоду на обов'язковість для них цієї Конвенції згідно з положеннями пунктів 1 та 2.

4. Для будь-якої держави, яка підписала Конвенцію та згодом висловлює згоду на її обов'язковість для себе, ця Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати висловлення такою державою згоди на обов'язковість для неї цієї Конвенції згідно з положеннями пунктів 1 та 2.

Стаття 37 – Приєднання до Конвенції

1. Після набуття чинності цією Конвенцією Комітет Міністрів Ради Європи після консультацій з державами, які є Сторонами цієї Конвенції, та висловлення їхньої одностайної згоди може запросити будь-яку державу, яка не є членом Ради Європи та не брала участь у розробці цієї Конвенції, приєднатися до неї. Таке рішення ухвалюється більшістю, передбаченою у статті 20 d) Статуту Ради Європи, та одностайним голосуванням представників Договірних Держав, які мають право брати участь у засіданнях Комітету Міністрів.

2. Для будь-якої держави, яка приєднується до Конвенції відповідно до вищенаведеного пункту 1, Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретареві Ради Європи.

Стаття 38 – Територіальне застосування

1. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може визначити територію або території, до яких застосовуватиметься ця Конвенція.

2. Будь-яка Сторона у будь-який пізніший час шляхом направлення заяви на ім'я Генерального секретаря Ради Європи може поширити дію цієї Конвенції на будь-яку іншу територію, визначену в заяві. Для такої території Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дня одержання заяви Генеральним секретарем.

3. Будь-яка заява, зроблена згідно з двома попередніми пунктами щодо будь-якої території, визначеної у такій заяві, може бути відкликана шляхом направлення повідомлення Генеральному секретареві Ради Європи. Відкликання набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 39 – Цілі Конвенції

1. Мета цієї Конвенції полягає у доповненні застосовних двосторонніх або багатосторонніх договорів або домовленостей між Сторонами, зокрема положень:

- Європейської конвенції про екстрадицію, відкритої для підписання у Парижі 13 грудня 1957 року (ETS №24);

- Європейської конвенції про взаємну допомогу у кримінальних справах, відкриту для підписання у Страсбурзі 20 квітня 1959 року (ETS №30);

- Додаткового протоколу до Європейської конвенції про взаємну допомогу у кримінальних справах, відкритого для підписання у Страсбурзі 17 березня 1978 року (ETS №99).

2. Якщо дві або більше Сторони вже уклали угоду або договір щодо питань, які регулюються цією Конвенцією, або іншим чином встановлюють відносини з таких питань, або якщо вони зроблять це у майбутньому, вони також матимуть право застосовувати таку угоду або договір або відповідно регулювати такі відносини. Однак у разі, якщо Сторони встановлюють свої відносини щодо питань, які регулюються цією Конвенцією, в інший спосіб, ніж передбачається нею, вони роблять це у такий спосіб, що не суперечить цілям та принципам Конвенції.

3. Ніщо в цій Конвенції не зачіпає інших прав, обмежень, зобов'язань та відповідальності Сторони.

Сторона 40 – Заяви

Шляхом направлення письмового повідомлення на ім'я Генерального секретаря Ради Європи будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може заявити, що вона користується можливістю запитати додаткові елементи, передбачені згідно зі статтями 2 та 3, пунктом 1 b) статті 6, статтею 7, пунктом 3 статті 9 та пунктом 9 e) статті 27.

Стаття 41 – Умови щодо федеральних держав

1. Федеральна держава може залишити за собою право брати на себе зобов'язання, передбачені у розділі II цієї Конвенції, відповідно до її основних принципів регулювання відносин між центральними органами влади та державами, що входять до складу федерації, або іншими подібними територіальними одиницями за умови, що вона все-таки спроможна співпрацювати відповідно до розділуIII.

2. Роблячи застереження відповідно до пункту 1, федеральна держава може не застосовувати умови такого застереження для того, щоб виключити або значно зменшити свої зобов'язання щодо передбачення заходів, згаданих у розділіII. Загалом вона забезпечує широкі та ефективні правоохоронні можливості щодо таких заходів.

3. Щодо положень цієї Конвенції, застосування яких входить до юрисдикції держав, що утворюють федерацію, або інших подібних територіальних одиниць, які згідно з конституційною системою федерації не зобов'язані вживати законодавчих заходів, федеральний уряд інформує компетентні органи таких держав про згадані положення, представляючи свою позицію, та заохочує їх до вжиття відповідних заходів для введення в дію таких положень.

Стаття 42 – Застереження

Шляхом направлення письмового повідомлення на ім'я Генерального секретаря Ради Європи будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може заявити, що вона користується застережен-

ням/застереженнями, передбаченими у пункті 2 статті 4, пункті 3 статті 6, пункті 4 статті 9, пункті 3 статті 10, пункту 3 статті 11, пункту 3 статті 14, пункту 2 статті 22, пункті 4 статті 29 та пункті 1 статті 41. Не може бути зроблено жодних інших застережень.

Стаття 43 – Статус та відкликання застережень

1. Будь-яка Сторона, яка зробила застереження відповідно до статті 42, може повністю або частково відкликати його, направивши повідомлення на ім'я Генерального секретаря. Таке відкликання набуває чинності в день отримання такого повідомлення Генеральним секретарем. Якщо у повідомленні зазначається, що відкликання застереження має набути чинності у визначений у повідомленні день та така дата є пізнішою, ніж дата отримання повідомлення Генеральним секретарем, відкликання набуває чинності у такий пізніший день.

2. Сторона, яка зробила застереження, згадане у статті 42, відкликає таке застереження повністю або частково, як тільки це дозволяють обставини.

3. Генеральний секретар Ради Європи може періодично запитувати Сторони, які зробили одне або декілька застережень, згаданих у статті 42, про можливості відкликання такого застереження/ таких застережень.

Стаття 44 – Зміни та доповнення

1. Зміни та доповнення до цієї Конвенції можуть пропонуватися будь-якою Стороною. Вони направляються Генеральним секретарем Ради Європи державам-членам Ради Європи, а також державам, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, та всім державам, які приєдналися або були запрошені приєднатися до цієї Конвенції згідно з положеннями статті 37.

2. Будь-які зміни або доповнення, запропоновані Сторонами, передаються до Європейського комітету з проблем злочинності (ЄКПЗ), який надає Комітетові Міністрів свою думку щодо таких запропонованих змін або доповнень.

3. Комітет Міністрів розглядає запропоновану зміну або доповнення та думку, представлену Європейським комітетом з проблем злочинності (ЄКПЗ) та після консультацій з з державами, які не є членами Ради Європи, але є Сторонами цієї

Конвенції, може прийняти зміну або доповнення.

4. Текст будь-якої зміни або доповнення, прийнятого Комітетом Міністрів згідно з пунктом 3 цієї статті, направляється Сторонам для прийняття.

5. Будь-які зміни та доповнення, прийняті відповідно до пункту 3 цієї статті набувають чинності після того, як всі Сторони повідомлять Генерального секретаря про їх прийняття.

Стаття 45 – Вирішення спорів

1. Європейський комітет з проблем злочинності (ЄКПЗ) інформується про тлумачення та застосування цієї Конвенції.

2. У разі спору між Сторонами щодо тлумачення або застосування цієї Конвенції вони намагаються вирішити спір шляхом переговорів або будь-

яких інших мирних засобів на свій вибір, включаючи подання спору до Європейського комітету з проблем злочинності (ЄКПЗ), до арбітражного суду, рішення якого є обов'язковим для виконання Сторонами, або до Міжнародного суду, за домовленістю заінтересованих Сторін.

Стаття 46 – Консультації Сторін

1. Сторони у разі необхідності регулярно консультуються з метою сприяння:

a) ефективному використанню та застосуванню цієї Конвенції, включаючи виявлення будь-яких її проблематичних питань, а також наслідків будь-якої заяви або застереження, зробленого згідно з цією Конвенцією;

b) обміну інформацією про суттєві зміни права, політики або технології, що стосуються кіберзлочинності, та збору інформації в електронній формі;

c) розгляду можливих додатків до цієї Конвенції.

2. Європейський комітет з проблем злочинності (ЄКПЗ) регулярно інформується про результати консультацій, згаданих у пункті 1.

3. Європейський комітет з проблем злочинності (ЄКПЗ) у разі необхідності сприяє проведенню консультацій, згаданих у пункті 1, та вживає необхідних заходів для надання допомоги Сторонам у їхніх зусиллях щодо внесення змін або доповнень до Конвенції. Щонайпізніше через три роки після набуття чинності цією Конвенцією Європейський комітет з проблем злочинності (ЄКПЗ) у співпраці зі Сторонами проводить перегляд всіх положень Конвенції та, у разі необхідності, пропонує відповідні зміни та доповнення.

4. Витрати, пов'язані з виконанням положень пункту 1, сплачуються Сторонами у визначений ними спосіб, крім випадків, коли такі витрати сплачуються Радою Європи.

5. Секретаріат Ради Європи допомагає Сторонам у виконанні ними їхніх функцій за цією статтею.

Стаття 47 – Денонсація

1. Будь-яка Сторона може в будь-який час денонсувати цю Конвенцію шляхом направлення письмового повідомлення Генеральному секретареві Ради Європи.

2. Така денонсація набуває чинності в перший день місяця, який наступає після завершення тримісячного періоду від дня отримання повідомлення Генеральним секретарем.

Стаття 48 – Повідомлення

Генеральний секретар Ради Європи повідомляє держави-члени Ради Європи та держави, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, а також всі держави, які приєдналися або були запрошені приєднатися до цієї Конвенції, про:

a) будь-яке підписання;

b) здачу на зберігання будь-якої ратифікаційної грамоти або документа про прийняття, схвалення або приєднання;

c) будь-яку дату набуття чинності цією Конвенцією відповідно до статей 36 і 37;

d) будь-яку заяву, зроблену відповідно до статей 40 та 41, або застереження, зроблене відповідно до статті 42;

e) будь-який інший акт, повідомлення або інформацію, що стосується цієї Конвенції.

На посвідчення чого нижчепідписані належним чином на це уповноважені підписали цю Конвенцію.

СОГЛАШЕНИЕ
о взаимном обеспечении сохранности межгосударственных секретов в области правовой охраны изобретений *

Принято 4 июня 1999 г.

Государства-участники настоящего Соглашения в лице правительств, далее – Стороны, основываясь на Соглашении о взаимном обеспечении сохранности межгосударственных секретов от 22 января 1993 года и Соглашении о мерах по охране промышленной собственности и создании Межгосударственного совета по вопросам охраны промышленной собственности от 12 марта 1993 года, исходя из необходимости правовой охраны секретных изобретений, созданных в бывшем Союзе ССР, учитывая взаимные интересы Сторон в обеспечении их государственной безопасности, согласились о нижеследующем:

Статья 1

Для целей настоящего Соглашения следующие термины означают:

секретные изобретения – изобретения, в которых содержатся сведения, составляющие в соответствии с национальным законодательством Сторон государственную тайну (межгосударственные секреты);

рассекречивание секретных изобретений – процедура снятия грифа секретности с документов, имеющих отношение к секретным изобретениям;

охранный документ на секретное изобретение – документ, который в соответствии с национальным законодательством Сторон обеспечивает правовую охрану секретного изобретения;

заявители – проживающие или находящиеся на территориях Сторон авторы, а также предприятия, учреждения, организации, подавшие заявки на выдачу авторского свидетельства или патента СССР на секретное изобретение;

заинтересованная Сторона – Сторона, на территории которой находятся заявители;

компетентные органы – государственные органы, определяемые Сторонами для выполнения настоящего Соглашения.

* Інформаційне законодавство: Збірник законодавчих актів: У 6 т. / За заг. ред. Ю. С. Шемшученка, І. С. Чижа. – Т 6. Міжнародні угоди України в інформаційній сфері. – К.: ТОВ «Видавництво «Юридична думка», 2005. — 160с., С.150-154

Статья 2

Стороны обеспечивают режим секретности в отношении имеющихся у них сведений о секретных изобретениях в соответствии с Соглашением о взаимном обеспечении сохранности межгосударственных секретов от 22 января 1993 года.

Статья 3

Стороны обязуются при рассекречивании секретных изобретений, на которые выданы авторские свидетельства СССР или поданы заявки на их выдачу, руководствоваться Правилами рассекречивания секретных изобретений, на которые выданы авторские свидетельства СССР или поданы заявки на выдачу авторских свидетельств или патентов СССР (Приложение 1), являющимися неотъемлемой частью настоящего Соглашения. Для рассмотрения представлений Сторон о необходимости рассекречивания секретных изобретений и принятия по ним решений, предусмотренных указанными Правилами, Стороны создают Временную рабочую группу (далее — ВРГ), организационно-техническое обеспечение которой возлагается на Российское агентство по патентным и товарным знакам (далее — Роспатент).

Статья 4

Стороны признают право заявителей ходатайствовать о выдаче охранных документов на секретные изобретения по заявкам на выдачу авторского свидетельства или патента СССР на секретные изобретения, делопроизводство по которым не завершено в СССР и по которым не истекли сроки действия охранного документа на секретное изобретение, в порядке, предусмотренном Правилами подачи ходатайств о выдаче охранных документов на секретные изобретения по заявкам на выдачу авторского свидетельства или патента СССР на секретные изобретения, делопроизводство по которым не завершено в СССР (Приложение 2), являющимися неотъемлемой частью настоящего Соглашения, если иное не предусмотрено национальным законодательством.

Статья 5

Действие на территории любой из Сторон авторского свидетельства СССР на секретное изобретение по ходатайству заявителей, подаваемому в порядке, установленном национальным законодательством, может быть прекращено, при этом одновременно производится выдача охранного документа на секретное изобретение на оставшийся срок действия авторского свидетельства, если иное не предусмотрено национальным законодательством.

Статья 6

Спорные вопросы, связанные с применением или толкованием настоящего Соглашения, разрешаются путем консультаций и переговоров между компетентными органами заинтересованных Сторон.

Статья 7

В настоящее Соглашение могут быть внесены с общего согласия Сторон изменения и дополнения в виде отдельных протоколов, которые вступают в силу в порядке, предусмотренном статьей 10 настоящего Соглашения.

Статья 8

Каждая Сторона может выйти из настоящего Соглашения, направив письменное уведомление об этом депозитарию не позднее, чем за 6 месяцев до выхода.

Статья 9

Настоящее Соглашение действует в течение 5-ти лет со дня его вступления в силу. По истечении этого срока настоящее Соглашение автоматически продлевается на последующие 5-летние периоды, если Стороны не примут иного решения.

Статья 10

Настоящее Соглашение вступает в силу со дня сдачи на хранение депозитарию третьего уведомления о выполнении подписавшими его Сторонами необходимых внутригосударственных процедур. Для Сторон, выполнивших необходимые процедуры позднее, оно вступает в силу со дня сдачи соответствующих документов депозитарию.

Статья 11

Настоящее Соглашение открыто для присоединения к нему государств-участников СНГ, разделяющих его цели и принципы, путем передачи депозитарию документов о таком присоединении.

Приложение 1

к Соглашению о взаимном обеспечении сохранности межгосударственных секретов в области правовой охраны изобретений

Правила рассекречивания секретных изобретений, на которые выданы авторские свидетельства СССР или поданы заявки на выдачу авторских свидетельств или патентов СССР

1. Настоящие Правила предусматривают порядок рассекречивания секретных изобретений, на которые выданы авторские свидетельства СССР или поданы заявки на выдачу авторских свидетельств или патентов СССР в соответствии с патентным законодательством СССР.

2. Рассмотрение возможности рассекречивания секретных изобретений, на которые выданы авторские свидетельства СССР, может быть осуществлено по инициативе любой Стороны.

3. Решение о необходимости рассекречивания секретного изобретения принимается заинтересованной Стороной в порядке, предусмотренном ее национальным законодательством, регулирующим рассекречивание сведений, относящихся к государственным секретам.

4. Представление о необходимости рассекречивания секретного изобретения направляется заинтересованной Стороной на заключение каждой из Сторон в ВРГ. Представление о рассекречивании должно быть мотивированным, содержать номера авторского свидетельства и заявки, по которой оно выдано, фамилию (фамилии) автора (авторов), его (их) местожительство на дату подачи заявки, наименование организации-заявителя, ее месторасположение и формулу изобретения.

5. ВРГ направляет представление о рассекречивании секретного изобретения в адрес компетентного органа каждой из Сторон. Заключение на представление о рассекречивании секретного изобретения направляется каждой Стороной в ВРГ в течение 4-х месяцев с даты направления ВРГ этого представления. В необходимых случаях заключение может быть направлено Стороной в более поздний срок, но не позднее 2-х месяцев со дня истечения указанного 4-месячного срока. В этом случае Сторона должна в течение указанного 4-месячного срока уведомить ВРГ о том, что заключение будет направлено позже. Если заключение не будет направлено Стороной в ВРГ в указанный 4- или 6-месячный срок с предварительным уведомлением, как это предусмотрено выше, признается, что эта Сторона согласна с представлением о рассекречивании сведений.

6. ВРГ рассматривает представление о рассекречивании с учетом мнений заинтересованных Сторон и принимает решение о возможности рассекречивания секретного изобретения.

О принятом решении ВРГ сообщает каждой из Сторон в течение одного месяца с даты поступления последнего заключения путем направления каждой Стороне копий всех полученных заключений. Решение о рассекречивании секретного изобретения считается принятым только в случае подтверждения каждой из Сторон возможности рассекречивания этого изобретения. В этом случае заинтересованная Сторона организует работы по рассекречиванию секретного изобретения в порядке, предусмотренном национальным законодательством, и в месячный срок сообщает ВРГ о результатах рассекречивания этого изобретения.

В случае несогласия с рассекречиванием секретного изобретения заключение должно содержать конкретные мотивы, по которым Сторона считает невозможным рассекречивание секретного изобретения. Возникшие разногласия разрешаются компетентными органами заинтересованных Сторон.

7. В случае принятия решения о рассекречивании секретного изобретения сведения о нем могут быть опубликованы или переданы третьим странам только заинтересованными Сторонами.

8. Рассекречивание секретных изобретений, на которые поданы заявки, но не выданы по ним авторские свидетельства или патенты СССР, может быть осуществлено по инициативе любой из заинтересованных Сторон в порядке, предусмотренном пунктами 3, 4, 5 и 6 настоящих Правил. При этом согласование рассекречивания указанных изобретений осуществляется только между этими Сторонами, для чего ВРГ направляет представление о рассекречивании секретного изобретения в компетентные органы Российской Федерации, на территории которой находится поданная заявка, и заинтересованной Стороны (Сторон). В этих случаях в представлении о необходимости рассекречивания секретного изобретения наряду со сведениями, предусмотренными пунктом 4 настоящих Правил, вместо номеров авторского свидетельства и заявки, по которой оно выдано, указывается номер заявки.

9. Рассекречивание сведений о секретных изобретениях с грифом «Совершенно секретно», на которые выданы авторские свидетельства СССР на основании решений министерств и ведомств СССР и сведения, о которых распространялись в СССР в специальных отраслевых и межотраслевых изданиях, осуществляется в порядке, предусмотренном пунктами 2, 3, 4, 5 и 6 настоящих Правил.

10. Рассекречивание сведений о секретных изобретениях с грифом «Совершенно секретно», на которые выданы авторские свидетельства СССР на основании решений министерств и ведомств СССР и сведения, о которых не распространялись в СССР в специальных отраслевых и межотраслевых изданиях, осуществляется в порядке, предусмотренном пунктом 8 настоящих Правил.

Приложение 2
к Соглашению о взаимном обеспечении сохранности межгосударственных секретов
в области правовой охраны изобретений

Правила подачи ходатайств

о выдаче охранных документов на секретные изобретения по заявкам на выдачу авторского свидетельства или патента СССР на секретные изобретения, делопроизводство по которым не завершено в СССР

1. Настоящие Правила устанавливают порядок подачи ходатайств о выдаче предусмотренных национальным законодательством охранных документов на секретные изобретения по заявкам на выдачу авторского свидетельства или патента СССР на секретные изобретения, делопроизводство по которым не завершено в СССР.

2. По заявкам, указанным в пункте 1 настоящих Правил, по ходатайству заявителей совместно с авторами Сторонами могут быть выданы предусмотренные их законодательством охранные документы на секретные изобретения с сохранением приоритета по ранее поданной в СССР заявке на секретное изобретение.

3. Ходатайство подается в компетентный орган Стороны, на территории которой испрашивается выдача охранного документа. Делопроизводство ведется в соответствии с законодательством Сторон.

К ходатайству прилагается документ о разрешении Стороны ее физическим и/или юридическим лицам на получение правовой охраны на секретное изобретение на территории другой Стороны. По просьбе компетентного органа Стороны, в который подано ходатайство, Роспатент представляет этому компетентному органу заверенную копию материалов заявки на выдачу авторского свидетельства или патента СССР на секретное изобретение. В случае если договоренность между заявителями о совместной подаче ходатайства не достигнута, выдача охранного документа не производится.

УТВЕРЖДЕНА
Указом Президента
Российской Федерации
от 17 декабря 1997 г. № 1300
(в редакции Указа Президента
Российской Федерации
от 10 января 2000 г. № 24)

Концепция национальной безопасности Российской Федерации

Концепция национальной безопасности Российской Федерации (далее именуется - Концепция) - система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности. В Концепции сформулированы важнейшие направления государственной политики Российской Федерации.

Под национальной безопасностью Российской Федерации понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации.

I. Россия в мировом сообществе

Положение в мире характеризуется динамичной трансформацией системы международных отношений. После окончания эры биполярной конфронтации возобладали две взаимоисключающие тенденции.

Первая тенденция проявляется в укреплении экономических и политических позиций значительного числа государств и их интеграционных объединений, в совершенствовании механизмов многостороннего управления международными процессами. При этом все большую роль играют экономические, политические, научно-технические, экологические и информационные факторы. Россия будет способствовать формированию идеологии становления многополярного мира на этой основе.

Вторая тенденция проявляется через попытки создания структуры международных отношений, основанной на доминировании в международном сообществе развитых западных стран при лидерстве США и рассчитанной на односторонние, прежде всего военно-силовые, решения ключевых проблем мировой политики в обход основополагающих норм международного права.

Формирование международных отношений сопровождается конкуренцией, а также стремлением ряда государств усилить свое влияние на мировую политику, в том числе путем создания оружия массового уничтожения. Значение военно-силовых аспектов в международных отношениях продолжает оставаться существенным.

Россия является одной из крупнейших стран мира с многовековой историей и богатыми культурными традициями. Несмотря на сложную международную обстановку и трудности внутреннего характера, она в силу значитель-

ного экономического, научно-технического и военного потенциала, уникального стратегического положения на Евразийском континенте объективно продолжает играть важную роль в мировых процессах.

В перспективе - более широкая интеграция Российской Федерации в мировую экономику, расширение сотрудничества с международными экономическими и финансовыми институтами. Объективно сохраняется общность интересов России и интересов других государств по многим проблемам международной безопасности, включая противодействие распространению оружия массового уничтожения, предотвращение и урегулирование региональных конфликтов, борьбу с международным терроризмом и наркобизнесом, решение острых экологических проблем глобального характера, в том числе проблемы обеспечения ядерной и радиационной безопасности.

Вместе с тем активизируются усилия ряда государств, направленные на ослабление позиций России в политической, экономической, военной и других областях. Попытки игнорировать интересы России при решении крупных проблем международных отношений, включая конфликтные ситуации, способны подорвать международную безопасность и стабильность, затормозить происходящие позитивные изменения в международных отношениях.

Во многих странах, в том числе в Российской Федерации, резко обострилась проблема терроризма, имеющего транснациональный характер и угрожающего стабильности в мире, что обусловливает необходимость объединения усилий всего международного сообщества, повышения эффективности имеющихся форм и методов борьбы с этой угрозой, принятия безотлагательных мер по ее нейтрализации.

II. Национальные интересы России

Национальные интересы России - это совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах. Они носят долгосрочный характер и определяют основные цели, стратегические и текущие задачи внутренней и внешней политики государства. Национальные интересы обеспечиваются институтами государственной власти, осуществляющими свои функции в том числе во взаимодействии с действующими на основе Конституции Российской Федерации и законодательства Российской Федерации общественными организациями.

Интересы личности состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина.

Интересы общества состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

Реализация национальных интересов России возможна только на основе устойчивого развития экономики. Поэтому национальные интересы России в этой сфере являются ключевыми.

Во внутриполитической сфере национальные интересы России состоят в сохранении стабильности конституционного строя, институтов государственной власти, в обеспечении гражданского мира и национального согласия, территориальной целостности, единства правового пространства, правопорядка и в завершении процесса становления демократического общества, а также в нейтрализации причин и условий, способствующих возникновению политического и религиозного экстремизма, этносепаратизма и их последствий — социальных, межэтнических и религиозных конфликтов, терроризма.

Национальные интересы России в социальной сфере заключаются в обеспечении высокого уровня жизни народа.

Национальные интересы в духовной сфере состоят в сохранении и укреплении нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Национальные интересы России в международной сфере заключаются в обеспечении суверенитета, упрочении позиций России как великой державы — одного из влиятельных центров многополярного мира, в развитии равноправных и взаимовыгодных отношений со всеми странами и интеграционными объединениями, прежде всего с государствами — участниками Содружества Независимых Государств и традиционными партнерами России, в повсеместном соблюдении прав и свобод человека и недопустимости применения при этом двойных стандартов.

Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Национальные интересы России в военной сфере заключаются в защите ее независимости, суверенитета, государственной и территориальной целостности, в предотвращении военной агрессии против России и ее союзников, в обеспечении условий для мирного, демократического развития государства.

Национальные интересы России в пограничной сфере заключаются в создании политических, правовых, организационных и других условий для обеспечения надежной охраны государственной границы Российской Федерации, в соблюдении установленных законодательством Российской Федера-

ции порядка и правил осуществления экономической и иных видов деятельности в пограничном пространстве Российской Федерации.

Национальные интересы России в экологической сфере заключаются в сохранении и оздоровлении окружающей среды.

Важнейшими составляющими национальных интересов России являются защита личности, общества и государства от терроризма, в том числе международного, а также от чрезвычайных ситуаций природного и техногенного характера и их последствий, а в военное время — от опасностей, возникающих при ведении военных действий или вследствие этих действий.

III. Угрозы национальной безопасности Российской Федерации

Состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, социально-политическая поляризация российского общества и криминализация общественных отношений, рост организованной преступности и увеличение масштабов терроризма, обострение межнациональных и осложнение международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности страны.

В сфере экономики угрозы имеют комплексный характер и обусловлены прежде всего существенным сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках — продовольствия и предметов потребления, включая предметы первой необходимости.

Ослабление научно-технического и технологического потенциала страны, сокращение исследований на стратегически важных направлениях научно-технического развития, отток за рубеж специалистов и интеллектуальной собственности угрожают России утратой передовых позиций в мире, деградацией наукоемких производств, усилением внешней технологической зависимости и подрывом обороноспособности России.

Негативные процессы в экономике лежат в основе сепаратистских устремлений ряда субъектов Российской Федерации. Это ведет к усилению политической нестабильности, ослаблению единого экономического пространства России и его важнейших составляющих — производственно-технологических и транспортных связей, финансово-банковской, кредитной и налоговой систем.

Экономическая дезинтеграция, социальная дифференциация общества, девальвация духовных ценностей способствуют усилению напряженности во взаимоотношениях регионов и центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу Российской Федерации.

Этноэгоизм, этноцентризм и шовинизм, проявляющиеся в деятельности ряда общественных объединений, а также неконтролируемая миграция

способствуют усилению национализма, политического и религиозного экстремизма, этносепаратизма и создают условия для возникновения конфликтов.

Единое правовое пространство страны размывается вследствие несоблюдения принципа приоритета норм Конституции Российской Федерации над иными правовыми нормами, федеральных правовых норм над нормами субъектов Российской Федерации, недостаточной отлаженности государственного управления на различных уровнях.

Угроза криминализации общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности, приобретает особую остроту. Серьезные просчеты, допущенные на начальном этапе проведения реформ в экономической, военной, правоохранительной и иных областях государственной деятельности, ослабление системы государственного регулирования и контроля, несовершенство правовой базы и отсутствие сильной государственной политики в социальной сфере, снижение духовно-нравственного потенциала общества являются основными факторами, способствующими росту преступности, особенно ее организованных форм, а также коррупции.

Последствия этих просчетов проявляются в ослаблении правового контроля за ситуацией в стране, в сращивании отдельных элементов исполнительной и законодательной власти с криминальными структурами, проникновении их в сферу управления банковским бизнесом, крупными производствами, торговыми организациями и товаропроводящими сетями. В связи с этим борьба с организованной преступностью и коррупцией имеет не только правовой, но и политический характер.

Масштабы терроризма и организованной преступности возрастают вследствие зачастую сопровождающегося конфликтами изменения форм собственности, обострения борьбы за власть на основе групповых и этнонационалистических интересов. Отсутствие эффективной системы социальной профилактики правонарушений, недостаточная правовая и материально-техническая обеспеченность деятельности по предупреждению терроризма и организованной преступности, правовой нигилизм, отток из органов обеспечения правопорядка квалифицированных кадров увеличивают степень воздействия этой угрозы на личность, общество и государство.

Угрозу национальной безопасности России в социальной сфере создают глубокое расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, увеличение удельного веса населения, живущего за чертой бедности, рост безработицы.

Угрозой физическому здоровью нации являются кризис систем здравоохранения и социальной защиты населения, рост потребления алкоголя и наркотических веществ.

Последствиями глубокого социального кризиса являются резкое сокращение рождаемости и средней продолжительности жизни в стране, деформа-

ция демографического и социального состава общества, подрыв трудовых ресурсов как основы развития производства, ослабление фундаментальной ячейки общества — семьи, снижение духовного, нравственного и творческого потенциала населения.

Углубление кризиса во внутриполитической, социальной и духовной сферах может привести к утрате демократических завоеваний.

Основные угрозы в международной сфере обусловлены следующими факторами:

- стремление отдельных государств и межгосударственных объединений принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН и ОБСЕ;
- опасность ослабления политического, экономического и военного влияния России в мире;
- укрепление военно-политических блоков и союзов, прежде всего расширение НАТО на восток;
- возможность появления в непосредственной близости от российских границ иностранных военных баз и крупных воинских контингентов;
- распространение оружия массового уничтожения и средств его доставки;
- ослабление интеграционных процессов в Содружестве Независимых Государств;
- возникновение и эскалация конфликтов вблизи государственной границы Российской Федерации и внешних границ государств — участников Содружества Независимых Государств;
- притязания на территорию Российской Федерации.

Угрозы национальной безопасности Российской Федерации в международной сфере проявляются в попытках других государств противодействовать укреплению России как одного из центров влияния в многополярном мире, помешать реализации национальных интересов и ослабить ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.

Серьезную угрозу национальной безопасности Российской Федерации представляет терроризм. Международным терроризмом развязана открытая кампания в целях дестабилизации ситуации в России.

Усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Возрастают уровень и масштабы угроз в военной сфере.

Возведенный в ранг стратегической доктрины переход НАТО к практике силовых (военных) действий вне зоны ответственности блока и без санкции Совета Безопасности ООН чреват угрозой дестабилизации всей стратегической обстановки в мире.

Увеличивающийся технологический отрыв ряда ведущих держав и наращивание их возможностей по созданию вооружений и военной техники нового поколения создают предпосылки качественно нового этапа гонки вооружений, коренного изменения форм и способов ведения военных действий.

Активизируется деятельность на территории Российской Федерации иностранных специальных служб и используемых ими организаций.

Усилению негативных тенденций в военной сфере способствуют затянувшийся процесс реформирования военной организации и оборонного промышленного комплекса Российской Федерации, недостаточное финансирование национальной обороны и несовершенство нормативной правовой базы. На современном этапе это проявляется в критически низком уровне оперативной и боевой подготовки Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, в недопустимом снижении *укомплектованности войск (сил)* современным вооружением, военной и специальной техникой, в крайней остроте социальных проблем и приводит к ослаблению военной безопасности Российской Федерации в целом.

Угрозы национальной безопасности и интересам Российской Федерации в пограничной сфере обусловлены:

- экономической, демографической и культурно-религиозной экспансией сопредельных государств на российскую территорию;
- активизацией деятельности трансграничной организованной преступности, а также зарубежных террористических организаций.

Угроза ухудшения экологической ситуации в стране и истощения ее природных ресурсов находится в прямой зависимости от состояния экономики и готовности общества осознать глобальность и важность этих проблем. Для России эта угроза особенно велика из-за преимущественного развития топливно-энергетических отраслей промышленности, неразвитости законодательной основы природоохранной деятельности, отсутствия или ограниченного использования природосберегающих технологий, низкой экологической культуры. Имеет место тенденция к использованию территории России в качестве места переработки и *захоронения опасных для окружающей среды материалов и веществ.*

В этих условиях ослабление государственного надзора, недостаточная эффективность правовых и экономических механизмов предупреждения и ликвидации чрезвычайных ситуаций увеличивают риск катастроф техногенного характера во всех сферах хозяйственной деятельности.

IV. Обеспечение национальной безопасности Российской Федерации

Основными задачами в области обеспечения национальной безопасности Российской Федерации являются:

своевременное прогнозирование и выявление внешних и внутренних угроз национальной безопасности Российской Федерации;

реализация оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз;

обеспечение суверенитета и территориальной целостности Российской Федерации, безопасности ее пограничного пространства;

подъем экономики страны, проведение независимого и социально ориентированного экономического курса;

преодоление научно-технической и технологической зависимости Российской Федерации от внешних источников;

обеспечение на территории России личной безопасности человека и гражданина, его конституционных прав и свобод;

совершенствование системы государственной власти Российской Федерации, федеративных отношений, местного самоуправления и законодательства Российской Федерации, формирование гармоничных межнациональных отношений, укрепление правопорядка и сохранение социально-политической стабильности общества;

обеспечение неукоснительного соблюдения законодательства Российской Федерации всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями;

обеспечение равноправного и взаимовыгодного сотрудничества России прежде всего с ведущими государствами мира;

подъем и поддержание на достаточно высоком уровне военного потенциала государства;

укрепление режима нераспространения оружия массового уничтожения и средств его доставки;

принятие эффективных мер по выявлению, предупреждению и пресечению разведывательной и подрывной деятельности иностранных государств, направленной против Российской Федерации;

коренное улучшение экологической ситуации в стране.

Обеспечение национальной безопасности и защита интересов России в экономической сфере являются приоритетными направлениями политики государства.

Важнейшими задачами во внешнеэкономической деятельности являются:

создание благоприятных условий для международной интеграции российской экономики;

расширение рынков сбыта российской продукции;

формирование единого экономического пространства с государствами – участниками Содружества Независимых Государств.

В условиях либерализации внешней торговли России и обострения конкуренции на мировом рынке товаров и услуг необходимо усилить защиту интересов отечественных товаропроизводителей.

Важнейшее значение приобретает проведение сбалансированной кредитно-финансовой политики, нацеленной на поэтапное сокращение зависимости России от внешних кредитных заимствований и укрепление ее позиций в международных финансово-экономических организациях.Необходимо усилить роль государства в регулировании деятельности иностранных банковских, страховых и инвестиционных компаний, ввести определенные и обоснованные ограничения на передачу в эксплуатацию зарубежным компаниям месторождений стратегических природных ресурсов, телекоммуникаций, транспортных и товаропроводящих сетей.

Эффективные меры должны быть приняты в сфере валютного регулирования и контроля в целях создания условий для прекращения расчетов в иностранной валюте на внутреннем рынке и предотвращения бесконтрольного вывоза капитала.

Основными направлениями обеспечения национальной безопасности Российской Федерации во внутриэкономической деятельности государства являются:

правовое обеспечение реформ и создание эффективного механизма контроля за соблюдением законодательства Российской Федерации;

усиление государственного регулирования в экономике;

принятие необходимых мер по преодолению последствий экономического кризиса, сохранению и развитию научно-технического, технологического и производственного потенциала, переходу к экономическому росту при снижении вероятности техногенных катастроф, повышению конкурентоспособности отечественной промышленной продукции, подъему благосостояния народа.

Переход к высокоэффективной и социально ориентированной рыночной экономике должен осуществляться путем постепенного формирования оптимальных механизмов организации производства и распределения товаров и услуг в целях максимально возможного роста благосостояния общества и каждого гражданина.

На первый план выдвигаются задачи, связанные с устранением деформаций в структуре российской экономики, с обеспечением опережающего роста производства наукоемкой продукции и продукции высокой степени переработки, с поддержкой отраслей, составляющих основу расширенного воспроизводства, с обеспечением занятости населения.

Существенное значение имеют усиление государственной поддержки инвестиционной и инновационной активности, принятие мер по созданию устойчивой банковской системы, отвечающей интересам реальной экономики, облегчение доступа предприятий к долгосрочным кредитам на финансирование капитальных вложений, оказание реальной государственной поддержки целевых программ структурной перестройки промышленности.

Важнейшие задачи – опережающее развитие конкурентоспособных отраслей и производств, расширение рынка наукоемкой продукции. В целях

их решения должны быть приняты меры, стимулирующие передачу новых военных технологий в гражданское производство, введен механизм выявления и развития прогрессивных технологий, освоение которых обеспечит конкурентоспособность российских предприятий на мировом рынке.

Решение указанных задач предполагает концентрацию финансовых и материальных ресурсов на приоритетных направлениях развития науки и техники, оказание поддержки ведущим научным школам, ускоренное формирование научно-технического задела и национальной технологической базы, привлечение частного капитала, в том числе путем создания фондов и использования грантов, реализацию программ развития территорий, обладающих высоким научно-техническим потенциалом, создание при поддержке государства инфраструктуры, обеспечивающей коммерциализацию результатов научно-исследовательских разработок с одновременной защитой интеллектуальной собственности внутри страны и за рубежом, развитие общедоступной сети научно-технической и коммерческой информации.

Государство должно содействовать созданию равных условий для развития и увеличения конкурентоспособности предприятий независимо от формы собственности, в том числе становлению и развитию частного предпринимательства во всех сферах, где это способствует росту общественного благосостояния, прогрессу науки и образования, духовному и нравственному развитию общества, защите прав потребителей.

В кратчайшие сроки должны быть разработаны механизмы поддержания жизнедеятельности и экономического развития особо кризисных регионов и районов Крайнего Севера, а также тарифная политика, обеспечивающая единство экономического пространства страны.

Приоритет экономических факторов в социальной сфере принципиально важен для укрепления государства, для реального государственного обеспечения социальных гарантий, для развития механизмов коллективной ответственности и демократического принятия решений, социального партнерства. При этом важно проведение социально справедливой и экономически эффективной политики в области распределения доходов.

Организация работы федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации по реализации конкретных мер, направленных на предотвращение и преодоление угроз национальным интересам России в области экономики, также требует дальнейшего совершенствования законодательства Российской Федерации в указанной области и обеспечения строгого его соблюдения всеми хозяйствующими субъектами.

Сближение интересов населяющих страну народов, налаживание их всестороннего сотрудничества, проведение ответственной и взвешенной государственной национальной и региональной политики позволит обеспечить в России внутриполитическую стабильность. Комплексный подход к решению этих задач должен составлять основу внутренней государственной политики,

обеспечивающей развитие Российской Федерации как многонационального демократического федеративного государства.

Укрепление российской государственности, совершенствование федеративных отношений и местного самоуправления должны способствовать обеспечению национальной безопасности Российской Федерации. Необходим комплексный подход к решению правовых, экономических, социальных и этнополитических проблем при сбалансированном соблюдении интересов Российской Федерации и ее субъектов.

Осуществление конституционного принципа народовластия требует обеспечения согласованного функционирования и взаимодействия всех органов государственной власти, жесткой вертикали исполнительной власти и единства судебной системы России. Это обеспечивается конституционным принципом разделения властей, установлением более четкого функционального распределения полномочий между государственными институтами, укреплением федеративного устройства России путем совершенствования ее отношений с субъектами Российской Федерации в рамках их конституционного статуса.

Основными направлениями защиты конституционного строя в России являются:

обеспечение приоритета федерального законодательства и совершенствование на этой основе законодательства субъектов Российской Федерации;

разработка организационных и правовых механизмов защиты государственной целостности, обеспечение единства правового пространства и национальных интересов России;

выработка и реализация региональной политики, обеспечивающей оптимальный баланс федеральных и региональных интересов;

совершенствование механизма, препятствующего созданию политических партий и общественных объединений, преследующих сепаратистские и антиконституционные цели, и пресечение их деятельности.

Требуется консолидация усилий, направленных на борьбу с преступностью и коррупцией. Россия крайне заинтересована в искоренении экономической и социально-политической основы этих общественно опасных явлений, выработке комплексной системы мер для эффективной защиты личности, общества и государства от преступных посягательств.

Приоритетное значение имеет формирование системы мер действенной социальной профилактики и воспитания законопослушных граждан. Эти меры должны быть направлены на защиту прав и свобод, нравственности, здоровья и собственности каждого человека независимо от расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также от других обстоятельств.

Важнейшими задачами в области борьбы с преступностью являются:

выявление, устранение и предупреждение причин и условий, порождающих преступность;

усиление роли государства как гаранта безопасности личности и общества, создание необходимой для этого правовой базы и механизма ее применения;

укрепление системы правоохранительных органов, прежде всего структур, противодействующих организованной преступности и терроризму, создание условий для их эффективной деятельности;

привлечение государственных органов в пределах их компетенции к деятельности по предупреждению противоправных деяний;

расширение взаимовыгодного международного сотрудничества в правоохранительной сфере, в первую очередь с государствами — участниками Содружества Независимых Государств.

Решения и меры, принимаемые органами государственной власти в области борьбы с преступностью, должны быть открытыми, конкретными и понятными каждому гражданину, носить упреждающий характер, обеспечивать равенство всех перед законом и неотвратимость ответственности, опираться на поддержку общества.

Для профилактики преступности и борьбы с нею в первую очередь необходимо развитие правовой базы как основы надежной защиты прав и законных интересов граждан, а также соблюдение международно-правовых обязательств Российской Федерации в сфере борьбы с преступностью и соблюдения прав человека. Важно лишить преступность питательной среды, обусловленной недостатками в законодательстве, кризисом в экономике и социальной сфере.

В целях предупреждения коррупции и устранения условий для легализации капиталов, нажитых незаконным путем, необходимо создать действенную систему финансового контроля, усовершенствовать меры административного, гражданского и уголовно-правового воздействия, отработать механизм проверки имущественного положения и источников доходов должностных лиц и служащих организаций и учреждений независимо от формы собственности, а также соответствия их расходов этим доходам.

Борьба с терроризмом, наркобизнесом и контрабандой должна осуществляться на основе общегосударственного комплекса контрмер по пресечению этих видов преступной деятельности.

Основываясь на международных соглашениях, необходимо эффективно сотрудничать с иностранными государствами, их правоохранительными органами и специальными службами, а также международными организациями, в задачу которых входит борьба с терроризмом. Необходимо также шире использовать международный опыт борьбы с этим явлением, создать скоординированный механизм противодействия международному терроризму, надежно перекрыть все возможные каналы незаконного оборота оружия и взрывчатых веществ внутри страны, а также их поступления из-за рубежа.

Федеральные органы государственной власти должны преследовать на территории страны лиц, причастных к террористической деятельности, независимо от того, где планировались и осуществлялись террористические ак-

ции, наносящие ущерб Российской Федерации.

Обеспечение национальной безопасности Российской Федерации включает в себя также защиту культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, сохранение культурного достояния всех народов России, формирование государственной политики в области духовного и нравственного воспитания населения, введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие, эксплуатирующих низменные проявления, а также включает в себя противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Духовное обновление общества невозможно без сохранения роли русского языка как фактора духовного единения народов многонациональной России и языка межгосударственного общения народов государств — участников Содружества Независимых Государств.

В целях обеспечения сохранности и развития нашего культурного и духовного наследия необходимо создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры.

В области охраны и укрепления здоровья граждан необходимы усиление внимания общества, органов государственной власти Российской Федерации к развитию государственной (федеральной и муниципальной) страховой и частной медицинской помощи, осуществление государственного протекционизма в отечественной медицинской и фармацевтической промышленности, реализация федеральных программ в области санитарии и эпидемиологии, охраны здоровья детей, оказания скорой и неотложной медицинской помощи, медицины катастроф.

К числу приоритетных направлений деятельности государства в экологической сфере относятся:

рациональное использование природных ресурсов, воспитание экологической культуры населения;

предотвращение загрязнения природной среды за счет повышения степени безопасности технологий, связанных с захоронением и утилизацией токсичных промышленных и бытовых отходов; предотвращение радиоактивного загрязнения окружающей среды, минимизация последствий произошедших ранее радиационных аварий и катастроф;

экологически безопасное хранение и утилизация выведенного из боевого состава вооружения, прежде всего атомных подводных лодок, кораблей и судов с ядерными энергетическими установками, ядерных боеприпасов, жидкого ракетного топлива, топлива атомных электростанций;

безопасное для окружающей природной среды и здоровья населения хранение и уничтожение запасов химического оружия;

создание и внедрение безопасных производств, поиск способов практического использования экологически чистых источников энергии, принятие

неотложных природоохранных мер в экологически опасных регионах Российской Федерации.

Необходимы новый подход к организации и ведению гражданской обороны на территории Российской Федерации, качественное совершенствование единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, в том числе дальнейшая интеграция ее с аналогичными системами иностранных государств.

Внешняя политика Российской Федерации должна быть направлена на:

проведение активного внешнеполитического курса;

упрочение ключевых механизмов многостороннего управления мировыми политическими и экономическими процессами, в первую очередь под эгидой Совета Безопасности ООН;

обеспечение благоприятных условий для экономического и социального развития страны, для сохранения глобальной и региональной стабильности;

защиту законных прав и интересов российских граждан за рубежом, в том числе с применением в этих целях мер политического, экономического и иного характера;

развитие отношений с государствами – участниками Содружества Независимых Государств согласно принципам международного права, развитие отвечающих интересам России интеграционных процессов в рамках Содружества Независимых Государств;

полноправное участие России в глобальных и региональных экономических и политических структурах;

содействие урегулированию конфликтов, включая миротворческую деятельность под эгидой ООН и других международных организаций;

достижение прогресса в сфере контроля над ядерными вооружениями, поддержание стратегической стабильности в мире на основе выполнения государствами своих международных обязательств в этой сфере;

выполнение взаимных обязательств в области сокращения и ликвидации оружия массового уничтожения, обычных вооружений, осуществление мер по укреплению доверия и стабильности, обеспечение международного контроля за экспортом товаров и технологий, а также за оказанием услуг военного и двойного назначения;

адаптацию существующих соглашений по контролю над вооружениями и по разоружению к новым условиям международных отношений, а также разработку при необходимости новых соглашений, в первую очередь по мерам укрепления доверия и безопасности;

содействие созданию зон, свободных от оружия массового уничтожения;

развитие международного сотрудничества в области борьбы с транснациональной преступностью и терроризмом.

Обеспечение военной безопасности Российской Федерации является важнейшим направлением деятельности государства. Главной целью в данной области является обеспечение возможности адекватного реагирования на уг-

розы, которые могут возникнуть в XXI веке, при рациональных затратах на национальную оборону.

В предотвращении войн и вооруженных конфликтов Российская Федерация отдает предпочтение политическим, дипломатическим, экономическим и другим невоенным средствам. Однако национальные интересы Российской Федерации требуют наличия достаточной для ее обороны военной мощи. Вооруженные Силы Российской Федерации играют главную роль в обеспечении военной безопасности Российской Федерации.

Важнейшей задачей Российской Федерации является осуществление сдерживания в интересах предотвращения агрессии любого масштаба, в том числе с применением ядерного оружия, против России и ее союзников.

Российская Федерация должна обладать ядерными силами, способными гарантированно обеспечить нанесение заданного ущерба любому государству-агрессору или коалиции государств в любых условиях обстановки.

Вооруженные Силы Российской Федерации боевым составом мирного времени должны быть способны обеспечить надежную защиту страны от воздушного нападения и решение совместно с другими войсками, воинскими формированиями и органами задач по отражению агрессии в локальной войне (вооруженном конфликте), а также стратегическое развертывание для решения задач в крупномасштабной войне. Вооруженные Силы Российской Федерации должны обеспечивать осуществление Российской Федерацией миротворческой деятельности.

Одним из важнейших стратегических направлений в области обеспечения военной безопасности Российской Федерации является эффективное взаимодействие и сотрудничество с государствами — участниками Содружества Независимых Государств.

Интересы обеспечения национальной безопасности Российской Федерации предопределяют при соответствующих обстоятельствах необходимость военного присутствия России в некоторых стратегически важных регионах мира. Размещение в них на договорной и международно-правовой основе, а также на принципах партнерства ограниченных воинских контингентов (военных баз, сил Военно-Морского Флота) должно обеспечивать готовность России выполнять свои обязательства, содействовать формированию устойчивого военно-стратегического баланса сил в регионах и давать возможность Российской Федерации реагировать на кризисную ситуацию в ее начальной стадии, способствовать реализации внешнеполитических целей государства.

Российская Федерация рассматривает возможность применения военной силы для обеспечения своей национальной безопасности, исходя из следующих принципов:

применение всех имеющихся в ее распоряжении сил и средств, включая ядерное оружие, в случае необходимости отражения вооруженной агрессии, если все другие меры разрешения кризисной ситуации исчерпаны или оказались неэффективными;

применение военной силы внутри страны допускается в строгом соответствии с Конституцией Российской Федерации и федеральными законами в случаях возникновения угрозы жизни граждан, территориальной целостности страны, а также угрозы насильственного изменения конституционного строя.

Важная роль в обеспечении национальных интересов России принадлежит оборонному промышленному комплексу. Реструктуризация и конверсия оборонного промышленного комплекса должна осуществляться без ущерба для развития новых технологий и научно-технических возможностей, модернизации вооружений, военной и специальной техники и укрепления позиций российских производителей на мировом рынке вооружений.

Требуется создать все необходимые условия для организации приоритетных фундаментальных, прогнозных и поисковых научных исследований, обеспечивающих создание в интересах обороны и безопасности государства перспективного и опережающего научно-технического задела.

Основными задачами Российской Федерации в пограничной сфере являются:

создание необходимой нормативной правовой базы;

развитие межгосударственного сотрудничества в этой области;

противодействие экономической, демографической и культурно-религиозной экспансии на территорию России со стороны других государств;

пресечение деятельности транснациональной организованной преступности, а также незаконной миграции;

осуществление коллективных мер по обеспечению безопасности пограничного пространства государств – участников Содружества Независимых Государств.

Важнейшими задачами обеспечения информационной безопасности Российской Федерации являются:

реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;

совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

противодействие угрозе развязывания противоборства в информационной сфере.

Особое значение для обеспечения национальной безопасности Российской Федерации имеет эффективное использование и всестороннее развитие возможностей разведки и контрразведки в целях своевременного обнаружения угроз и определения их источников.

Система обеспечения национальной безопасности Российской Федерации создается и развивается в соответствии с Конституцией Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, федеральными программами в этой области.

Основу системы обеспечения национальной безопасности Российской Федерации составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства.

Полномочия органов и сил обеспечения национальной безопасности Российской Федерации, их состав, принципы и порядок действий определяются соответствующими законодательными актами Российской Федерации.

В формировании и реализации политики обеспечения национальной безопасности Российской Федерации принимают участие:

Президент Российской Федерации – руководит в пределах своих конституционных полномочий органами и силами обеспечения национальной безопасности Российской Федерации; санкционирует действия по обеспечению национальной безопасности; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы обеспечения национальной безопасности; выступает с посланиями, обращениями и директивами по проблемам национальной безопасности, в своих ежегодных посланиях Федеральному Собранию уточняет отдельные положения Концепции национальной безопасности Российской Федерации, определяет направления текущей внутренней и внешней политики страны;

Федеральное Собрание Российской Федерации – на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формирует законодательную базу в области обеспечения национальной безопасности Российской Федерации;

Правительство Российской Федерации – в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетов в области обеспечения национальной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти, а также органов исполнительной власти субъектов Российской Федерации, формирует в установленном порядке статьи федерального бюджета для реализации конкретных целевых программ в этой области;

Совет Безопасности Российской Федерации – проводит работу по упреждающему выявлению и оценке угроз национальной безопасности Российской Федерации, оперативно готовит для Президента Российской Федерации проекты решений по их предотвращению, разрабатывает предложения в области обеспечения национальной безопасности Российской Федерации, а также предложения по уточнению отдельных положений Концепции национальной безопасности Российской Федерации, координирует деятельность сил и органов обеспечения национальной безопасности, контро-

лирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений в этой области;

федеральные органы исполнительной власти – обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области национальной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их Президенту Российской Федерации и Правительству Российской Федерации;

органы исполнительной власти субъектов Российской Федерации – взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области национальной безопасности Российской Федерации, а также федеральных программ, планов и директив, издаваемых Верховным Главнокомандующим Вооруженными Силами Российской Федерации, в области военной безопасности Российской Федерации; совместно с органами местного самоуправления проводят мероприятия по привлечению граждан, общественных объединений и организаций к оказанию содействия в решении проблем национальной безопасности согласно законодательству Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения национальной безопасности Российской Федерации.

***

Российская Федерация намерена решительно и твердо обеспечивать свою национальную безопасность. Созданные правовые демократические институты, сложившаяся структура органов государственной власти Российской Федерации, широкое участие политических партий и общественных объединений в реализации Концепции национальной безопасности Российской Федерации – залог динамичного развития России в XXI веке.

Президент
Российской Федерации
В.Путин
9 сентября 2000 г.

УТВЕРЖДАЮ

Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина служит основой для:

формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

I. Информационная безопасность Российской Федерации

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной

целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;

усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

гарантировать свободу массовой информации и запрет цензуры;

не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение го-

сударственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;

обеспечить защиту сведений, составляющих государственную тайну;

расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- ✓ угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- ✓ угрозы информационному обеспечению государственной политики Российской Федерации;
- ✓ угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- ✓ угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- ✓ принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- ✓ создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- ✓ противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- ✓ нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- ✓ противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- ✓ неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- ✓ неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- ✓ дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- ✓ нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- ✓ вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- ✓ девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- ✓ снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- ✓ манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- ✓ монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- ✓ блокирование деятельности государственных средств массовой инфор-

мации по информированию российской и зарубежной аудитории;

- ✓ низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- ✓ противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- ✓ закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- ✓ вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- ✓ увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- ✓ противоправные сбор и использование информации;
- ✓ нарушения технологии обработки информации;
- ✓ внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- ✓ разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- ✓ уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- ✓ воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- ✓ компрометация ключей и средств криптографической защиты информации;
- ✓ утечка информации по техническим каналам;

- ✓ внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- ✓ уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- ✓ перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- ✓ использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- ✓ несанкционированный доступ к информации, находящейся в банках и базах данных;
- ✓ нарушение законных ограничений на распространение информации.

3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

- ✓ деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- ✓ стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- ✓ обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- ✓ деятельность международных террористических организаций;
- ✓ увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- ✓ деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- ✓ разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- ✓ критическое состояние отечественных отраслей промышленности;

- ✓ неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- ✓ недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- ✓ недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- ✓ неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- ✓ недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- ✓ недостаточная экономическая мощь государства;
- ✓ снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- ✓ недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- ✓ отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созданию

механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов. Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- ✓ разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- ✓ развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государст-

венную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;

- ✓ разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- ✓ разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- ✓ совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- ✓ установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- ✓ координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;
- ✓ развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения "информационного оружия";
- ✓ разработка и создание механизмов формирования и реализации государственной информационной политики России;
- ✓ разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;
- ✓ обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- ✓ разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

- ✓ развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- ✓ создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- ✓ расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- ✓ обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- ✓ создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

II. Методы обеспечения информационной безопасности Российской Федерации

5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

- ✓ внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;
- ✓ законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и

механизмов участия в этой деятельности общественных объединений, организаций и граждан;

- ✓ разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- ✓ уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- ✓ законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- ✓ определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- ✓ создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуника-

ционных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;

формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

В сфере экономики. Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

система государственной статистики;

кредитно-финансовая система;

информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной

информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

В сфере внутренней политики. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

конституционные права и свободы человека и гражданина;

конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики. К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

распространение за рубежом дезинформации о внешней политике Российской Федерации;

нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:

разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;

разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и

социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

научно-технические кадры и система их подготовки;

системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);

политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств — участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;

неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;

серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;

сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники — это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

В сфере духовной жизни. Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;

свобода массовой информации;

неприкосновенность частной жизни, личная и семейная тайна;

русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств-участников Содружества Независимых Государств;

языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;

объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

развитие в России основ гражданского общества;

создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;

совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;

формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;

разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных

объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;

введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах. Основными объектами обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

лицензирование деятельности организаций в области защиты информации;

аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны. К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются:

все виды разведывательной деятельности зарубежных государств;

информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;

преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

ненадежное функционирование информационных и телекоммуникационных систем специального назначения;

возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;

нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;

нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны являются:

систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;

проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;

постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;

совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;

подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

В правоохранительной и судебной сферах. К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;

отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

создание защищенной многоуровневой системы интегрированных банков данных оперативно-разыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;

повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций. Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в ус-

ловиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс;

к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;

совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;

повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;

прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;

разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности – неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно

осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания "информационного оружия". Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

запрещение разработки, распространения и применения "информационного оружия";

обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами — участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

III. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;

организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;

поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

формулирует и реализует государственную информационную политику России;

организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;

способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации.

Это предполагает:

оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

создание организационно-правовых механизмов обеспечения информационной безопасности;

определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;

создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;

разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправ-

ных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;

совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концеп-

ции правового обеспечения информационной безопасности Российской Федерации;

разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;

принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;

гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации

10. Основные функции системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;

создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;

организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;

проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;

организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;

защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законо-

дательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации. Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения

по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Реализация первоочередных мероприятий по обеспечению информационной безопасности Российской Федерации, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом Российской Федерации.

КОНЦЕПЦІЯ (ОСНОВИ ДЕРЖАВНОЇ ПОЛІТИКИ) ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Проект УЦЕПД

ВСТУП

Предметом цієї Концепції є інформаційна безпека як важлива складова національної безпеки України.

Концепція (основи державної політики) інформаційної безпеки України (далі — Концепція) розроблена з метою розвитку положень Концепції (основ державної політики) національної безпеки України і є основою для: формування та реалізації державної інформаційної політики; підготовки пропозицій щодо вдосконалення правового, організаційного, фінансового, науково-технічного та іншого забезпечення інформаційної безпеки України; розробки цільових програм розвитку інформаційної сфери України, захисту її від внутрішніх і зовнішніх загроз.

Концепція визначає: національні інтереси України в інформаційній сфері; основні загрози національним інтересам; основні внутрішні та зовнішні чинники ескалації загроз; пріоритетні напрями державної політики забезпечення інформаційної безпеки України та першочергові заходи щодо їх реалізації.

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Основні визначення

Національні інтереси України в інформаційній сфері — це суспільно визнані та законодавчо закріплені життєво важливі інформаційні потреби особи, суспільства, держави, задоволення яких забезпечує стабільне існування, вільний, всебічний розвиток особи та суспільства, ефективне функціонування держави.

Інформаційна безпека — стан захищеності національних інтересів України в інформаційній сфері, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через: неповноту, несвоєчасність, недостовірність інформації; несанкціоноване поширення та використання інформації; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій.

Об'єкт інформаційної безпеки. *Соціальними об'єктами* інформаційної безпеки є: особа — її права та свободи в інформаційній сфері; суспільство — його духовні цінності, засади солідарної діяльності; держава — її конституційний лад, суверенітет, ефективне функціонування. *Технічними об'єктами* інформаційної безпеки є інформаційні ресурси, інформаційна інфраструктура, інформаційні технології.

Загроза інформаційній безпеці — явище, дія негативних чинників або процес, через які: соціальні об'єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері; порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об'єктів інформаційної безпеки.

Система забезпечення інформаційної безпеки України — організована державою сукупність суб'єктів (державних органів, посадових осіб, громадських організацій, окремих громадян), об'єднаних цілями та завданнями захисту національних інтересів України в інформаційній сфері, які здійснюють узгоджену діяльність у межах законодавства України.

Інформаційний простір України — середовище, в якому здійснюються продукування, зберігання та поширення інформації, і на яке розповсюджується юрисдикція України.

Інформаційна інфраструктура — сукупність систем, що забезпечують: продукування, накопичення, зберігання та поширення інформаційної продукції; виробництво засобів виробництва інформаційної продукції та їх поширення; виробництво інформаційних технологій; сервісне обслуговування елементів інфраструктури; підготовку кадрів.

1.2. Основні принципи забезпечення інформаційної безпеки України

Основними принципами забезпечення інформаційної безпеки України є:

- пріоритет прав людини;
- верховенство права;

- пріоритет договірних (мирних) засобів у вирішенні інформаційних конфліктів;
- адекватність заходів захисту національних інтересів України в інформаційній сфері реальним та потенційним загрозам;
- громадський контроль за діяльністю органів державної влади, що входять до системи забезпечення інформаційної безпеки України;
- додержання балансу інтересів особи, суспільства, держави, їх взаємна відповідальність;
- чітке розмежування повноважень та функцій органів державної влади в системі забезпечення інформаційної безпеки України.

РОЗДІЛ 2. НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Національні інтереси України в інформаційній сфері відображають фундаментальні цінності та прагнення Українського народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення та способи задоволення.

Національні інтереси України в інформаційній сфері та їх пріоритетність зумовлюються конкретною ситуацією, що складається в країні та за її межами.

Національними інтересами України в інформаційній сфері є:

- забезпечення конституційних прав і свобод громадян в інформаційній сфері: свободи слова; права на отримання інформації та користування нею; права на приватну таємницю, таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень; захищеності конфіденційної інформації (персональних даних); права на інтелектуальну власність;
- формування відкритого й безпечного інформаційного простору, що сприяє розвитку громадянського суспільства через: забезпечення доступності інформації, незалежності ЗМІ; посилення контролю представницьких органів за діяльністю державних ЗМІ; розвиток інформаційної інфраструктури; розробку та впровадження новітніх інформаційних технологій; постійне поповнення та надійний захист національного інформаційного ресурсу; недопущення монополізму в усіх ланках продукування, накопичення, зберігання та поширення інформації; запобігання розповсюдження інформації, що провокує політичну або соціальну нетерпимість, міжетнічні або міжконфесійні конфлікти, сепаратизм; обмеження негативного інформаційного впливу на суспільну свідомість і психіку громадян;
- захист інформаційного простору України від негативного зовнішнього впливу через: забезпечення захищеності вітчизняних інформаційних систем (*насамперед, інформаційно-аналітичних систем органів державної* влади та місцевого самоврядування, автоматизованих систем уп-

равління військових формувань) від несанкціонованого доступу; недопущення витоку таємної, конфіденційної та іншої інформації з обмеженим доступом; протидію інформаційній експансії з боку інших держав; подолання технічної та технологічної залежності вітчизняної інформаційної інфраструктури від зарубіжних виробників;

- якісне інформаційно-аналітичне забезпечення діяльності органів державної влади та місцевого самоврядування через: забезпечення відкритості органів державної влади (в т.ч. силових структур), громадського контролю за їх діяльністю; активне залучення інтелектуального потенціалу наукових установ, неурядових аналітичних центрів, громадських організацій; автоматизацію процесів збору, аналізу та використання інформації; створення системи інформаційних мереж, сполучених баз даних центральних і місцевих органів державної влади та місцевого самоврядування; впровадження систем електронного документообігу; створення мережі ситуаційних центрів для оперативного інформаційно-аналітичного забезпечення керівництва держави в надзвичайних (нештатних) ситуаціях;
- перетворення виробництва інформаційної продукції та послуг на потужний чинник економічного зростання України через: забезпечення пріоритетного розвитку вітчизняного виробництва інформаційних технологій та комп'ютерних систем; усунення монополізму та інших перешкод становленню ринкових відносин в інформаційній сфері; державну підтримку, в т.ч. пільгове оподаткування суб'єктів господарювання, які виробляють та/або впроваджують новітні інформаційні технології; зосередження зусиль на загальній комп'ютеризації; підвищення комп'ютерної грамотності населення; збільшення обсягів та підвищення рівня підготовки фахівців у цій галузі, створення гідних умов для їх працевлаштування в Україні;
- інтеграція України до світового інформаційного простору через: гармонізацію законодавства України в інформаційній сфері з нормами міжнародного права; адаптацію вітчизняної системи стандартів до світових аналогів; підвищення конкурентоспроможності вітчизняних ЗМІ, поширення їх діяльності на зарубіжні країни; створення іномовних інформаційних ресурсів про економічний, науковий, освітній, культурний, туристичний потенціал України; модернізацію систем зв'язку; інтенсивний розвиток вітчизняного сегменту мережі Інтернет;
- збереження власної культурної ідентичності за умов посилення процесів глобалізації через: розвиток внутрішніх джерел поповнення інформаційних ресурсів (освіти, науки, культури); захист від інформаційно-культурної експансії з боку інших держав; накопичення україномовних інформаційних ресурсів; забезпечення користувачів комп'ютерної техніки мовно адаптованими програмними продуктами.

РОЗДІЛ 3. ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Основні загрози інформаційній безпеці України, чинники та можливі негативні наслідки їх ескалації наводяться в таблиці "Загрози інформаційній безпеці України".

Система забезпечення інформаційної безпеки України здійснює постійний моніторинг та прогнозування загроз, уточнення їх переліку та пріоритетності, відповідно до нових умов.

РОЗДІЛ 4. СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Конституція України визначає забезпечення інформаційної безпеки як одну з найважливіших функцій держави.

Для формування збалансованої державної інформаційної політики, здійснення комплексу узгоджених заходів щодо захисту національних інтересів України в інформаційній сфері створюється система забезпечення інформаційної безпеки України.

Правову основу функціонування та розвитку системи забезпечення інформаційної безпеки України складають: Конституція України, Концепція (основи державної політики) інформаційної безпеки України, закони України, інші нормативно-правові акти, що регулюють відносини в інформаційній сфері.

Основними елементами системи забезпечення інформаційної безпеки України є: громадяни України; Верховна Рада України; Президент України; Рада національної безпеки і оборони України; Кабінет Міністрів України; міністерства, інші центральні органи виконавчої влади, зокрема, Міністерство освіти і науки України, Міністерство культури й мистецтв України, Державний комітет інформаційної політики, телебачення і радіомовлення України, Державний комітет зв'язку та інформатизації України, Державний комітет архівів України, Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України; Національна Рада України з питань телебачення і радіомовлення; Конституційний Суд України, суди загальної юрисдикції; Генеральна прокуратура України; Рада Міністрів Автономної Республіки Крим, обласні державні адміністрації, Київська та Севастопольська міські державні адміністрації; органи місцевого самоврядування; інші державні органи та організації; засоби масової інформації; політичні партії та рухи; громадські організації; професійні спілки; заклади академічної науки та освіти; неурядові дослідницькі організації, інші організації та установи, що здійснюють діяльність в інформаційній сфері.

Система забезпечення інформаційної безпеки України виконує наступні основні функції, що розподіляються між її окремими елементами.

1. Створення та забезпечення діяльності державних органів – елементів системи забезпечення інформаційної безпеки України, що включає:

- створення правових засад для побудови, розвитку та функціонування системи;

- формування організаційної структури системи та її окремих елементів, визначення та раціональний розподіл їх функцій;
- комплексне забезпечення діяльності елементів системи: кадрове, фінансове, матеріальне, технічне, інформаційне та ін.;
- підготовку елементів системи до виконання покладених на них функцій згідно з призначенням.

2. Управління діяльністю системи забезпечення інформаційної безпеки України, що включає:

- вироблення стратегії та планування конкретних заходів щодо забезпечення інформаційної безпеки;
- організацію і безпосереднє керівництво системою та її структурними елементами;
- оцінку результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки та їх наслідків.

3. Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки України, що включає:

- визначення національних інтересів в інформаційній сфері та їх пріоритетів;
- прогнозування, виявлення та оцінку можливих загроз, дестабілізуючих чинників та конфліктів в інформаційній сфері, причин їх виникнення, а також наслідків їх ескалації;
- запобігання та усунення впливу загроз та дестабілізуючих чинників на національні інтереси в інформаційній сфері;
- локалізацію, деескалацію та розв'язання інформаційних конфліктів;
- ліквідацію наслідків інформаційних конфліктів або впливу дестабілізуючих чинників.

4. Міжнародне співробітництво в сфері інформаційної безпеки, що включає:

- розробку нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;
- входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення проблем інформаційної безпеки;
- участь у роботі керівних, виконавчих підрозділів та підрозділів забезпечення цих структур (організацій), спільне проведення планових та оперативних заходів.

Повноваження, функції та схему взаємодії елементів системи забезпечення інформаційної безпеки України визначають: Конституція України, Концепція (основи державної політики) інформаційної безпеки України, закони України, акти Президента України, постанови Кабінету Міністрів України, інші нормативно-правові акти, що регулюють відносини в інформаційній сфері.

Визначення (уточнення) та розподіл (перерозподіл) повноважень і функцій органів державної влади, побудова більш раціональної схеми їх взаємодії здійснюються на основі функціонального обстеження цих органів,

всебічного обгрунтування організаційних заходів, що пропонуються, з урахуванням нових умов, потреб і можливостей їх ресурсного забезпечення.

Діяльність системи забезпечення інформаційної безпеки України є відкритою для контролю відповідно до чинного законодавства.

РОЗДІЛ 5. ОСНОВНІ НАПРЯМИ ТА ПЕРШОЧЕРГОВІ ЗАХОДИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Державна політика інформаційної безпеки України визначається, виходячи з пріоритетності національних інтересів України в інформаційній сфері, та здійснюється шляхом реалізації відповідних стратегій і програм у сфері інформаційної безпеки згідно з чинним законодавством.

Основними напрямами державної політики інформаційної безпеки України є:

- забезпечення конституційних прав і свобод громадян в інформаційній сфері;
- формування відкритого й безпечного інформаційного простору;
- забезпечення захисту інформаційного простору України від негативного зовнішнього впливу;
- якісне інформаційно-аналітичне забезпечення діяльності органів державної влади та місцевого самоврядування;
- перетворення виробництва інформаційної продукції та послуг на потужний чинник економічного зростання України;
- інтеграція України до світового інформаційного простору;
- збереження власної культурної ідентичності за умов посилення процесів глобалізації;
- створення умов для ефективної діяльності системи забезпечення інформаційної безпеки України.

Серед першочергових заходів по забезпеченню інформаційної безпеки України необхідно здійснити наступні.

1. З метою забезпечення конституційних прав і свобод громадян в інформаційній сфері необхідно:

а) внести зміни та доповнення до чинного законодавства:

- до Кодексу України про адміністративні правопорушення, Кримінального кодексу України, якими встановити адміністративну та кримінальну відповідальність посадових осіб, засновників ЗМІ, умисні дії яких перешкоджають журналістам у виконанні ними своїх службових обов'язків чи пов'язані зі встановленням цензури;
- до Закону України "Про друковані засоби масової інформації (пресу) в Україні", до Цивільного та Кримінального кодексів України, якими передбачити: (1) верхню межу сум компенсацій заподіяної моральної шкоди та/або підвищення розміру державного мита до 5% від суми позов-

них вимог; (2) чіткі критерії визначення розміру компенсації заподіяної моральної шкоди; (3) розмежування оцінок журналістів та звинувачень, що можуть не відповідати дійсності; (4) створення Комісій з питань журналістської етики (досудові органи), які надають експертні висновки, що могли б враховуватися судами при прийнятті рішень; (5) скасування статей 125 "Наклеп" і 126 "Образа" Кримінального кодексу України. Справи про поширення відомостей, що не відповідають дійсності, принижують честь і гідність особи, надалі проводити лише в рамках цивільного судочинства;

- до Законів України "Про податок на додану вартість", "Про державну підтримку ЗМІ і соціальний захист журналістів", "Про оподаткування прибутку підприємств", "Про Єдиний митний тариф", інших законодавчих актів, якими передбачити пільгове оподаткування українських ЗМІ (крім видань еротичного, рекламного, розважального характеру); скасувати ПДВ на папір та друкування (на всьому технологічному циклі); ввізне мито на газетний папір, поліграфічне обладнання; податок на прибуток на добровільні пожертвування, гранти, благодійні внески, що надаються ЗМІ; вартість розповсюдження преси встановити залежно від ваги видання та відстані його доставки, але не вище граничних розцінок, встановлених Кабінетом Міністрів (крім видань еротичного, рекламного, розважального характеру);
- ухвалити Закон України "Про захист персональних даних", яким заборонити їх поширення без дозволу особи; узгодити його основні положення з Директивою 95/46/ЄС Європейського Парламенту та Ради ЄС від 24 жовтня 1995р. "Про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних та про вільну передачу таких даних". Підписати і ратифікувати Конвенцію Ради Європи від 21 січня 1981р. №108 "Про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних";
- скасувати положення статті 27 Закону України "Про Національну Раду України з питань телебачення і радіомовлення", якими Раді надається право (за погодженням з Міністерством фінансів) встановлювати максимальні рівні розцінок за рекламу;
- до Цивільного кодексу України, якими визначити особливості захисту особистих немайнових прав, прав на інтелектуальну власність у мережі Інтернет, захистити права на реєстрацію власних доменних імен, що відповідають прізвищам відомих осіб, компаній;

б) вжити організаційних заходів:

- відмовитися від надання вибіркових пільг для розповсюдження друкованих ЗМІ, передбачити такі пільги лише для дитячих, наукових та освітніх видань;
- посилити контроль над діяльністю монополістів в окремих сегментах інформаційного простору, провести їх поетапну демонополізацію. Про-

вести тендер на визначення кількох компаній, які б займалися розповсюдженням друкованих ЗМІ, заборонити їм відмовлятися від розповсюдження видань з будь-яких, окрім фінансових, причин. Скасувати рішення про обмеження кількості Інтернет-провайдерів, які здійснюють передачу даних за кордон;

- здійснювати перевірки ЗМІ лише згідно із заздалегідь оприлюдненим планом, не частіше одного разу на рік;
- забезпечити максимальну відкритість, парламентський контроль за розслідуванням тяжких злочинів проти журналістів, можливість (у випадку необхідності) звернення за допомогою до зарубіжних урядових і неурядових організацій.

2. З метою формування відкритого й безпечного інформаційного простору необхідно:

а) внести зміни та доповнення до чинного законодавства:

- ухвалити Концепцію роздержавлення ЗМІ, якою передбачити: (1) поступову, протягом двох-трьох років передачу прав засновників від держави до державних госпрозрахункових підприємств, з наступною приватизацією; (2) обмеження, а потім і припинення бюджетного фінансування ЗМІ після їх роздержавлення; (3) заборону в подальшому органам державної влади та місцевого самоврядування, підприємствам з бюджетним фінансуванням засновувати ЗМІ, крім інформаційних видань та web-сайтів в Інтернет; (4) передбачити в приватизаційних зобов'язаннях можливість певного обсягу державного мовлення на радіо- та телеканалах з програмами освітнього, учбового і культурологічного характеру;
- до Законів України "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", якими рекомендувати ЗМІ здійснювати попередню правову експертизу матеріалів, що можуть містити інформацію, потенційно здатну завдати моральної шкоди;
- ухвалити Закон України "Про обмеження поширення засобами масової інформації порнографії, жахів і насильства", яким передбачити: (1) визначення понять "порнографія", "насильство", "жахи"; (2) створення спеціальної Комісії з питань захисту громадської моралі (на основі вже діючої експертної комісії Міністерства культури й мистецтв) з числа державних службовців, громадських діячів, вчених, діячів культури, представників політичних партій і громадських організацій. Комісія повинна приймати рішення щодо наявності насильства, жахів та порнографії в кінофільмах, телепередачах тощо та про заборону їх показу в загальнодоступних кінотеатрах, на загальнодоступних і загальнонаціональних телеканалах; (3) здійснення продажу еротичних видань виключно в спеціалізованих магазинах, лише для повнолітніх, у закритому спеціальними обкладинками вигляді; (4) класифікацію кіно-, відео- телефільмів за категоріями, враховуючи ступінь їх можливого негативного впливу на

громадську мораль. Категорія А — показ по телебаченню лише після 22:00, у кінотеатрах — лише громадянам від 18 років; категорія Б — показ по телебаченню лише після 24:00., у кінотеатрах — громадянам від 21 року; категорія В — показ виключно в спеціальних кінотеатрах та по спеціальних каналах телебачення; категорія С — заборона розповсюдження і показу в Україні; (5) уточнення відповідальності за поширення порнографії в мережі Інтернет, встановлення вікових обмежень доступу до порнографічних web-сайтів;

- до Кодексу України про адміністративні правопорушення, Кримінального кодексу України, якими посилити адміністративну та кримінальну відповідальність за показ і розповсюдження кіно- і відеопродукції без ліцензії;
- ухвалити Закон України "Про психологічний захист населення" для зменшення негативного інформаційного впливу на індивідуальну та суспільну свідомість;

б) вжити організаційних заходів:

- створити систему суспільного (публічно-правового) телебачення197, фінансування якої передбачити за рахунок абонентської плати власників телевізорів;
- посилити контроль за виконанням чинного законодавства в інформаційній сфері;
- рекомендувати прийняти Хартію етики журналіста, в якій викласти основні морально-етичні та корпоративні правила поведінки журналістів; створити спеціальний, обраний усіма журналістами, видавцями, орган (Рада з питань діяльності ЗМІ), який би визначав порушення зазначених правил та вживав до порушників заходів громадського осуду;
- регулярно проводити парламентські слухання з питань поширення порнографії, жахів, насильства в інформаційному просторі України;
- створити умови для виробництва спеціальних пристроїв, що обмежують доступ неповнолітніх до порнографічних web-сайтів; встановити спеціальні фільтри на комп'ютерах в органах державної влади, освітніх закладах, бюджетних установах;
- утворити державну науково-дослідну структуру для вивчення впливу новітніх релігійних практик на психічне здоров'я людини та інформування громадськості про можливі загрози.

3. З метою забезпечення захисту інформаційного простору України від негативного зовнішнього впливу необхідно:

а) внести зміни та доповнення до чинного законодавства:

- ухвалити Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", яким передбачити: (1) вимоги та правила захисту інформації в цих мережах (зокрема, в інформаційних системах органів державної влади та місцевого самоврядування, автоматизованих системах управління військових формувань), що є власністю держави,

або інформації з обмеженим доступом, захист якої гарантується державою; (2) обов'язкові умови захисту інформації при наданні послуг передачі даних, у т.ч. з використанням Інтернет; (3) проведення законного моніторингу мереж передачі даних виключно на засадах національного та міжнародного законодавства, зокрема, положень резолюцій Ради Європи ENFOPOL 98; зобов'язати Інтернет-провайдерів зберігати відомості про Інтернет-трафік протягом півроку та надавати свідчення про нього за рішенням суду;

- ухвалити новий розділ Кримінального кодексу України, в якому визначити види комп'ютерних злочинів та встановити кримінальну відповідальність за їх вчинення: (1) несанкціонований доступ до інформації в автоматизованих системах (АС); (2) несанкціонований доступ до програмних засобів АС; (3) умисне порушення цілісності, спотворення, блокування, знищення інформації в АС; (4) умисне спотворення чи знищення програмних засобів в АС; (5) несанкціоноване використання інформації з АС; (6) умисне порушення функціонування АС;

б) вжити організаційних заходів:

- провести комплексну експертизу впровадження в Україні стандартів Міжнародної організації стандартів (ISO) в галузі криптографічного захисту інформації;
- створити умови для виробництва вітчизняного програмного забезпечення для використання в органах державної влади та місцевого самоврядування, оснащених комп'ютерними системами, в яких зберігається та обробляється інформація з обмеженим доступом;
- розробити правила закупівлі комп'ютерів, програмного забезпечення для їх використання в органах державної влади;
- правоохоронним органам надавати допомогу та рекомендації державним органам, суб'єктам господарювання та окремим користувачам стосовно боротьби з комп'ютерними вірусами та комп'ютерною злочинністю; створити web-сайт з вільним доступом, на якому б оприлюднювалася така інформація;
- у складі Міністерства внутрішніх справ створити підрозділи для боротьби зі злочинністю в сфері новітніх інформаційних технологій (комп'ютерною злочинністю); розробити програму підготовки (перепідготовки) кадрів для потреб цих підрозділів;
- створити умови для зацікавлення страхових компаній у впровадженні страхування від наслідків комп'ютерних злочинів та інших інформаційних ризиків.

4. **З метою якісного інформаційно-аналітичного забезпечення діяльності органів державної влади та місцевого самоврядування необхідно:**

а) внести зміни та доповнення до чинного законодавства:

- до Кодексу України про адміністративні правопорушення, якими встановити адміністративну відповідальність державних службовців за неви-

конання статті 32 Закону України "Про інформацію", в т.ч. заборонити їм на певний час займати посади на державній службі;

- до статті 27 Закону України "Про друковані засоби масової інформації (пресу) в Україні", статті 34 Закону України "Про телебачення і радіомовлення", якими передбачити повідомлювальний принцип акредитації журналістів при органах державної влади, їх вільний доступ на брифінги, прес-конференції посадових осіб за редакційними посвідченнями;
- до статті 32 Закону України "Про інформацію", якими визначити необхідність відповіді на інформаційні запити та звернення громадян, подані електронною поштою;

б) вжити організаційних заходів:

- створити цілісну систему інформаційно-аналітичної підтримки діяльності органів державної влади, яка б виконувала наступні функції: (1) автоматизація процесу збору, обробки та використання інформації, електронний документообіг; (2) формування бази даних центральних і місцевих органів державної влади, органів місцевого самоврядування; (3) здійснення оперативного інформаційно-аналітичного забезпечення керівництва держави в надзвичайних (нештатних) ситуаціях, зокрема, через створення мережі ситуаційних центрів; (4) формування бази даних типових моделей вирішення проблемних ситуацій за різними напрямами державного управління, в т.ч. на основі досвіду інших країн; (5) сприяння координації діяльності органів державної влади з використанням можливостей системи. Передбачити: можливість доступу громадян до відкритої інформації в системі; захист її від несанкціонованого доступу (організаційно-адміністративні заходи, програмні та інженерно-технічні засоби); адаптованість системи до світових інформаційних мереж; єдині нормативно-правові, програмні, технічні, лінгвістичні вимоги до неї;
- затвердити програму підготовки (перепідготовки) державних службовців для освоєння ними новітніх інформаційних технологій, отримання знань і практичних навичок щодо захисту інформації;
- впровадити практику публічного обговорення проектів нормативно-правових актів Кабінету Міністрів, міністерств, центральних органів виконавчої влади, місцевих державних адміністрацій; публікувати тексти проектів нормативно-правових актів у центральній та місцевій пресі відповідно, практикувати обговорення запланованих державних рішень на радіо і телебаченні;
- розповсюдити практику організації "гарячих телефонних ліній" на рівень місцевих державних адміністрацій, публікувати в місцевій пресі звіти про виконання заходів, яких було вжито (аналогічні звіти про дії Уряду оприлюднювати в газеті "Урядовий кур'єр");
- створити web-сайти всіх міністерств, центральних органів виконавчої влади, обласних державних адміністрацій, на яких розміщувати: відо-

мості про організаційну структуру, склад та основні види діяльності установи, номер "гарячого телефону"; тексти нормативних актів, прийнятих установою; оперативну інформацію; важливі повідомлення; бланки документів;

- щорічно публікувати звіти міністерств, центральних органів виконавчої влади, місцевих державних адміністрацій, органів місцевого самоврядування про проведену роботу та структуру витрат бюджетних (позабюджетних) коштів;
- створити єдину систему зв'язків із громадськістю; при місцевих державних адміністраціях утворити Громадські ради, на засідання яких виносити актуальні питання регіонального розвитку та шляхи їх вирішення; до складу Громадських рад можуть входити представники політичних партій, громадських організацій, вчені, підприємці, представники ЗМІ.

5. **З метою перетворення виробництва інформаційної продукції та послуг на потужний чинник економічного зростання України необхідно:**

а) внести зміни та доповнення до чинного законодавства:

- до Законів України "Про податок на додану вартість", "Про оподаткування прибутку підприємств", "Про Єдиний митний тариф", інших законодавчих актів, якими встановити податкові пільги для діяльності в сфері виробництва і розповсюдження новітніх інформаційних технологій, програмного забезпечення, виробництва комп'ютерів, Інтернет-ринку;
- до Закону України "Про державний бюджет на 2001р." (і далі), якими забезпечити через захищені статті державного бюджету пріоритетне фінансування Національної програми інформатизації відповідно до визначених потреб;
- ухвалити Закони України "Про електронні документи і електронний документообіг", "Про електронний цифровий підпис", до їх прийняття ухвалити відповідні Укази Президента України;
- ухвалити Закон України "Про Інтернет-видання", яким визначити правовий статус, особливості діяльності, повідомлювальний порядок реєстрації Інтернет-видань;

б) вжити організаційних заходів:

- створити робочу групу із залученням представників компаній, що працюють у сфері новітніх інформаційних технологій, для: (1) розробки Концепції та Державної програми розвитку Інтернет в Україні; (2) підготовки законопроектів з цих питань; (3) розробки механізмів захисту інформації, моніторингу та фільтрації протиправної інформації; (4) розгляду питань адміністрування національного домену .ua;
- впровадити систему підготовки (перепідготовки) висококваліфікованих кадрів у сфері інформаційних технологій, у т.ч. за кордоном (за рахунок іноземних програм технічної допомоги). З особами, які направляються за кордон, укладати контракт, що передбачає відшкодування витрат дер-

жави у випадку їх неповернення до України. Укладати договори з країнами, куди від'їджають українські фахівці, щодо надання їм гарантій (трудових, пенсійних, соціальних, на інтелектуальну власність). Вирішити питання щодо компенсації українській стороні витрат на підготовку фахівців у випадку їх виїзду за кордон, спрощення візових процедур для забезпечення контактів цих фахівців з родичами, розподілу податків від їх доходів;

- сприяти ініціативі Інтернет-провайдерів щодо Інтернет-підтримки середніх навчальних закладів, особливо в сільській місцевості;
- модернізувати та реконструювати інформаційну інфраструктуру, зокрема, лінії зв'язку (подальше впровадження оптико-волоконих ліній, цифрового сегменту), мережі передачі даних, збільшити кількість електронних АТС;
- збільшити кількість годин у шкільних програмах на вивчення та опанування навичками роботи в Інтернет, розробити та видати шкільні підручники з цього предмету, продовжити роботу по комп'ютеризації шкіл. У межах кошторисів на утримання шкіл передбачити оплату Інтернет-послуг. Регулярно проводити всеукраїнські олімпіади з комп'ютеризації для школярів і студентів. Надати їх переможцям пільги для вступу до ВНЗ та зарахування на роботу. У ВНЗ ввести додаткові курси, пов'язані з вивченням Інтернет; спільно із зацікавленими Інтернет-провайдерами створити спеціальні учбові web-сайти з різних предметів (математики, фізики та ін.);
- створити організацію, яка б здійснювала реєстрацію доменних імен зони .ua;
- створити умови для впровадження електронної системи купівлі квитків, бронювання номерів в готелях, електронної комерції тощо.

6. **З метою інтеграції України до світового інформаційного простору необхідно:**

а) внести зміни та доповнення до чинного законодавства:

- узгодити основні положення законопроектів "Про кабельне, ефірно-кабельне телебачення і телеінформаційні мережі", "Про телекомунікації", "Про міжнародний обмін масовою інформацією", "Про національні інформаційні ресурси", "Про діяльність у сфері інформатизації" з принципами законодавства Європейського Союзу;
- ратифікувати Європейську Конвенцію про транскордонне телебачення;

б) вжити організаційних заходів:

- приєднатися до стандартів ISO в галузі новітніх інформаційних технологій;
- організувати мовлення каналу супутникового телебачення для трансляції на зарубіжні країни, забезпечити його державне фінансування; створити іномовні інформаційні ресурси про економічний, науковий, освітній, культурний, туристичний потенціал України;

- сприяти обміну ефірним часом у FM-діапазоні між радіостанціями світових столиць і України; розповсюдженню державних офіційних видань за кордоном; визначити підготовку новин для закордонних інформаційних агентств однією з пріоритетних функцій Укрінформу;
- розвивати співпрацю з Генеральним директоратом Європейської Комісії "Інформаційне суспільство";
- взяти участь у конкурсі ЄС: проекти для програми IST (Information Society Technologies);
- з метою просування позитивного іміджу України у світовий інформаційний простір, запровадити цільові програми "Світові зірки України" (створення web-сайтів, закордонні поїздки відомих у світі українців, поширення матеріалів через ЗМІ тощо); залучити громадські організації, незалежних експертів до обговорення проблем інтеграції України до світового інформаційного простору, підготовки та проведення окремих заходів;
- створити інформаційні центри при посольствах України із залученням джерел спонсорського фінансування їх діяльності. Визначити одним із пріоритетів нової Державної програми співпраці з українською діаспорою залучення інформаційного, культурного потенціалу українців за кордоном;
- організувати систему професійної підготовки з інформаційних технологій для державних службовців, які представляють Україну за кордоном. Проводити перепідготовку на курсах PR співробітників посольств і закордонних представництв (радників з питань преси та інформації, прес-аташе, радників з питань культури та освіти). При Дипломатичній академії МЗС України організувати вищі курси міжнародних PR-технологів;
- створити умови для організації неурядового Фонду, який сприяв би формуванню позитивного міжнародного іміджу України. Його засновниками можуть бути крупні вітчизняні бізнесові структури, зацікавленні у просуванні своєї продукції на зовнішні ринки, впливові громадські організації та ЗМІ.

7. **З метою збереження власної культурної ідентичності за умов посилення процесів глобалізації необхідно:**

а) внести зміни та доповнення до чинного законодавства:

- внести зміни та доповнення до Закону України "Про друковані засоби масової інформації (пресу) в Україні", якими встановити, що видання, які мають закордонні аналоги, повинні містити не менше 50% інформації українського походження;

б) вжити організаційних заходів:

- забезпечити виконання Державної програми розвитку національного книговидання та преси; передбачити державне фінансування реконструкції та розвитку поліграфічної бази;

- створити умови для підвищення конкурентоспроможності українських ЗМІ, якості їх технічної оснащеності, підвищення фінансової спроможності; підвищити рівень соціального захисту працівників ЗМІ;
- створити Національну систему інформаційних ресурсів, електронні каталоги центральних і регіональних бібліотек, архівів (до 2004р. їх основні фонди перевести в електронний вигляд) та забезпечити доступ до них через Інтернет; збільшити кількість інформаційно-пошукових систем, які б могли здійснювати повноцінний пошук українською мовою, мовно адаптованих програмних продуктів;
- посилити боротьбу з контрабандою іноземних друкованих видань та книг, аудіо-, відео-, кіно- та іншої інформаційної продукції.

8. З метою створення умов для ефективної діяльності системи забезпечення інформаційної безпеки необхідно:

- посилити роль РНБО України як головного органу координації та контролю на міжвідомчому рівні у сфері інформаційної безпеки; питання інформаційної безпеки розглядати на засіданнях РНБО України не рідше одного разу на рік198; у структурі Апарату РНБО України створити Управління проблем інформаційної безпеки, на яке покласти функції моніторингу загроз інформаційній безпеці України, підготовки заходів щодо їх запобігання та локалізації;
- перед прийняттям організаційних рішень проводити функціональне обстеження діючих органів державної влади. Відповідні укази глави держави повинні включати додатки, в яких визначаються повноваження, функції та схема взаємодії органів державної влади, що утворюються або реформуються;
- провести комплексне функціональне обстеження всіх державних органів, що утворюють систему забезпечення інформаційної безпеки України, з метою уникнення дублювання ними окремих функцій (ліквідації надмірних структур), забезпечення виконання повного переліку функцій, необхідних для забезпечення ефективної роботи цілісної системи. Подати Президентові України конкретні пропозиції щодо структурних змін у системі державних органів, а також зміни та доповнення до положень, що визначають засади їх діяльності;
- утворити в структурі обласних державних адміністрацій управління реалізації державної політики інформатизації.

ЗАКОН УКРАЇНИ
Про інформаційну безпеку України
Проект

Цей Закон визначає та регулює правові та організаційні засади забезпечення інформаційної безпеки України.

На підставі Конституції України Закон надає гарантії розвитку та захисту національного інформаційного простору і зміцнення інформаційної безпеки як складової частини національної безпеки України.

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Мета і сфера дії Закону

Метою Закону є забезпечення правових основ інформаційної безпеки України.

Закон створює сприятливі умови та надає гарантії розвитку і захисту інтересів, прав та свобод людини, захищає національні інтереси суспільства та держави щодо розбудови системи розгалуженого, розвинутого і захищеного інформаційного середовища в Україні.

Дія цього Закону поширюється на суспільні відносини у сфері інформаційної діяльності, формування і здійснення збалансованої політики та стратеги розвитку інформаційних ресурсів суспільства та держави.

Дія цього Закону не поширюється на регулювання інформаційних відносин у процесі побутового спілкування, літературно-мистецької та науково-творчої діяльності, на зміст інформації, що є продуктом художньої творчості, а також на проведення різного роду дискусій, симпозіумів, конференцій, з'їздів, семінарів, літературно-мистецьких заходів тощо, за виключенням публічної інформації про ці заходи, її поширення та використання.

Стаття 2. Основні поняття і терміни, використані в цьому Законі

У цьому Законі використані наступні поняття і терміни:

інформаційна безпека України — комплекс системних превентивних заходів із надання гарантій захисту життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз;

національний інформаційний простір України — сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства, держави з їх рівним правом доступу до

відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб субєктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм;

інформаційна інфраструктура — це сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництва інформаційних технологій, сервісного обслуговування елементів інфраструктури і системи підготовки кадрів;

інформаційна система — організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів; загальна структура і мережа інформаційних систем у їх взаємодії у національному просторі України;

інформаційно-телекомунікаційні структури — це територіально розподілені державні і корпоративні комп'ютерні мережі, телекомунікаційні мережі й системи спеціального призначення і загального користування, мережі й канали передачі даних, засоби комутації та управління інформаційними потоками;

система засобів масової інформації — це сукупність друкованих і електронних засобів масової інформації — телерадіокомпаній, інформаційних агентств, комплексів книговидання, кінематографічного, бібліотечного, архівного тощо;

інформаційне середовище — усталене поєднання окремих суб'єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах;

інформаційний продукт — матеріалізований результат інформаційної діяльності, документований на будь-якому носії або оголошений публічно і призначений для забезпечення інформаційних потреб користувача;

ідентифікація в інформаційних відносинах — обов'язкове застосування засобами масової інформації у національному інформаційному просторі України системи відкритих повідомлень, спеціальних позначок та символів, якими забезпечується чітке розпізнання країни походження, мови оригіналу, авторства і виробника інформаційного продукту, літературного, мистецького, наукового або іншого твору, а також установлення в разі необхідності на підставі документів інформаційних відносин, відповідно до законів України, власника, постачальника, розповсюджувача та замовника інформаційного продукту;

інформаційні послуги — інформаційна або інформаційно-посередницька діяльність, спрямована на задоволення замовних запитів і потреб користувачів інформаційної продукції;

інформаційні процеси — здійснення створення, пошуку, збирання, обробки, накопичення, виробництва, зберігання, захисту, передачі, поширення та споживання інформаційної продукції;

інформаційні технології – організована сукупність систем, засобів, методів і способів, яка на базі інформаційної інфраструктури забезпечує процеси обробки, зберігання, розвитку, поширення, використання та захисту інформаційних ресурсів;

національні інформаційні ресурси – це окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази й банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості й знання, зафіксовані на відповідних носіях інформації, є обєктами права власності всіх субєктів України і мають споживацьку вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо).

світовий інформаційний простір – визначене міжнародним співтовариством, введене до міжнародно-правових документів поняття, що означає сферу (об'ємний простір), у якій відбувається інформаційна діяльність людства, впорядкована, як правило, міжнародними конвенціями і договорами;

злочин у цифрових телекомунікаційних мережах – протиправна дія, яка виражається у використанні або спробі використання автоматизованої комп'ютерної системи (мережі, комп'ютера) із корисливою або хуліганською метою, становить загрозу інформаційним ресурсам, самій автоматизованій комп'ютерній системі (мережі, комп'ютеру), завдає економічної, політичної, фізичної та іншої шкоди людині, суспільству, державі.

Стаття 3. Об'єкти регулювання Законом

Об'єктами регулювання цим Законом є суспільні відносини, пов'язані з:

формуванням та здійсненням державної інформаційної політики;

розвитком, використанням та захистом національного інформаційного простору, інформаційної інфраструктури та національних інформаційних ресурсів України;

захистом прав, свобод та інтересів суб'єктів інформаційної діяльності.

Стаття 4. Суб'єкти інформаційної безпеки

Суб'єктами інформаційної безпеки виступають вітчизняні юридичні та фізичні особи, юридичні та фізичні особи іноземних держав, органи державної влади, органи місцевого та регіонального самоврядування, інші суб'єкти, які здійснюють інформаційну діяльність у національному інформаційному просторі.

Стаття 5. Об'єкти інформаційної безпеки

Об'єктами інформаційної безпеки є:

- у сфері економіки;

інформаційно-аналітична система державної статистики;

джерела інформації про комерційну діяльність суб'єктів усіх форм власності;

інформаційно-аналітичні системи збору та обробки фінансової, податкової, митної, зовнішньоекономічної інформації;

- в галузі оборони:

інформаційно-аналітичні системи, інформаційні ресурси апарату Міністерства оборони, Генерального штабу Збройних Сил України;

інформаційні ресурси військово-оборонних підприємств та науково-дослідних установ, які працюють у цій галузі;

системи зв'язку та управління військами та зброєю;

морально-психологічний стан Збройних Сил України;

- у духовній сфері:

світогляд людини, її життєві цінності та ідеали;

соціальні та особистісні орієнтації;

культурні та естетичні позиції;

- у політичній сфері:

суспільна свідомість та політична орієнтованість суспільних верств та населення окремих регіонів країни;

система вироблення, прийняття і впровадження політичних рішень;

права політичних партій, організацій, громадських об'єднань;

система інформування населення про політичне, економічне та інше життя країни;

система формування громадської думки, до якої входять інституції вивчення та аналізу громадської думки.

Стаття 6. Національний інформаційний простір України

Держава виступає гарантом цілісності національного інформаційного простору України на основі:

єдиної державної політики, визначеної законами, обов'язковими для всіх учасників інформаційної діяльності в національному інформаційному просторі України незалежно від форм власності;

збереження права власності держави на провідні об'єкти національного інформаційного простору, використання нею належної бази та економічних важелів для здійснення регулятивного впливу на суспільні відносини у сфері інформації;

державної системи професійного навчання і підвищення кваліфікації працівників засобів масової інформації, наукової та експериментальної діяльності;

економічного забезпечення цільових програм, здійснення відповідних протекціоністських заходів.

Об'єктами національного інформаційного простору є інформаційна продукція в усіх її різновидах, включаючи твори літератури і мистецтва, наукові праці, публічні виступи, використані в інформаційній діяльності, національні інформаційні ресурси, інформаційні послуги, організаційні та майнові функціональні елементи інформаційної інфраструктури.

Стаття 7. Загрози національному інформаційному просторові й інформаційній безпеці України

Загрозами національному інформаційному просторові й інформаційній безпеці України є:

прояви обмеження свободи слова та доступу громадян до інформації;

поширення засобами масової інформації сцен насильства, жорстокості, порнографії;

злочинність у цифрових телекомунікаційних мережах типу Інтернет та комп'ютерний тероризм;

розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

заподіяння шкоди життєво важливим інтересам особи, суспільства та держави через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення інформації, забороненої чи обмеженої для поширення законами України;

намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації;

однобока політична орієнтація інституцій масової інформації та формування суспільної думки під адміністративним впливом державних органів чи під економічним впливом комерційних чи кримінальних структур;

пропагандистський, психологічний та інший вплив на політичну орієнтацію населення, котрий здійснюється вітчизняними чи іноземними засобами інформації в інтересах окремих політичних сил;

відсутність чи слабкість державної політики залучення суспільства до системи вироблення, прийняття та впровадження політичних рішень;

відсутність законодавства, котре зобов'язує державну владу регулярно та повно інформувати населення про свою діяльність та стан справ у державі;

створення перешкод із боку держави з питань здійснення законних та рівних прав на використання засобів інформації різними політичними чи громадськими об'єднаннями;

фальсифікація, перекручування чи замовчування інформації про події, що відбуваються у житті суспільства;

тенденційність чи упередженість при інтерпретації результатів опитувань, референдумів, виборів.

Стаття 8. Забезпечення інформаційної безпеки України

Забезпечення інформаційної безпеки України здійснюється шляхом:

законодавчого формування державної інформаційної політики;

створення і використання можливостей, які відповідають законам України, із метою досягнення інформаційної достатності для прийняття рішень

органами державної влади, громадянами і об'єднаннями громадян, іншими суб'єктами права в Україні;

гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;

створення розвиненої інформаційної інфраструктури;

підтримки державою розвитку національних інформаційних ресурсів України з урахуванням новітніх досягнень науки і техніки та особливостей духовно-культурного життя і традицій народу України;

створення та впровадження безпечних прогресивних інформаційних технологій;

захисту права власності всіх учасників інформаційної діяльності в національному інформаційному просторі України;

збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України;

охорони державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою;

створення загальної системи охорони інформації, зокрема, охорони державної таємниці, а також іншої інформації з обмеженим доступом;

захисту національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

установлення законодавством режиму доступу інших держав або їхніх представників до національних інформаційних ресурсів України та порядку використання цих ресурсів на основі договорів з іншими державами;

законодавчого визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України;

усунення негативних чинників порушення інформаційного простору, інформаційної та культурної експансії та інформаційної дискримінації України;

створення системи незалежного та гласного громадського контролю за діяльністю інституцій масової інформації, вивчення суспільної думки, служб зв'язку з населенням;

створення розвиненої інформаційної інфраструктури;

активізації упереджувальної діяльності інститутів державної влади та дипломатичних зусиль щодо запобігання інформаційно-пропагандистському втручанню у внутрішні справи країни;

формування та розповсюдження духовних цінностей, котрі відповідають національним інтересам країни та сприяють вихованню громадянського та патріотичного обов'язку.

Стаття 9. Правова основа інформаційної безпеки

Правову основу інформаційної безпека України становлять Конституція України, цей Закон, закони України "Про основи національної безпеки Ук-

раїни", "Про державну таємницю", "Про Національну систему конфіденційного зв'язку", "Про Раду Національної безпеки і оборони України", "Про інформацію", "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", "Про захист інформації в автоматизованих системах", "Про національний архівний фонд та архівні установи", "Про інформаційні агентства", "Про зв'язок", "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації", "Про захист суспільної моралі", інші закони, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Розділ II. ОСНОВНІ НАПРЯМИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Стаття 10. Основні напрями державної інформаційної політики та інформаційної безпеки України

Основними напрямами державної політики в інформаційній сфері України є:

забезпечення інформаційного суверенітету України;

вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Головною метою державної інформаційної політики та інформаційної безпеки України є забезпечення належних правових, економічних, внутрішньо – і зовнішньополітичних, організаційних та інших умов для:

створення розвинутого та захищеного інформаційного середовища суспільства;

сприяння міжнародному співробітництву в інформаційній сфері;

унеможливлення реалізації загроз заподіяння в процесі інформаційної діяльності шкоди життєво важливим інтересам особи, суспільства та держави.

Збалансована державна інформаційна політика України формується як складова частина соціально-економічної політики держави, виходячи з пріоритетності національних інтересів та загроз національній безпеці України, грунтується на засадах правової демократичної держави і впроваджується шляхом реалізації відповідних національних доктрин, стратегій, концепцій та програм відповідно до чинного законодавства.

Основними напрямами державної інформаційної політики України є

- в організаційній сфері:

створення умов для своєчасного, якісного і ефективного інформаційного забезпечення громадян, органів державної влади, органів місцевого самоврядування, об'єднань громадян на основі національних інформаційних ресурсів;

адміністративний, технічний, судовий, міжнародно-правовий захист вітчизняного (національного) інформаційного продукту України, загалом її інформаційних ресурсів, особливо тих, які є національним надбанням України;

- у сфері інформаційної безпеки:

захист населення України від інформаційної продукції, яка загрожує його фізичному, інтелектуальному, морально-психологічному здоров'ю (пропаганда жорстокості, насильства, порнографії, окультизму, вплив на підсвідомість тощо);

посилення інформаційної безпеки як невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки України;

усебічне сприяння наданню інформаційних послуг (інформаційного забезпечення) правоохоронним відомствам для виконання ними своїх функцій;

охорона державної таємниці та іншої інформації з обмеженим доступом, що є об'єктом права власності держави або об'єктом лише володіння, користування чи розпорядження державою, а також здійснення державного контролю за режимом доступу до цієї інформації;

- у міжнародній сфері:

активне сприяння створенню інформаційної продукції у глобальних комп'ютерних мережах та системах українською мовою;

дотримання принципів Європейської Конвенції про права людини, міжнародних документів у галузі міждержавного інформаційного співробітництва, ратифікованих Україною;

забезпечення ефективної присутності України у світовому інформаційному просторі шляхом розвитку транскордонного й прикордонного мовлення, *поширення вітчизняної культурно-мистецької і друкованої продукції*;

- у виробничій сфері:

збереження та ефективне використання державної та комунальної власності на підприємства, інші об'єкти національного інформаційного простору України, які в установленому законодавством порядку визнаються об'єктами стратегічного значення;

створення сприятливих умов для розвитку та захист прав суб'єктів права всіх форм власності на об'єкти національного інформаційного простору України і прав їхніх власників;

сприяння конкуренції, недопущення монополізації ринків у сфері інформаційної діяльності, в тому числі рекламної;

економічна підтримка державою реалізації планів розвитку інформаційної інфраструктури та інформаційної системи України в цілому незалежно від форм власності на об'єкти, що будуються і розвиваються, сприяння розробці і впровадженню новітніх інформаційних технологій;

- у сфері суспільних відносин:

забезпечення права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційної діяльності в національному інформаційному просторі України, недопущення втручання у зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законом відповідно до Конституції України;

збереження вітчизняного (національного) інформаційного продукту, національно-культурних та духовних цінностей України,

забезпечення інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі;

усебічна державна підтримка засобів масової інформації та забезпечення соціально-правового захисту журналістів, інших професійних творчих працівників, які займаються інформаційною діяльністю;

- у галузі науки, культури, навчання та підвищення кваліфікації:

формування загальнодержавної комп'ютерної мережі освіти, науки, культури, охорони здоров'я тощо, як частини світового інформаційного простору;

послідовне здійснення заходів, спрямованих на підвищення кваліфікації, вдосконалення, використання та заохочення творчих кадрів в інформаційній сфері.

Стаття 11. Система забезпечення інформаційної політики та інформаційної безпеки України

Відповідно до Конституції України:

- Верховна Рада України:

визначає засади та головні напрями інформаційної політики та інформаційної безпеки України;

здійснює законодавче регулювання суспільних і виробничих відносин у сфері інформаційної діяльності;

приймає загальнодержавні концепції та стратегії розвитку національного інформаційного простору, інформатизації, телебачення і радіомовлення, концепції участі України в глобальних інформаційно-комунікаційних мережах і системах;

схвалює в рамках державних програм економічного, науково-технічного, військового, соціального, національно-культурного розвитку програми

(перспективні плани) розвитку інформаційної системи та інфраструктури України;

затверджує перелік об'єктів права державної власності в національному інформаційному просторі України, які не підлягають приватизації;

визначає засади утворення і діяльності засобів масової інформації в Україні;

визначає головні напрями державної інформаційної політики та інформаційної безпеки України;

запроваджує контроль за діяльністю органів державної влади та посадових осіб щодо здійснення ними відповідних повноважень у сфері державної інформаційної політики та інформаційної безпеки України.

- Президент України:

забезпечує послідовне проведення державної інформаційної політики та інформаційної безпеки України.

– Кабінет Міністрів України :

організовує здійснення виконання державної інформаційної політики;

уживає заходів щодо зміцнення інформаційної безпеки України;

забезпечує здійснення концепцій і програм (перспективних планів) розвитку інформаційної системи, використання і захисту радіочастот та інформаційної інфраструктури України, формування та використання її національних інформаційних ресурсів;

створює відповідні умови і сприяє запровадженню та розвитку прогресивних технологій у галузях зв'язку та інформатизації у сфері засобів масової інформації в Україні, їх державної підтримки, соціального захисту журналістів та працівників інформаційної сфери.

- Рада національної безпеки і оборони України:

координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки України.

Розділ III. ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ СТАНОВЛЕННЯ ТА РОЗВИТКУ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Стаття 12. Національні інформаційні ресурси і право власності на них

Інформаційні ресурси інформаційної системи України є об'єктами відносин фізичних, юридичних осіб, держави, складають національні інформаційні ресурси України та захищаються відповідно до чинного законодавства нарівні з іншими ресурсами України.

До складу національних інформаційних ресурсів України входять інформаційні ресурси державної, комунальної та інших форм власності.

Основу національних інформаційних ресурсів України становить сукупний вітчизняний (національний) інформаційний продукт.

Придбана суб'єктами національного інформаційного простору України на законних підставах зарубіжна інформаційна продукція стає частиною національних інформаційних ресурсів України.

До складу державної та комунальної власності входять інформаційні ресурси, які створюються, закуповуються, накопичуються за рахунок Державного бюджету України або місцевих бюджетів, а також ті, що передаються в державну чи комунальну власність у спадщину, шляхом дарування, а також в інший установлений спосіб.

Національні інформаційні ресурси, які є власністю держави, перебувають на обліку та у віданні органів державної влади і організацій відповідно до їхньої компетенції.

Юридичні та фізичні особи є власниками тих документів, окремих масивів документів, документів і масивів документів в інформаційних системах, які створені за рахунок їхніх коштів, придбані ними на законних підставах, отримані в порядку дарування або спадщини, а також в інший, дозволений законом, спосіб.

Національні інформаційні ресурси можуть бути товаром, за винятком випадків, передбачених законом України.

Право власності на об'єкти інформаційної інфраструктури, технології та засоби обробки і поширення інформації не створює права власності на інформаційні ресурси, які належать іншим власникам.

Стаття 13. Національні інформаційні ресурси виняткового державного значення

Національними інформаційними ресурсами виняткового державного значення визнаються інформаційні ресурси, які своїм змістом можуть істотно впливати на стан національної безпеки України.

Віднесення інформації, документів, масивів документів, належних суб'єктам права власності в Україні, до складу національних інформаційних ресурсів виняткового державного значення або виключення їх із цього складу, здійснюється в порядку, встановленому законами України.

У разі появи документів, масивів документів, інших кінцевих результатів інтелектуальної діяльності виняткового державного значення поза державною власністю (шляхом створення або придбання в дозволений законом спосіб) держава викуповує їх у юридичних та фізичних осіб у порядку, встановленому законами України.

Власник не викуплених державою інформаційних ресурсів, які відносяться до інформаційних ресурсів виняткового державного значення, зобов'язаний забезпечити їхню охорону і збереження та може розпоряджатися ними лише з урахуванням положень, встановлених законами України.

Стаття 14. Віднесення інформаційних ресурсів до національного надбання України

Найбільш вагома, вартісна частина інформаційних ресурсів, особливо кінцеві результати інтелектуальної, творчої діяльності, кращі зразки вітчизняного (національного) інформаційного продукту без позбавлення права власності на

них можуть оголошуватись національним надбанням України і незалежно від форм власності охоронятись державою як пам'ятки історії та культури.

Продаж, дарування, передавання в інший спосіб інформаційних ресурсів, віднесених до національного надбання України, іноземним юридичним і фізичним особам контролюється державою в порядку, встановленому законами України.

Стаття 15. Мови в національному інформаційному просторі України

Використання мов у національному інформаційному просторі України регулюється Конституцією України, законами України "Про мови в Україні", "Про інформацію", "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", "Про інформаційні агентства", цим та іншими законами.

Держава постійно вживає заходи, спрямовані на розширення сфери використання української мови в національному інформаційному просторі України.

Кабінетові Міністрів України, уповноваженим ним на це центральним органам виконавчої влади дозволяється встановлювати заохочувальні тарифи, ставки, пільги, а також обов'язкові норми на поширення інформаційної продукції, поширення та виконання художніх творів українською мовою вітчизняними і зарубіжними виробниками, авторами та виконавцями.

Держава відповідно до законів України гарантує вільне використання в інформаційній діяльності мов народів і національних меншин України з метою задоволення їх інформаційних, лінгвістичних, національно-культурних, правових, освітніх запитів і потреб.

Функціонування іноземних мов у національному інформаційному просторі України визначається потребами поширення вітчизняного (національного) інформаційного продукту за рубежем та необхідністю культурно-освітніх програм і видань іноземними мовами для населення України, а також відповідно до інтересів участі України в міжнародному інформаційному співробітництві за укладеними нею угодами.

Продукція зарубіжних телерадіоорганізацій поширюється в Україні державною мовою чи мовами національних меншин України або в обов'язковому супроводі перекладу на державну мову чи мови національних меншин України, за винятком випадків, передбачених законодавством (викладання іноземних мов, музичні програми і передачі тощо). Друковані видання іноземними мовами поширюються в Україні на основі міжнародних договорів, ратифікованих Україною, в порядку, визначеному Законами України "Про інформацію", "Про друковані засоби масової інформації (пресу) в Україні" та "Про видавничу справу".

Стаття 16. Інформаційна інфраструктура України

Інформаційна інфраструктура України складається з організаційних структур, що забезпечують формування, функціонування й розвиток інфор-

маційного простору, а також збирання, обробку, зберігання, поширення та ефективне використання інформаційних ресурсів. Інформаційно – телекомунікаційні структури та інформаційні технології виконують обслуговуючу (науково-методичне, інформаційне, матеріально-технічне, кадрове, фінансове забезпечення) роль щодо діяльності цих елементів.

Держава контролює збереження, реконструкцію та реорганізацію елементів і об'єктів інформаційної інфраструктури шляхом ліцензування та реєстрації, незалежно від їх форм власності.

В ході структурної перебудови економіки, реконструкції матеріально-технічної бази та в процесі приватизації перепрофілювання об'єктів інформаційної інфраструктури України провідного значення допускається за програмами приватизації у встановленому законами порядку.

Приватизація майна та об'єктів інформаційної інфраструктури регулюється нормами законів України "Про державну підтримку засобів масової інформації та соціальний захист журналістів", "Про зв'язок", "Про приватизацію" з урахуванням інтересів держави та її інформаційної безпеки.

Верховна Рада України за поданням Кабінету Міністрів України затверджує перелік об'єктів та майна інформаційної інфраструктури України (телерадіопередавальні центри, окремі об'єкти зв'язку, кінокопіювальні підприємства, фонди, приміщення та обладнання архівів тощо), які приватизації не підлягають.

Держава забезпечує захист прав усіх суб'єктів права власності на об'єкти та майно інформаційної інфраструктури України.

Використання об'єктів інформаційної інфраструктури України, здійснюється на підставі угод (договорів) між їх власниками та користувачами.

Регулятивні та контрольні повноваження державних органів спрямовуються виключно на сприяння цілісному функціонуванню інформаційної інфраструктури і не можуть використовуватись для втручання в хід інформаційних процесів, перешкоджати свободі інформаційної діяльності.

Стаття 17. Інформаційні системи, технології та засоби їх забезпечення

Державні та недержавні установи, а також громадяни мають рівні права на розробку та вироблення інформаційної продукції, інформаційних систем, технологій та засобів їх забезпечення згідно чинного законодавства.

Усі види інформаційних технологій, їх виробництва та засоби забезпечення цих технологій становлять спеціальну сферу народногосподарської діяльності, розвиток якої визначається державною інформаційною політикою та Національною програмою інформатизації.

Завдання Національної програми інформатизації на наступні три роки та пріоритетні напрями розвитку інформатизації, обсяги, джерела і порядок їх бюджетного фінансування на наступний рік щорічно затверджуються Верховною Радою України.

Держава сприяє впровадженню новітніх технологій в інформаційній інфраструктурі України, створює сприятливі умови для проведення науково-дослідних та конструкторських робіт у цій галузі.

Визначення завдань Національної програми інформатизації, пріоритетних напрямів розвитку інформатизації, обсягів, джерел і порядку їх бюджетного фінансування покладається на Кабінет Міністрів України.

Інформаційні системи, технології та засоби їх забезпечення підлягають сертифікації у встановленому законом порядку, а організації, які виконують роботи в галузі проектування та виробництва засобів обробки і захисту інформації, мають одержати ліцензії на цей вид діяльності відповідно до чинного законодавства.

Стаття 18. Економічні взаємини в межах національного інформаційного простору України

Економічні взаємини між суб'єктами інформаційної діяльності, засади національного інформаційного простору України, пов'язані з інформаційними процесами в Україні, регулюються законами України.

Основними принципами економічних взаємин у національному інформаційному просторі є:

сприяння розвитку ринкових відносин в інформаційній сфері;

підтримка, заохочення інформаційної діяльності, спрямованої на реалізацію внутрішньої і зовнішньої політики України;

недопущення монопольної діяльності у національному інформаційному просторі;

задоволення гуманітарних потреб, духовно-культурних запитів суспільства;

відродження звичаїв і традицій, культурних і духовних надбань українського народу;

застосування конкурсного підходу до розробки та виробництва новітніх інформаційних технологій та систем;

захисту національного інформаційного простору від поширення інформаційної продукції низької якості, аморального і антигуманного змісту, розрахованої лише на здобуття прибутків та надприбутків, а також від переважання в інформаційних процесах, зокрема, в рекламі, продукції іноземного походження.

Інформаційний продукт та послуги відповідно до чинного законодавства є об'єктом права власності.

Інформаційний продукт та послуги установ, організацій, підприємств, окремих громадян, які здійснюють інформаційну діяльність у національному інформаційному просторі України, можуть бути товаром, який є об'єктом економічних відносин, якщо це не суперечить міжнародним договорам та чинному законодавству України.

Державний контроль економічної діяльності у національному інформаційному просторі України не може використовуватись як утручання у зміст

інформації та інформаційних процесів, які здійснюються відповідно до Конституції і законів України.

Розділ IV. ЗАХИСТ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Стаття 19. Зміст, предмет та об'єкти захисту

Держава забезпечує цілісність національного інформаційного простору України та захист у ньому:

державної таємниці, *а також інформації з обмеженим доступом, що є* об'єктом права власності держави або об'єктом лише володіння, користування чи розпорядження державою, інформаційних ресурсів виняткового державного значення;

інформаційних ресурсів, віднесених до національного надбання, державних та таких, що охороняються державою архівів, музейних фондів;

інформаційних ресурсів у цілому — від руйнування, розкрадання, спекуляції, поширення проти волі власника, несанкціонованого в установленому законом порядку транскордонного переміщення;

таємниці телефонних розмов і листування;

інформаційної інфраструктури та інформаційних процесів — від шкідливих наслідків індустріальної діяльності.

Національний інформаційний простір України охороняється державою від поширення в ньому:

інформації, яка містить заклики до повалення конституційного ладу насильницьким шляхом, розпалювання національної, расової, релігійної ворожнечі, посягання на права і свободи людини;

спотвореної та недостовірної інформації;

інформаційної продукції в якій пропагується жорстокість, насильство, порнографія, окультизм;

інформаційної продукції з небезпекою впливу на підсвідомість, особливо від інформації, поширюваної аудіовізуальними засобами масової інформації, через системи цифрових телекомунікаційних мереж типу Інтернет та інформаційних обмінів.

З метою захисту національного інформаційного простору України держава в порядку, встановленому законами України, переслідує за:

корисливе використання інформації посадовими особами, працівниками, які мають доступ до неї у зв'язку з виконанням своїх службових обов'язків;

незаконне підключення до телефонних і комп'ютерних мереж системи Інтернет та *інших і приховане використання телефонних номерів, засобів* комп'ютерного зв'язку, що перебувають у власності державних та недержавних організацій і приватних осіб, для отримання і поширення інформації та

встановлення за їхньою допомогою протиправного зв'язку з абонентами всередині країни і за рубежем;

використання засобів ведення інформаційної війни (комп'ютерних вірусів, "логічних бомб", генераторів електромагнітних імпульсів, пристроїв інформаційного впливу з автоматичним режимом ініціювання, засобів дистанційного знімання інформації з комп'ютерних мереж та перешкоджання інформаційним процесам у телекомунікаційних мережах тощо);

установлення монопольного контролю з боку іноземних громадян та контрольованих ними структур над каналами українського теле- і радіомовлення, іншими об'єктами інформаційної системи України;

порушення встановленого законодавством порядку охорони державної таємниці та інформації з обмеженим доступом.

Стаття 20. Обмеження щодо поширення інформаційної продукції

Спеціальними правилами (положеннями), які відповідно до законодавства затверджує Кабінет Міністрів України, обмежується поширення інформаційної продукції, не призначеної для дітей та юнацтва, і застосовуються засоби (символи) попередження про інформацію в глобальних комп'ютерних мережах, телевізійних та радіопередачах, які заборонені (небажані) для перегляду і прослуховування дітьми, людьми з певними хворобами та деякими іншими категоріями споживачів інформації.

Забороняється поширення інформаційної продукції порнографічного характеру.

Поширення інформаційної продукції еротичного характеру та продукції, що містить елементи насильства та жорстокості, дозволяються виключно за умови дотримання обмежень, встановлених законодавством.

Забороняються виробництво та розповсюдження інформаційної продукції, яка:

пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України;

пропагує фашизм та неофашизм;

принижує або ображає націю чи особистість за національною ознакою;

пропагує неповагу до національних і релігійних святинь;

принижує особистість, є проявом знущання з приводу фізичних вад (каліцтва), із душевнохворих, літніх людей;

пропагує невігластво, неповагу до батьків;

пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички.

Стаття 21. Організація, методи і засоби захисту інформаційного простору України

Організація захисту інформаційного простору України відповідно до її Конституції і законодавства покладається на відповідні центральні органи виконавчої влади, правосуддя, спеціалізовані організації забезпе-

чення контролю, охорони телерадіокомунікацій, радіочастотного ресурсу тощо.

Захист інформації, об'єктів національного інформаційного простору за виданими державою ліцензіями можуть здійснювати організації та установи недержавних форм власності.

Безліцензійна діяльність у сфері національного інформаційного простору забороняється.

Для захисту національного інформаційного простору застосовуються методи і засоби:

правового регулювання та контролю;

економічного (податкового, тарифного, митного, заохочувального тощо) регулювання та контролю;

державного ліцензування та сертифікації суб'єктів національного інформаційного простору України, об'єктів інформаційної інфраструктури;

упереджувальної та дипломатичної діяльності щодо запобігання інформаційно-пропагандистському втручанню у внутрішні справи країни;

технічного захисту;

криптографічного захисту, протидії засобам ведення інформаційної війни;

застосування дисциплінарної, цивільно-правової, адміністративної або кримінальної відповідальності за порушення, що містять загрозу інформаційній безпеці України, передбачені цим Законом, іншими законами України.

У випадках, передбачених законами України, контроль інформації, яка передається в межах єдиної національної системи зв'язку України, здійснюється Службою безпеки України.

Стаття 22. Порядок входження суб'єктів національного інформаційного простору України в глобальні інформаційно-комунікаційні мережі та системи

Входження суб'єктів національного інформаційного простору України в глобальні інформаційно-комунікаційні мережі та системи здійснюється згідно норм і правил, встановлених власником цих мереж і систем та відповідно до чинного законодавства України.

Держава заохочує входження суб'єктів національного інформаційного простору України в глобальні інформаційно-комунікаційні мережі та системи за умови дотримання вимог законів України щодо відповідності діяльності цих суб'єктів інтересам національної безпеки України, захисту прав людини.

Телекомунікаційний оператор (провайдер), який надає доступ до цифрових телекомунікаційних мереж типу Інтернет, зобов'язаний забезпечити:

можливість ідентифікації власної мережі та її технічну сумісність із національною (локальною) мережею;

параметри надійності та якості не нижче прийнятих у глобальній мережі;

необмежений і рівноправний доступ користувачів до всіх відкритих джерел інформації;

захист інформації від несанкціонованого доступу, видозмінення або руйнування її неавторизованими користувачами.

Відомості про власників інформації та про абонентів мережі надаються тільки на вимогу правоохоронних органів або за згодою самих власників та абонентів, відповідно до законодавства.

Відповідальність за поширення інформації, забороненої для поширення законами України, та відповідальність за її зміст у комп'ютерних мережах, несе власник цієї інформації.

У випадку встановлення факту поширення інформації, забороненої для поширення законами України, телекомунікаційна організація має право розірвати контракт із власником інформації, іншим відповідальним за це порушення клієнтом, в односторонньому порядку.

Стаття 23. Регулювання збору інформації на території України зарубіжними дослідниками та передача її за межі України

Правове становище і професійна діяльність зарубіжних дослідників (іноземних кореспондентів, інших представників іноземних засобів масової інформації і науковців) на території України регулюються законами України "Про інформацію", "Про державну таємницю", "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", "Про інформаційні агентства", іншими законами, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Законами, підзаконними актами Кабінету Міністрів України та міжнародними договорами, укладеними Україною та ратифікованими Верховною Радою України.

Не обмежується збір зарубіжними дослідниками на території України відкритої інформації.

Переміщення через кордон обмежується на підставі забезпечення інтересів національної безпеки, контролюється митними органами та органами охорони державної таємниці відповідно до законів України та підзаконних актів Кабінету Міністрів України.

Режим доступу акредитованих в Україні зарубіжних дослідників до національних інформаційних ресурсів України, зокрема, до правової, соціологічної, неопублікованої статистичної інформації визначається Кабінетом Міністрів України або уповноваженими ним центральними органами виконавчої влади на підставі законів України.

Стаття 24. Злочини в цифрових телекомунікаційних мережах типу Інтернет і організація боротьби з ними

Держава забезпечує, відповідно до Конституції та законів України, загальну системну охорону та захист інформації, запобігання, виявлення і припинення злочинів у цифрових телекомунікаційних мережах, застосування

адекватних норм відповідальності за ці злочини на основі вдосконалення правових засад боротьби зі злочинністю в цифрових телекомунікаційних мережах.

До злочинів у цифрових телекомунікаційних мережах типу Інтернет відносяться:

отримання грошей в електронних банківських системах взаєморозрахунків, власності або послуг шляхом прикриття фальшивими приводами і обіцянками чи видавання себе за іншу особу;

умисна зміна, перегляд, фальсифікація, пошкодження, знищення, несанкціоноване копіювання або викрадення машинної інформації (із банків даних і баз знань, систем математичного забезпечення), що міститься в автоматизованій комп'ютерній системі (мережі, комп'ютері), а також викрадення (розкрадання) машинного часу, системного і прикладного забезпечення, комп'ютерів, обчислювальних систем, мереж комп'ютерів;

незаконне використання комп'ютера з метою аналізу або моделювання злочинних дій для їх здійснення, в комп'ютерних системах (мережах);

шантаж, інформаційна блокада, саботаж та інші методи комп'ютерного тиску;

комп'ютерне шпигунство і передавання комп'ютерної інформації особам, які не мають права доступу до неї;

розроблення і розповсюдження комп'ютерних вірусів в інформаційно-обчислювальних системах та мережах;

умисне порушення зв'язку між комп'ютерами, інформаційно-обчислювальними системами та мережами;

недбалість при розробці та створенні інформаційно-обчислювальних систем і мереж, програмного та інформаційного забезпечення, що призводить до небажаних наслідків і втрати інформаційних ресурсів;

механічні, електричні, електромагнітні та інші види впливів на інформаційно-обчислювальні системи (мережі) та лінії телекомунікацій, що викликають їх пошкодження чи руйнування;

використання інших можливостей корисливого застосування автоматизованих комп'ютерних систем (мереж, комп'ютерів), які виникають у результаті сучасного розвитку науково-технічного прогресу.

Збереження конфіденційності інтересів фізичних та юридичних осіб, які стали жертвами комп'ютерних злочинів, гарантується відповідно до законів України.

Стаття 25. Судочинство у сфері інформаційної безпеки України

Відповідно до Конституції та законодавства України судочинство у сфері інформаційної безпеки України здійснюють суди загальної юрисдикції.

Вищою інстанцією в цьому судочинстві виступає підрозділ Верховного Суду України – Судова палата у цивільних справах.

Розділ V. КОНТРОЛЬ ЗА ДОТРИМАННЯМ ТА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ УКРАЇНИ

Стаття 26. Нагляд та контроль за дотриманням законодавства України про інформаційну безпеку України

Контроль за діяльністю органів державної влади і посадових осіб щодо виконання ними повноважень у сфері проведення державної інформаційної політики, забезпечення інформаційної безпеки України здійснює Верховна Рада України.

Нагляд та контроль за дотриманням законодавства України про інформаційний суверенітет та інформаційну безпеку України здійснюють органи виконавчої влади в порядку, визначеному Кабінетом Міністрів України, на підставі законів України.

Регулювання, нагляд і контроль здійснюються виключно з метою:

підтримки, заохочення інформаційної діяльності, спрямованої на реалізацію внутрішньої і зовнішньої політики України;

задоволення гуманітарних потреб, духовно-культурних запитів суспільства;

відродження звичаїв і традицій, культурних і духовних надбань українського народу;

захисту національного інформаційного простору від поширення інформаційної продукції низької якості, аморального і антигуманного змісту, розрахованої лише на здобуття прибутків та надприбутків, а також від переважання в інформаційних процесах, зокрема, в рекламі, продукції іноземного походження.

Координація діяльності органів виконавчої влади щодо регулювання, нагляду і контролю за дотриманням законодавства України про інформаційну безпеку України покладається на Раду національної безпеки і оборони України.

Державний контроль діяльності в національному інформаційному просторі України не може використовуватись як утручання у зміст інформації та інформаційних процесів, які здійснюються відповідно до Конституції і законів України.

Стаття 27. Суб'єкти відповідальності

Суб'єктами відповідальності є фізичні та юридичні особи України, фізичні та юридичні особи іноземних держав, особи без громадянства, що ведуть інформаційну діяльність на території України і допустили порушення цього Закону, відповідних норм інших законодавчих актів, перелічених у статті 9 цього Закону.

Стаття 28. Відповідальність за порушення законодавства про інформаційну безпеку України

Порушення законодавства про інформаційну безпеку України тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність відповідно до законів України.

Розділ VI. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон уводиться в дію з часу офіційного опублікування.

2. До приведення інших законодавчих актів відповідно до цього Закону вони застосовуються і діють у частині, що не суперечить йому.

3. Кабінетові Міністрів України у тримісячний термін після набрання чинності цим Законом привести відповідно до нього свої нормативно – правові акти та забезпечити перегляд відомчих нормативних актів, внести на розгляд Верховної Ради України протягом трьох місяців після набрання чинності цим Законом проекти законів про внесення змін до відповідних законів із метою узгодження їх з цим Законом.

УГОДА

між Урядом України та Урядом Французької Республіки про взаємну охорону таємної інформації та матеріалів

Прийнята 7 грудня 1999 р.

Уряд України (Кабінет Міністрів України) та Уряд Французької Республіки (далі – Сторони), бажаючи забезпечити охорону всієї таємної інформації та матеріалів, якими Сторони обмінюються в рамках угод про співробітництво, укладених або тих, що готуються до підписання, а також в рамках тендерів, контрактів чи замовлень організацій держав Сторін незалежно від їх форми власності, прагнучи розробити правила охорони такої таємної інформації та матеріалів, погодилися про таке:

Стаття 1

У цій Угоді терміни вживаються у такому значенні:

1) «таємна інформація та матеріали» — інформація та матеріали будь-якого характеру, яким був присвоєний ступінь секретності, зазначений у статті 5 цієї Угоди, і які в інтересах національної безпеки відповідно до національного законодавства Сторін підлягають охороні від одного з таких випадків:

- компрометації, знищення, нецільового використання, крадежу, розголошення або втрати таємної інформації та матеріалів;
- доступу до такої таємної інформації та матеріалів будь-якої особи, що не має допуску;

2) «таємна інформація» — будь-яка інформація, зміст якої є таємним, незалежно від форми, у якій вона подана, та способу її передачі;

3) «таємні матеріали» — будь-які носії інформації, незалежно від їх виду, зокрема будь-який документ або виріб, на/в яких таємна інформація записана чи поміщена, не порушуючи їх фізичних ознак;

4) «Сторона-одержувач» – Сторона, якій передається таємна інформація та/або матеріали відправником;

5) «Сторона-джерело» — Сторона, яка надає або передає таємну інформацію та матеріали;

6) «користувач» — фізична або юридична особа, яка відповідає за виконання вимог, обумовлених контрактом або замовленням, і яка була перевірена з точки зору забезпечення охорони при поводженні з переданою таємною інформацією та матеріалами певного ступеня секретності, в розпорядженні якої є адекватні засоби забезпечення охорони таємної інформації та матеріалів відповідно до їх ступеня секретності;

7) «запитувач» — Сторона або організація, уповноважена нею, яка робить запит щодо отримання таємної інформації та матеріалів;

8) «організація» — будь-яка організація незалежно від форми власності, де обробляється, зберігається і охороняється таємна інформація та матеріали;

9) «третя сторона» — уряди держав, які не визначені цією Угодою як «Сторони», а також громадяни або юридичні особи цих держав;

10) «відправник» — фізична або юридична особа, яка є джерелом таємної інформації та матеріалів;

11) «компетентний орган» — державний орган, уповноважений Стороною.

Стаття 2

1. Сторони у відповідності зі своїм національним законодавством вживають необхідних заходів щодо охорони таємної інформації та матеріалів, які надаються іншою Стороною під час виконання цієї Угоди, та гарантують таку саму охорону одержаної таємної інформації та матеріалів, як і власної таємної інформації та матеріалів з еквівалентним ступенем секретності відповідно до пункту 1 статті 5 цієї Угоди.

2. Сторони надаватимуть доступ третій стороні до таємної інформації та матеріалів тільки після попередньої письмової згоди Сторони-джерела.

3. Сторони зобов'язуються забезпечити на території своїх держав необхідні перевірки заходів охорони та дотримання правил охорони таємної інформації та матеріалів.

Стаття 3

1. Державними органами, відповідальними за виконання цієї Угоди, є:

- в Україні — Служба безпеки України;
- у Франції — Генеральний секретаріат національної оборони.

Стаття 4

Доступ до таємної інформації та матеріалів обмежується виключно колом осіб, службові обов'язки яких вимагають від них доступу до цієї таємної інформації та матеріалів на підставі необхідності ознайомлення з ними і яким надано компетентними органами допуск і дозвіл.

Стаття 5

1. Сторони, враховуючи вимоги щодо охорони таємної інформації та матеріалів, передбачені їх відповідним національним законодавством та нормативними актами, зобов'язуються забезпечити охорону таємної інформації та матеріалів, обмін якими здійснюється під час дії цієї Угоди, і погоджуються на еквівалентність ступенів секретності, зазначених у нижченаведеній таблиці:

УкраїнаФранціяЦілком таємноSecret defenseТаємноConfidentiel defense

2. Кожна із Сторін зобов'язується після отримання таємної інформації та матеріалів від іншої Сторони надати їм власні національні грифи секретності на основі визначених у вищенаведеній таблиці еквівалентів.

3. Інформація та матеріали, які спільно розроблені обома Сторонами та підлягають охороні, називаються «міждержавними секретами». Відповідальні органи визначені у статті 3, за взаємною згодою визначають ступінь секретності такої інформації та матеріалів з урахуванням таблиці еквівалентів, наведеної у пункті 1 цієї статті. Стосовно цього типу інформації та матеріалів, які спільно розроблені та підлягають охороні, вони разом вирішують питання про розсекречування або зміну ступенів секретності.

4. Сторони здійснюватимуть взаємне інформування про будь-яку подальшу зміну ступенів секретності переданої таємної інформації та матеріалів.

5. Сторони здійснюватимуть взаємне інформування про будь-яку подальшу законодавчу або нормативну зміну, що стосується режиму секретності.

Стаття 6

З метою досягнення відповідності еквівалентним вимогам щодо охорони таємної інформації та матеріалів та її підтримання кожна Сторона після звернення іншої Сторони передасть останній інформацію щодо своїх правил, методик та практики, що склалася, у сфері охорони таємної інформації та матеріалів і сприятиме, з цією метою, контактам з відповідальним органом іншої Сторони.

Стаття 7

1. Таємна інформація та матеріали передаються іншій Стороні дипломатичним чи військовим шляхом.

2. Сторони можуть домовитися за взаємною згодою про те, що таємна інформація та матеріали можуть передаватися іншим шляхом, крім дипломатичного чи військового, якщо використання цих шляхів передачі виявиться непридатним або складним.

3. Сторона-одержувач підтверджує отримання таємної інформації та матеріалів та передає їх користувачу згідно з його визначенням у статті 1, відповідно до національного законодавства у сфері охорони таємної інформації та матеріалів.

Стаття 8

1. Кожна Сторона повідомляє організаціям своєї держави про наявність цієї Угоди, коли таємна інформація та матеріали їх стосуються.

2. Кожна Сторона зобов'язується забезпечити, щоб всі організації, які отримують таємну інформацію та матеріали, дотримувалися належним чином положень цієї Угоди.

3. Відповідальні органи кожної з Сторін розробляють і розсилають до організацій своїх держав інструкції і правила щодо порядку охорони таємної інформації та матеріалів.

Стаття 9

1. Доступ до таємної інформації та матеріалів і місць, де здійснюються секретні роботи, надається однією Стороною громадянину держави іншої Сторони за умови наявності попереднього дозволу компетентного органу Сторони, що приймає.

2. Дозвіл, зазначений у пункті 1 цієї статті, надається тільки на підставі заявок на візити громадянам, які мають допуск належного рівня відповідно до ступеня секретності робіт та повноваження щодо роботи з таємною інформацією та матеріалами (далі – відвідувачі).

3. Компетентний орган Сторони, що направляє, повідомляє прізвища відвідувачів компетентному органу Сторони, що приймає, щонайменше за 20 днів до запропонованої дати візиту. У випадку особливої потреби дозвіл на візит, зазначений у пункті 1 цієї статті, надається Сторонами у найкоротші терміни.

4. Заявки на візити оформляються відповідно до процедури Сторони, що приймає, і містять, як мінімум, інформацію, передбачену додатком, який є невід'ємною частиною цієї Угоди.

5. За згодою обох Сторін для будь-яких робіт, програм або окремого контракту можуть складатися списки регулярних відвідувачів, які попередньо узгоджуються з компетентними органами. Ці списки початкове чинні протягом дванадцяти місяців з можливим подальшим продовженням за згодою компетентних органів на додаткові періоди, але не більше дванадцяти місяців. Зазначені списки повинні складатися і подаватися відповідно до чинних положень, визначених Стороною, що приймає.

Оформлення візитів осіб, прізвища яких зазначені в списку, після затвердження списку здійснюється безпосередньо у відповідних організаціях.

6. Відвідувачі повинні поводитися з таємною інформацією та матеріалами, які можуть бути їм надані або про які вони можуть дізнатися під час візиту, у відповідності з положеннями цієї Угоди.

Стаття 10

1. У разі передачі таємної інформації та матеріалів однією Стороною для користувачів іншої Сторони Сторона-одержувач зобов'язана, по відношенню до користувача:

- впевнитися в тому, що на їхніх об'єктах можливо належним чином здійснювати охорону таємної інформації та матеріалів;
- надати їм дозвіл (ліцензію) необхідного рівня на право роботи з таємною інформацією та матеріалами;
- оформити допуск необхідного рівня особам, службові обов'язки яких потребують доступу до цієї таємної інформації та матеріалів;
- впевнитися в тому, що всі особи, які мають доступ до цієї таємної інформації та матеріалів, ознайомлені з нормами про їх відповідальність за охорону таємної інформації та матеріалів відповідно до чинного законодавства;
- здійснювати регулярні перевірки режиму секретності на їхніх об'єктах.

2. До будь-якого контракту, у тому числі на здійснення субпідрядних робіт, пов'язаного з таємною інформацією та матеріалами, складається додаток щодо охорони таємної інформації та матеріалів. У цьому додатку відправник зазначає таємну інформацію та матеріали, які підлягають захисту з боку Сторони-одержувача, а також присвоєні їм відповідні ступені секретності. Тільки відправник може змінювати ступінь секретності таємної інформації та матеріалів, зазначених у додатку щодо таємної інформації та матеріалів.

Стаття 11

1. У разі компрометації, знищення, нецільового використання, крадежу, недозволеного копіювання, розголошення, дійсної чи ймовірної втрати таємної інформації та матеріалів Сторона, якій вони були надані, проводить розслідування та вживає всіх відповідних заходів згідно з її національним законодавством та невідкладно повідомляє відправника про ці факти, вжиті заходи та результати розслідування.

2. Зазначене у пункті 1 цієї статті повідомлення повинно бути достатньо докладним для того, щоб відправник міг приступити до повного визначення збитків.

Стаття 12

1. Будь-яке спірне питання щодо тлумачення або застосування передбачених цією Угодою заходів вирішується шляхом переговорів між представниками обох Сторін.

2. Під час вирішення спірного питання обидві Сторони продовжують дотримуватися своїх зобов'язань, визначених цією Угодою.

Стаття 13

Кожна Сторона, в межах своїх фінансових ресурсів, бере на себе всі витрати, пов'язані з впровадженням цієї Угоди та застосуванням її положень.

Стаття 14

1. Ця Угода набирає чинності з дати отримання Сторонами останнього повідомлення про виконання ними внутрішньодержавних процедур, необхідних для набрання нею чинності.

З цього моменту її положення розповсюджуються також на таємну інформацію та матеріали, обмін якими відбувся до набуття чинності цією Угодою.

2. Ця Угода в будь-який час може бути доповнена або змінена за письмовою згодою обох Сторін. Доповнення та зміни до тексту цієї Угоди набирають чинності в такому ж порядку, як і сама Угода.

3. Ця Угода укладається на невизначений термін та залишається чинною до моменту письмового повідомлення однієї з Сторін про свій намір припинити її дію.

4. Уразі припинення дії цієї Угоди Сторони зобов'язуються спільно визначити таємну інформацію та матеріали, якими вони обмінялися або які вони отримали, на які розповсюджуються у подальшому вимоги режиму секретності.

Стаття 15

На підтвердження вищенаведеного особи, уповноважені Урядом України та Урядом Французької Республіки, підписали цю Угоду та скріпили її печатками.

ІНФОРМАЦІЯ ПРО АВТОРІВ

Бахтіяров О.Г. – кандидат філософських наук, Генеральний директор Центру психологічних та соціальних технологій

Білоусова Н.Б. – кандидат фізико-математичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Богуш Д.А. – Президент Центру дослідження маніпулятивних технологій, генеральний директор Агентства Інтерактив PR Груп

Валевська І.А. – кандидат філософських наук, доцент кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Головченко В.І. – доктор політичних наук, професор кафедри країнознавства Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Гондюл В.П. – завідувач відділення міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка, професор, кандидат технічних наук

Гуцал А.Ф. – перший заступник директора Національного інституту проблем міжнародної безпеки при РНБОУ, доцент кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Даниленко С.І. – кандидат філологічних наук, доцент кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Запорожець О.Ю. – кандидат політичних наук, молодший науковий співробітник кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Зернецька О.В. – доктор політичних наук, провідний науковий співробітник відділу глобалістики, геополітики та геоекономіки Інституту світової економіки і міжнародних відносин НАН України, лауреат Премії імені академіка М.В.Птухи НАН України, член Міжнародної асоціації медіа- та комунікаційних досліджень

Іванов В.Ф. – доктор філологічних наук, професор, завідувач кафедри реклами та зв'язків з громадськістю Інституту журналістики Київського національного університету імені Тараса Шевченка

Камінський Є.Є. – доктор історичних наук, професор, завідувач відділу трансатлантичних відносин Інституту світової економіки і міжнародних відносин НАН України

Кучмій О.П. – кандидат політичних наук, молодший науковий співробітник кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Литвиненко О.В. – доктор політичних наук, керівник департаменту апарату Ради національної безпеки і оборони України

Макаренко Є.А. – доктор політичних наук, професор, завідувач кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Недбаєвський С.Л. – Державний експерт відділу інформаційної безпеки та міжнародних інформаційних відносин Національного інституту проблем міжнародної безпеки при РНБОУ

Ожеван М.А. – доктор філософських наук, професор, завідувач відділу інформаційної безпеки та міжнародних інформаційних відносин Національного інституту проблем міжнародної безпеки при РНБОУ

Панченко Ж.О. – кандидат політичних наук, асистент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Піскорська Г.А. – кандидат історичних наук, старший науковий співробітник кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Рижков М.М. – кандидат історичних наук, доцент кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Романенко Ю.В. – доктор соціологічних наук, доцент кафедри міжнародних комунікацій і зв'язків з громадськістю Інституту міжнародних відносин Київського Національного університету імені Тараса Шевченка

Сербіна Н. Ф. – кандидат історичних наук, доцент кафедри країнознавства Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Солонська С.А. – директор Інституту політичного консалтингу

Тихомирова Є.Б. – доктор політичних наук, завідувач кафедри міжнародної інформації Рівненського інституту слов'янознавства Київського славістичного університету

Толстов С.В. – кандидат історичних наук, провідний науковий співробітник Інституту світової економіки і міжнародних відносин НАН України

Фролова О.М. – кандидат політичних наук, асистент кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Швець О.В. – кандидат політичних наук, науковий співробітник кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Шевченко О. В. – кандидат політичних наук, доцент кафедри міжнародних комунікацій та зв'язків з громадськістю Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Яковець А.В. – кандидат філологічних наук, доцент факультету соціальних наук і соціальних технологій НаУКМА

Коонтактна інформація:
тел: 481-44-69.

ЛІТЕРАТУРА

1. Goodby J.E. Europe Undivided. The NewLogic of U.S. – Russian Relations. – Pub. by US Inst. of Peace, 1998. – P. 4-5.
2. Kissinger H.A. Diplomacy. – N.Y.: Pub. by DIANE Pub. Company, 1994. – 909 p.
3. Brzezinski Zb. The Graund Chessboard. American Primacy and Its Geostrategic Imperatives. Basic Books A Division of Harper Collins Publisher. – 254 p.
4. Mearsmeiher J. Back to the future. //International Security. – (Summer), 1990.
5. Nye J.S., Owens W.Jr. America's Informational edgel Strategy and force planning /Faculty, National Security Decision Making Department, Naval War College. – 460 p.
6. Berkowitz B.D. Warfare in information Age //Strategy and force planning Faculty, National Security Decision Making Department, Naval War College. /Lloyd R.M., course director; Bartlett H.C. et all. 2nd ed. – P. 465-477.
7. Johnson I.S. F Major Intelligence Challenge. Toward a Functional Model of Informa-tion Warfare. http://www.odci.gov/csi/studies/97unclas/warfare.html.
8. Joshi A. The Information Revolution and National Power: Political Aspects. //Strategic Analysis. – 1999. – Vol. XXIII. – N 6. – P. 1005-1028.
9. Buzan B. From international system tointernational society: Structural realism and regim theory meet the English school /International Organisation HZ, – 1993. – 64 p.
10. Libicky M.C. What is information Warfare? – Wash. NDU, 1995. – 59 p. – http://www.ndu.edu/ogi-bir/wais.pe.
11. Hirschman A.O. Deux siecles de rhethorique reactionnaire. – Fayard, Paris, 1992. – P. 23-29.
12. Lasswell H. Propaganda technology in the World War. – N.Y., 1927. – P. 64.
13. Huntington S.P. The Clash of Civilization? //Foreign Affaries. – 1993 (Summer).
14. Плетт В. Стратегическая разведка. Основные принципы.– М.: Изд. дом "Форум", 1997. – 376 с.
15. Аннан К. Обновление на переходном этапе. Годовой доклад о работе Организации. – Нью-Йорк:ООН, 1997. – 69 с.
16. Галі Б. Порядок денний для миру. Превентивна дипломатія, миротворчість і підтримання миру. Нью-Йорк: ООН, 1992. – 500 с.

17. Ланцов С. Мировая политика и международные отношения. СПб.: Издательство В.А. Михайлова, 2000. – 60 с.
18. Цыганков П. Международные отношения: социологические подходы. – М., 1998. – 356 с.
19. Крутских А., Федоров А. О международной информационной безопасности // Международная жизнь. – 2000. – № 2. – С. 37-48.
20. Лебедева М. Политическое урегулирование конфликтов. – М.: Аспект Пресс, 1999.– 268 с.
21. Камінський Є., Несук М. Україна в зарубіжних доктринах і стратегіях XX століття //Політична думка. – 1995. – № 2-3.
22. Ніколаенко І. Проблема міжнародної безпеки і діяльність політичних партій. ООН і майбутні покоління. К.: "Логос", 1996. – 192 с.
23. Бруз В. ООН і врегулювання міжнародних конфліктів. – К.: Либідь, 1995. – 110 с.
24. Ожеван М. Перед викликами глобального тероризму: нова роль масмедіа – http://www.nisp.gov.ua/
25. Толстов С. Глобалізація і геополітичні зміни сучасного середовища міжнародної безпеки // Глобалізація і безпека розвитку. Монографія. /Білорус О.Г., Лук'яненко Д.Г. та ін. – К.: КНЕУ, 2001. – С. 103-195.
26. Перепелица Г.Н. Прогнозирование военно-политического конфликта. //Военно-политические конфликты: методология исследования и урегулирования. – К.: Институт государства и права имени Корецкого НАН Украины, 1996. – С. 10-15.
27. Resolution adopted by the General Assembly UN [on the report of the First Committee (A/53/576)] "Development in the field of information and telecommunication in the context of information security". – Distr. General A/RES/53/70, 4 January, 1999, N.Y.
28. Галі Б. Порядок денний для миру. Превентивна дипломатія, миротворчість і підтримання миру. Нью-Йорк: ООН, 1992. – 500 с.
29. Крутских А. Информационный вызов безопасности на рубеже XXI века //Международная жизнь, 1999. – № 2. – С. 82-89.
30. Nye J.S., Owens W.Jr. America's Informational edgel Strategy and force planning. – http://www.infowar.com/
31. The Balkan Conflict: Stabilization Force (SFOR) – http://www.cybercom.ul
32. Егорова Е. США в международных кризисах.// Вашингтон: психологические аспекты принятия внешнеполитических решений. – М.: МГУ, 1988. – С. 50-57.
33. Уайт Д. Модель інформаційної війни в операції "Помста". – http://www.whitehouse.gov

34. Bigo D. The European international security ficed: shakes and rivalries in a newly developing area of police intervention //Malcolm Andersou L Monica Deu Baer. – Pinter Publication, 1994. – 241 p.
35. The Balkan Conflict: Stabilization Force (SFOR) – http://www.cyber-com.ul
36. Бахтияров О. Информационные технологии: введение в психонетику. – К.: ЕКСПИР, 1997. – 160 с.
37. Резолюция ГА ООН A/RES/42/93 "Всеобъемлющая система мира и безопасности" (1987) – http://daccessdds.un.org
38. Резолюция ГА ООН A/RES/42/93 "Укрепление международном мира, безопасности и международного сотрудничества во всех его аспектах в соответствии с Уставом ООН" (1989) – http://daccessdds.un.org
39. Резолюция ГА ООН A/RES/53/73 "Роль науки и техники в контексте международной безопасности и разоружения" – http://daccessdds.un.org
40. Резолюция ГА ООН A/RES/53/70 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности"
41. Технологический прогресс и своевременные международные отношения. – М.: Просвещение, 2004.– С.448.
42. Резолюция ГА ООН A/RES/54/49 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" –
43. Крутских А.В. Война и мир: международные аспекти информационной безопасности// Международная жизнь, 2000. –№2.– С.37-48.
44. Доклад Генерального секретаря A/55/140 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" – http://www.iss-eu.org
45. Резолюция ГА ООН A/RES/55/28 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" – http://www.iss-eu.org
46. Резолюция ГА ООН A/RES/56/19 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" – http://www.iss-eu.org
47. Резолюция ГА ООН A/RES/56/121 "Борьба с преступным использованием информационных технологий" – http://www.iss-eu.org
48. Супертерроризм: новый вызов нового века. Под редакцией А.В. Фёдорова.– М.: Права человека, 2002.– С.262; 2.
49. Information security. A new challenge for the EU. Chaillot Paper №76, March, 2005 – http://www.iss-eu.org
50. Резолюция ГА ООН A/RES/57/53 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности". –htth://www.iss-eu.org

51. Резолюция ГА ООН A/RES/57/239 "Создание глобальной культуры кибербезопасности" – http://www.iss-eu.org
52. Резолюция ГА ООН A/RES/57/27 "Меры по ликвидации международного терроризма". – http://www.iss-eu.org
53. Доклад Генерального секретаря на 60-й сессии ГА ООН A/60/202 –
54. Панарин М.Н. Информационная война и дипломатия. – М.: 2004. – С. 528
55. Резолюция ГА ООН A/RES/60/45 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" –
56. Резолюция ГА ООН A/RES/60/51 "Роль науки и техники в контексте международной безопасности и разоружения" – http://www.iss-eu.org
57. Резолюция ГА ООН A/61/55 "Роль науки и техники в контексте международной безопасности и разоружения" .-http://www.iss-eu.org
58. Доклад Генерального секретаря на 61-й сессии ГА ООН A/61/161 –
59. Макаренко Є.А. Міжнародні інформаційні відносини.– К.: ННК, 2002. – 474с.
60. Журавський В., Родіонов М., Жиляєв І. Під редакцією М. Згуровського. Україна на шляху до інформаційного суспільства.–– К.: 2004, – 481с.
61. Закон України „Про національну систему конфіденційного зв'язку" (2002) // Законодавство України – http://zakon.rada.gov.ua
62. Закон України „Про державну таємницю" (1994) // Законодавство України – http://zakon.rada.gov.ua
63. Закон України „Про захист інформації в автоматизованих системах" (1994) // Законодавство України – http://zakon.rada.gov.ua
64. Закон України „Про концепцію технічного захисту інформації в Україні" (1997) // Законодавство України – http://zakon.rada.gov.ua
65. Закон України „Про телекомунікації" (2004) // Законодавство України – http://zakon.rada.gov.ua
66. Закон України „Про першочергові завдання щодо впровадження новітніх ІКТ-технологій" (2005) // Законодавство України – http://zakon.rada.gov.ua
67. Указ Президент України підписав „Про цільовий план Україна – НАТО на 2006 р. у рамках Плану дій Україна – НАТО" // Законодавство України – http://zakon.rada.gov.ua
68. Розпорядження Кабінету Міністрів України „" (2006) // Законодавство України – http://zakon.rada.gov.ua
69. Гондюл В.П. Методологічні засади аналізу та прогнозування міжнародних відносин і міжнародних політичних конфліктів на зламі тисячоліть.// Актуальні проблеми міжнародних відносин. Збірник наукових праць.

Випуск 27 (частина 1). – К.: Київський національний університет імені Тараса Шевченка, Інститут міжнародних відносин, 2001.– С. 3 – 28.

70. Гондюл В.П. Методологія політичного аналізу та прогнозування міжнародних відносин і міжнародних політичних конфліктів. Вісник Київського національного університету імені Тараса Шевченка. Філософія. Політологія. Випуски 42 – 45. – К.: ВПЦ "Київський університет", 2002. – С. 248 – 254.
71. Гондюл В.П. Чинники, що визначають умови та причини виникнення й ескалації міжнародних політичних конфліктів.// Актуальні проблеми міжнародних відносин. Збірник наукових праць. Випуск 30 (частина 1). – К.: Київський національний університет імені Тараса Шевченка, Інститут міжнародних відносин, 2001. – С. 26 – 34.
72. Гондюл В.П. Моделі відображення станів держави при аналізі міжнародних відносин. – Науковий вісник дипломатичної Академії України. Випуск 7. – К.: 2002. – С. 37 – 46.
73. Гондюл В.П. Цикли в моделюванні та прогнозуванні криз і конфліктів у міжнародних відносинах. //Актуальні проблеми міжнародних відносин. Збірник наукових праць. Випуск 31 (частина 1). – К.: Київський національний університет імені Тараса Шевченка, Інститут міжнародних відносин, 2002. – С. 3 – 18.
74. Гондюл В.П. Моделі взаємодії Україна – НАТО. Матеріали інтерактивного семінару "Як набути статусу країни – члена НАТО: досвід посткомуністичних країн та можливості його застосування в Україні", Київ, 30 травня 2002 р. – К.: //Науковий журнал "Економічний часопис XXI", №№ 7 – 8, 2002. – С.29 – 31.
75. Яковец Ю.В. Циклы. Кризисы. Прогнозы. – М.: Наука, 1999. – 448 с.
76. Светлов В.А. Аналитика конфликта.–- СПб.: ООО "Росток", 2001. – 512 с.
77. Цыганков П.А. Международные отношения.– М.: Новая школа, 1996. –320 с.
78. Глухова А.В. Политические конфликты. – М.: Эдиториал УРСС, 2000. – 280 с.
79. Лебедева М.М. Политическое урегулирование конфликтов. Подходы, решения, технологии. – М.Аспект Пресс, 1997. – 272 с.
80. Лисицин Е.М. Генезис та еволюція концепцій і стратегій глобального і регіонального розвитку // Глобальні трансформації і стратегії розвитку. Під. Ред.О.Г.Білоруса. – К.: Віпол, 1998.- С. 35.
81. Белов А. Информационная сфера национальной безопасности // Зеркало недели. – 4 сент. 1999 г. – С. 6.
82. Зернецька О.В. Глобальна комунікаційна політика і демократичний розвиток // Дослідження світової політики: Зб. Наук. пр. Інституту світової

економіки і міжнародних відносин НАН України. – К., 2000. Вип. 9. – С. 3 – 9.

83. Білорус О.Г., Зернецька О.В. Право на комунікацію // Віче. – 2000. — № 2. – С. 115-132.
84. Панкратова Н.Д. Тенденции и проблемы развития системного анализа как научной дисциплины // Сучасні інформаційні технології та системний аналіз – шлях до інформаційного суспільства: Ювілейний зб. наук. пр. – К.: ІПСА Мін. освіти та НАН України при Національному технічному університеті України "Київський політехнічний інститут", 1998.– С. 10.
85. Зернецька О.В. Нове "диджитальне" диво. Нові глобальні тенденції в інформаційно-комунікаційному секторі світової економіки // Політика і час, 2002. –№ 12. – С. 34 -40.
86. Зернецька О.В. Глобальний розвиток систем масової комунікації і міжнародні відносини. – К.: Освіта, 1999. – С. 151- 160.
87. Mowlana H. Political and Social Implications of Communication Satellite Applications in Developed and Developing Countries / Pelton J.N. and Marcellus S.S. Economic and Police Problems in Satellite Communications. – New York: Praeger, 1977. — P. 124-142;
88. Communication Yearbook. Vol. 1. Ed. by B.D. Ruben. – New York: Brunswick. N.J.: Transaction Books, 1977. —P. 427 – 428.
89. Rothkopf D. In Prise of Cultural Imperialism? // Foreign Policy, 1997, № 107, Summer. – P. 39.
90. Лисицин Е.М. Питання теорії міжнродних конфліктів, національної і міжнародної безпеки / /Глобальні трансформації і стратегії розвитку. – К.: Віпол, 1999. – С. 41-49.
91. D'Arcy J. The Right to Communicate: Studies of the MacBride Commission. CIC-Paper № 36. – UNESCO: Paris, 1979. — P. 14.
92. Nordenstreng K., Gonzales-Manet E., Kleinwaechter W. New International Information and Communication Order. — 1998, Prague.
93. Towards a World-Wide Information Society // Media Development, 1996. – № 2. – P. 9.
94. Панкратова Н.Д., Курилин Б.И. Концептуальные основы системного анализа рисков в динамике управления безопасностью сложных систем // Проблемы управления и автоматики, 2000. — № 6. — С.110-132.
95. Borrus A. On-line Privacy: Congress Has no Time to Waste // BusinessWeek, September 18, 2000. — P. 35.
96. Microsoft: Now, Privacy Concerns // BusinessWeek, July 2, 2001.- P. 64.
97. Тейлор К. Сетевые шпионы // Столичные новости, 1-7 ноября 2002. – С. 13.

98. Чанфанелли Р. Интернет по-иракски // Столичные новости, 1-7 ноября 2002.– С. 13.

99. Feist S. Bad of the Board // Time, Feb.26, 2001. – P. 51 – 52; Levy S. Courting a Crypto Win // Newsweek, Vay 17, 1999. – P. 79.

100. Kuttner R. Verzion's Crash Couse in High-Tech Unionsm // BusinessWeek, September 11, 2000. — P. 2.

101. Зернецька О.В. "Битва розкруток", і не тільки. Британські вибори-2001 в умовах інформаційної доби // Віче, 2002. – № 4. – С. 12 – 16.

102. Слепынин О. Компьютерное бешенство //Зеркало недели, 25 мая 2002. – С. 15.

103. Кичева Е., Сорокин П. Любитель женских пальчиков // Аргументы и факты в Украине, 2001. – № 27. – С. 10.

104. В Греции запрещены компьютерные игры // Зеркало недели, 7 сент. 2002. — С. 11.

105. Владимирская А., Побережный М. Женщина в сетях // Зеркало недели. – 3 февр. 2001. — С. 20.

106. Приходько О. // Зеркало недели, 3 февр. 2001. — С. 20.

107. Глобалізація і безпека розвитку / Монографія. / Білорус О.Г. та ін. – К.: КНЕУ, 2001. – 733 с.

108. Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы. – М.: Логос, 2000. – 304 с.

109. Макаренко Є. А. Міжнародні інформаційні відносини. – К.: Наша культура і наука, 2002. – 452 с.

110. Макаренко Є.А. Європейська інформаційна політика. – К.: Наша культура і наука, 2000. – 368 с.

111. Правове регулювання інформаційної діяльності в Україні: Станом на 1 січня 2001 р. / Упоряд. С.Е. Демський; Відп. ред. С.П. Павлюк. – К.: Юрінком Інтер, 2001. – 688 с.

112. Указ Президента України "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні". – http://president.gov.ua

113. Литвиненко О.В. Інформаційні впливи та операції: Теоретико-аналітичні нариси. – К.: НІДС, 2003. – 240 с.

114. Яковлев Н. ЦРУ против СССР. – М : Политиздат. – 1983. – С. 78.

115. Конопатов С.Н., Юдин В.В. Традиционный смысл понятия «война» устарел // Воен. мысль. – 2001. – № 1. — С. 53-57.

116. Токов Е., Касюк А. Психологические операции ВС США в войнах и конфликтах 20 века // Зарубеж. воен. обозр. — 1997. — .№ 6.- С. 12–17.

117. Остерманн К. США и события 17 июня 1953 года в ГДР // Вопр. истории. – 1999. – № 11-12. –С. 19 – 66.

118. Пашко В. Психологические операции многонациональных сил в Северном Ираке // Зарубеж. воен. обозр. — 1995.– № 7. — С. 12-14.

119. Psychological operations in support of operations "Restore hope, 12/9/92 -5/4/93. – Washington: Unified Task Force Somalia, 1993.

120. Михайлов Б. Психологические операции вооруженных сил США в конфликтах низкой интенсивности // Зарубеж. воен. обозр. –1996.- № 8. — С. 2-8.

121. Егоров А. Информационно – психологическое обеспечение операции ООН в Сомали // Зарубеж. воен. обозр. — 1995.–№ 12. — С. 9-12.

122. Соколов В. Он победил СССР без оружия. Бывший лидер боевиков «Саюдиса» и министр обороны Литвы, бывший заключенный Аудрюс Буткявичюс не знает, кто в январе 1991 года стрелял в мирное население с вильнюсской телебашни // НГ. –2000. –4 авг. — С. 7.

123. Широнин В. КГБ против ЦРУ. -–М.: Палея, 1999. — 425 с.

124. Шарп Дж. От диктатуры до демократии: концептуальные основы освобождения.

125. Знаменский А. Успехи оперативной группы «Орел» // НВО. — 1996. – № 9. — С. 2.

126. The Balkan Conflict: Stabilization Force (SFOR.) // . Profiles in Peace //www.pathway.net

127. Путилов С. Война в эфире продолжается // НВО. — 1997. — № 22 – С. 8.

128. Бондаренко А. Циклические трансформации нашей «информации» // НВО. —1996. – 10 окт.

129. Заграничный П. Центральная Азия — накануне лета // Новости Центральной Азии и Кавказа. — 2000. — № 16. — С. 9.

130. Жуков В. Информационное обеспечение военных операций в ВС США и ОВС НАТО // Зарубеж. воен. обозр.– 2000. – № 4. — С. 2-6.

131. Большаков М. Подготовка кадров для служб психологических операций и по работе с гражданским населением в США // Зарубеж. воен. обозр. – 1998. – № 3. — С. 9-10.

132. Павлов Н. К. Германские политические фонды // Полис. — 1999.

133. Кияк Т. Інформаційне суспільство XXI ст.: Аналіт. мат. / НІСД. — К., 2000. – 15 с.

134. Пашко В. Силы специальных операций вооруженных сил Индии // Зарубеж. воен. обозр. — 1995. — № 6. — С. 5—7.

135. Joshi A. The Information Revolution and National Power. Political Aspects — II // Strategic Analisis. – 1999. – Vol. XXIII. – № 6. – p. 1005-1028.

136. Альтшуллер А. «Моссад» против СССР не работал. Потому что этим занимались другие спецслужбы Израиля // НВО. – 2000. – № 26. – С. 7.

137. Квицинский Ю.А. Разоружение: венское начало. У дипломатии суровое лицо // Квицинский Ю.Д. Время и случай. Заметки професионала М.: ОЛМА – ПРЕСС, 1999. – С. 328-329.

138. Казанский П.Е. Русский язык в Австро-Венгрии. Одесса: Б. и., 1912.– С. 12-13. / Цит. за: Восточная Европа в политических планах Российской империи и начале войны. Восточная Галиция и Российская империя накануне и в начале первой мировой войны // Бахтурина А. Ю. Политика Российской империи в Восточной Галиции в годы первой мировой войны / Под ред. Г.А. Бордюгова.– М.: АИРО-XX, 2000. – С 50. (Сер. «Первая монография»).

139. Очерки истории российской внешней разведки: В 6 т. М.: Междунар. отнош., 1996.– Т. 2: 1917-1933 годы. – С. 12.

140. Острое оружие дезинформации // Очерки истории российской внешней разведки: В 6 т. М.: Междунар. отнош., 1996.– Т. 2: 1917-1933 годы. – С. 106- 109.

141. Леонтьєва Л.С. Історія використання спеціальних психологічних операцій Німеччиною та Радянським Союзом в роки другої світової війни (1941 – 1945 рр.): Дис. канд. іст. наук / Львівська політехніка. – Л., 1997.– 154 с.

142. Крайников К.В. Оружие особого рода. – М., 1964. – С. 22.

143. Bittman L. The KGB and Soviet dizinfrmation. – Brassey's Int. Defanse Publishers, 1985. — 229 p.

144. Український визвольний рух у боротьбі з НКВД – КГБ. — Б. м.: Організаційно—кадрова референтура ОУП, 1958. –Кн. II.– С. 98-101.

145. «Комитет за возвращение на родину» агентурно-розвідувальна станція КГБ // Український визвольний рух у боротьбі з НКВД-КГБ. — Б. м.: Організаційно – кадрова референтура ОУП, 1958. – Кн. II. –С. 118 – 141.

146. Шебаршин А. День начальника разведки. М: Междунар. отнош., 1994. — С. 127.

147. Симонов К. Глазами человека моего поколения. – М.: Знамя, 1989. — С. 45.

148. Стыкалин А.С. Политика сталинского режима но формированию общественного мнения за рубежом (вторая половина 40-х годов) // Авторитарные режимы в Центральной и Восточной Европе (1917 -1990-е годы). – М.: Ин – т славяноведения РАН, 1999. — С. 94 – 126.

149. Квицинский Ю.А. Quo vadis? Птенец гнезда Андрея Андреевича Громыко // Время и случай. Заметки профессионала. М.: ОЛМА – ПРЕСС, 1999. – С. 281.

150. Кеварков С. Тайный канал. — М.: Междунар. отнош., 1998.

151. Оставили без последствий // Источник. – 1993. –№ 3. — С. 75-82.

152. Воронов В. От лубянского информбюро... Особенности национального компромата // Новое время. — 1999. — № 44. — С. 14—15; Савченко И. Черноморский флот. — К., 1997.

153. Ортнер С.Л. Системный анализ для решения деловых и промышленных проблем. — М.: Сов. радио, 1969. — 216 с.

154. Strategy and force planning Facylti, National Security Decision Vaking Department, Naval War College. R.M. Lloyd, couese director; H.C. Bartlett... [et al.]. – 2nd ed. – 666 p.

155. Кара – Мурза С.Г. Манипуляция сознанием. — М.: Аграф, 2000.

156. Богданов А.А. Тектология. — М.: Финансы, 1989.

157. Доценко Е. Психология манипуляции. — Ростов-на-Дону: РГУ, 1996. — С. 15.

158. Новиков В. Записки контрразведчика. — М., 2000. — 240 с. — (Сер. «Архивы контрразведки»; Вып. 1).

159. Wilson M. Modern Political Warfare. – Memphis: The Nemesis Group, 1993. – P. 27.

160. Черняк Е. Донесения из гарема // Черняк Е. Пять веков тайной войны. — М.: Б. и., б. г. — С. 36 — 41.

161. Орешкова С. Ф. Султанский двор и гарем в Османской империи первой половины XVII в. // Орешкова С. Ф. Политическая интрига на Востоке. — М.: Восточная литература, 2000. — С. 236 — 245.

162. Широнин В. Под колпаком контрразведки. — М.: Палея, 1997. — С. 27.

163. Крючков В.А. Личное дело. –М.: Б. и., 1996. – т. 1. – С. 236.

164. Чалдини Р. Психология влияния. — СПб.: Питер Ком, 1999. — 272 с. — (Сер. «Мастера психологии»).

165. Бінько І. Формувати, щоб врятувати // Урядовий кур'єр. — 1998. — 12 трав.

166. Чумак В.М. Ядерна стратегія США: від перевершення до нерозповсюдження: Монографія. — К.: НІСД, 1999. — 304 с.

167. Грамши А. Общие вопросы философии и эстетики. Тюремные тетради // Искусство и политика: В 2 т. — М.: Искусство, 1991. — Т. 1. – С. 268.

168. Фуко М. Слова и вещи. Археология гуманитарного знания. — М.: Книга, 1998. – 453 с.

169. Крымский С.Б., Пилипенко В.Е., Салюк Ю.В. Верификация социальных прогнозов (методологический аспект) / АН Украины, Ин-т социологии; Отв. ред. Ю.Н. Пахомов. К.: Наук, думка, 1992. – С. 8.

170. Грамши А. Критические заметки о попытке создания «Популярного очерка по социологии»// Грамши А. Тюремные тетради: В 3 ч. – М: Политиздат, 1991. – Ч. 1. — С. 166.

171. Ашин Г.К. Современные теории плиты: критический очерк. М: Междунар. отнош., 1985. — С. 59.

172. Винер Н. Кибернетика. — М.: Радио. 1968. — С. 43.

173. Мангейм Д.Б., Рич Р.К. Политология. Методы исследования / Предисл. А.К. Соколова. – М.: Весь мир, 1997. — 544 с.

174. Янч Э. Прогнозирования НТП. – М.: Прогресс, 1974. — С. 156.

175. Пригожин И. От существующего к возникающему. Время и сложность в физических науках / Под ред. Ю.Л. Климентовича. – М.: Наука, 1985. – С. 17.

176. Гуцал А.Ф., Ожеван М. Віртуальна Росія. Сходження до реальної ринкової економіки // Страт. Панорама. – 1998. – № 3 – 4.

177. Грамши А. Тюремные тетради // Избр. произв. : В 3 т. — Б. г. : Б. и., б. г. – Т. 3. – С. 124.

178. Моисеев Н. Н. Пути к созиданию. — М.: Республика, 1992. — С. 105.

179. Рыскова Т. М. Политический портрет как метод диагностики статуса и влиятельности лидера // Вестн. Моск. ун-та. Сер. 12, Полит. науки. – 1996. – № 4. – С. 2 – 14.

180. Почепцов Г. Г. Методы анализа текстов политических лидеров // Почепцов Г. Г. Информационные войны. – М. : РИП-Холдинг, 1999. – С. 297-330.

181. Breslauer S. The operational cod of the Politburo // Contemporary Soviet Propaganda and Disinformation. A. Conference Report. — Arsley. Virginia. — USDS and CIA. – 1985. – June 25-27. – P. 246-275.

182. Швейцар П. *Победа. Роль тайной стратеги администрации* США в распаде Советского Союза и социалистического лагеря. – Минск: Авеста, 1995. – 464 с.

183. Ракитянский Н. Проблема психодіагностики политических лидеров // ОНС. – 1995. – № 6. – С. 110.

184. Кожин В. Черносотенство и революция. – М.: Палея, 1998. – 327 с.

185. Dobbs M. U.S. Advice Guided Milosevic Opposition // Washington Post Foreign Service. – 2000. – 11 Dec. – P. A01.

186. Марцун Є. Майбутній світоустрій очима китайських політологів // Людина і політика. – 2003. – № 4. – С. 63-72.

187. Mark A.Stokes. China's Strategic Modernization: Implication's for the United States / Strategic Studies Institute. USA. – 1999. – 168 p.

188. Соколовський М. США і Китай – гра тільки починається... // Дзеркало тижня. – 2001, 21 квітня.

189. Pillsbury M. China Debates the Future Security Environment. – Washington, 2000. – 184 p.

190. Бжезинский З. Великая шахматная доска. Господство Америки и его геостратегические императивы. – М., 1999. – 256 с.

191. Kristensen H.M., Kile S. World nuclear forces // SIPRI Yearbook 2003: Armaments, Disarmament and International Security. – Oxford, 2003. – P.101-125.

192. The Washington Times, 29.8.2001.

193. Бурдье П. Социология политики. –М.: 1993. —С.187

194. Many Tools of Big Brother are Up and Running by John Markoff and John Schwartz // New York Times, December 23. — 2002.

195. Бабенко Ю. Інформаційна війна України в глобалізованому світі. Інститут Масової Інформації / 20.04.2000

196. Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны. – Конфидент, 1996.– № 4.– С. 9-12.

197. Завадский И. И. Информационная война – что это такое? – Конфидент, 1996.– № 4. — С. 13-20.

198. Изард К. Э. Психология эмоций / Перев. с англ. – СПб.: Издательство "Питер", 2000. – 464 с.

199. Кондратьев Н.Д. Избранные сочинения. М.: Экономика, 1993. – 544 с.

200. Глазьев С.Ю. Теория долгосрочного технико-экономического развития. М.: "ВлаДар" – 1993.– 310 с.

201. Социокультурная динамика в период становления постиндустриального общества: закономерности, противоречия, приоритеты. Материалы к III Международной Кондратьевской конференции. М.: 1998. – 495 с.

202. Хохлов И. И. Исламский терроризм – Глобальный джихад Салафи международная террористическая сеть Аль-Каида.

203. Крутов В. Сегодня терроризм – это серьезный и мощный бизнес.

204. Игнатенко А. Милостыня для террориста. {RTF bookmark start: }_Hlt151961347{RTF bookmark end: }_Hlt151961347

205. Хеннесси П., Кайт М. Британия проигрывает "Аль-Кайеде" борьбу. Telegraf. Перевод на сайте Inopressa 23-10-2006 .

206. Александер И. Международный терроризм сегодня и завтра.

207. Манипулятивные стратегии в политике, экономике, бизнесе и методы противодействия им. – К.: Институт психотехнологий, 2001. – 225 с.

208. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Мн.: Харвест, 2004.– С. 406 – 410.

209. Организационная психология / Сост. И общ. Редакция Л. В. Винокурова, И. И. Скрипюка. – СПб.: Питер, 2001. – 512с.

210. Психологические войны / Г. Г. Почепцов. – М.: "Рефл-бук", К.: "Ваклер", 2002 – 528с.

211. Подорога В. ГУЛаг в уме. Наброски и соображения // Индекс – Досье на цензуру, 1999.– №7-8.

212. Зимовец С. Молчание Герасима: психоаналитические и философские эссе о русской культуре.– М., 1996.

213. Виртуальная реальность // Руднев В.П. Словарь культуры XX столетия.– М., 1997.

214. Lobe J. Learn from Cuba // IPS-World Bank. April 30. 2001.

215. Лотман М.Ю. Изъявление Господне или азартная игра? Закономерное и случайное в историческом процессе // Ю.М.Лотман и тартусско-московская семиотическая школа. – М.. 1994. – С. 353-369.

216. Макаренко В.П. Феномен "квазиполитики" и проблема политических объектов // Вестник Московского университета. Серия 12. Политические науки. – 1998. – № 3. – С.31-33.

217. Бахтияров О.Г. Постинформационные технологии: введение в психонетику. Киев, 1997.

218. Шевченко В.А. Универсальный природный цикл.– Киев, 1992.

219. Кизима В.В. Тоталлогические аллюзии. В сб. Totallogy.– Киев, 1995.

220. Доценко Е.Л. Психология манипуляции.– Москва, 2000.

221. Смирнов И.В. и др. Психотехнологии.– Москва, 1996.

222. Бахтияров О.Г Деконцентрация.– Киев, 2001.

223. Современная идеологическая борьба: Словарь/ Под общ. ред. Н.В. Шишлина, Сост. С.И.Беглов. – М.: Политиздат, 1988. – 431 с.

224. Федоров И.А. Имидж как программирование поведения людей. Рязань: "Новое время", –1997.–240 с.

225. Лукашев А.В., Пониделко А.В. "Черный PR" как способ овладения властью или борьба для имиджмейкера. 2-е изд. – СПб.: Изд. Дом "Бизнес-пресса", 2001. – 176 с.

226. Потеряхин А.Л. Психология слухов (Научно-практическое пособие). – Черновцы, 2000. – 68 с.

227. Гульбинский Н.А., Сорокина Е.С. "Краткий курс" для эффективных политиков. – М.: Аванти, – 1999. – 184 с., 10 ил.

228. О'Коннор Джозеф, Сеймор Джон. Введение в нейролингвистическое программирование. – Челябинск: "Версия", 1997. – 256 с.

229. Гарифуллин Р.Р. Иллюзионизм личности как новая философско-психологическая концепция. Психология обмана, манипуляций, кодирования.– Казань ,1997. – 403 с.

230. Тараненко В.И. Конспект лекций, 2000 .

231. Ильясов Ф.Н. Политический маркетинг. Искусство и наука побеждать на выборах, М.: ИМА-пресс, 2000 г. – 200 с.

232. Кара-Мурза С. Манипуляция сознанием.– М., 2000. – 300 с.

233. Почепцов Г.Г. Теория коммуникации. – К.: "Киевский университет", 1999. – 308 с.

234. Броди Ричард. Психические вирусы: как защититься от программирования психики.– М.: "Современные психотехнологии", 2001 . – 192 с.

235. Фаер С. Приемы стратегии и тактики предвыборной борьбы. – СПб: Изд-во "Стольный град", 1998. – 136 с.

236. Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 черв.1996 р. – К.: Преса України, 1997. – 80 с.

237. Національна безпека і оборона.– 2001.– №1.

238. Концепція (Основи державної політики) національної безпеки України: Схвалена Постановою Верховної Ради України від 16 січня 1997 року № 3/97-ВР.

239. Шевченко В.О., Іващенко М.М. Концепція національних інтересів України. – К.: Слов'янський світ, 1996 – 63 с.

240. Національна безпека і оборона.– 2000.– №3. – С.14-15.

241. Столяренко Л.Д. Основы психологии. – Ростов н/Д: Феникс, 2001.

242. Демидов А.И., Федосеев А.О. Основы политологии.– М.: Наука, 1995.

243. Почепцов Г.Г. Русская семиотика.– М.: Рефл-бук,– К.: Ваклер, 2001.

244. Почепцов Г.Г. Психологические войны.– М.: Рефл-бук,– К.: Ваклер, 2001.

245. Кардаш А.В. Изменённые состояния сознания.– М.: Наука, 1984.

246. Психология господства и подчинения: Хрестоматия / Сост. А.Г. Черняв-ская.– Мн.: Харвест, 1998.

247. Юнг К.Г. Бог и бессознательное.– М.: Олимп, ООО "Издательство АСТ-ЛТД", 1998.

248. Аронсон Э. Общественное животное. – М.: Аспект-Пресс, 1998.

249. Аронсон Э., Пратканис Э. Эпоха пропаганды: Механизмы убеждения. Повседневное использование и злоупотребление.– СПб.: прайм-Еврознак, 2002.

250. Бахтин М.М. Эстетика словесного творчества.– М.: Искусство, 1979.

251. Бендлер Р., Гриндер Д. Семинар по НЛП. Передовые психотехнологиии в психотерапии и в бизнесе. – М.: ПРАЙМ, 1998.

252. Бурдье П. Социология политики: Пер. с фр./ Сост., общ.ред.и предисл. Н.А. Шматко./ – М.: Socio-Logos, 1993.

253. Кабаченко Т.С. Методы психологического воздействия: Учебное пособие.– М.: Педагогическое общество России, 2000.

254. Психология масс. Хрестоматия.– Самара, "БАХРАХ",1998.

255. Расторгуев С.П. Философия информационной войны.– М.: Вузовская книга, 2001.

256. Фрейд З. Собрание сочинений.– В 26-ти тт.– СПб.: ВЕИП , 2006.

257. Юнг К. Г. Очерки по психологии бессознательного.– М.: Когито-Центр, 2006 – 352 с.

258. Юнг К. Г. Душа и миф. Шесть архетипов.– М.: Харвест, 2005. – 400 с.
259. Юнг Карл Густав. Дух в человеке, литературе и искусстве. М.: Харвест , 2003. – 384 с.
260. Юнг К. Г., Фуко М. Матрица безумия.– М.: Алгоритм, Эксмо ,2006. – 384 с.
261. Лебон Г. Психология народов и масс. – М.: Макет , 1995 –320 с.
262. Бэндлер Р., Гриндер Дж. Структура магии.– М.: Прайм – Еврознак, 2004 – 256 с.
263. Эфрон Э. Тенденциозная редакторская политика в американских СМИ. The news twisters. New York – 1972.
264. Средства массовой информации в странах СНГ. Анализ политической, законодательной и социально-экономической структур. Под ред. Дж. МакКормак. – Европейский Институт средств массовой информации, Германия,1999.
265. Бессонов Б.Н. Идеология духовного подавления – М., 1978.
266. Шиллер Г. Манипуляторы сознанием. – М., 1980. – С. 120.
267. Матвієнко В.Я. Соціальні технології. – К.: Українські пропілеї, 2001.
268. Крысько В. Секреты психологической войны (цели, задачи, методы, опыт). – Минск, 1999.
269. Грачев Г., Мельник И. Манипулирование личностью: организация, способи и технологии информационно-психологического воздействия. — М., 1999.
270. Аристотель. О софистических опровержениях / Сочинения в четырех томах. Т.2, М. – 1978; Він же. Риторика. – Минск: Литература, 1998.
271. Карнеги Д. "Как завоевывать друзей и оказывать влияние на людей", "Как вырабатывать уверенность в себе и влиять на людей, выступая публично", "Как перестать беспокоиться и начать жить". – М., 1989.
272. Макиавелли Н. Государь. – М., 1990.
273. Фромм Э. Бегство от свободы. – М., 1989.
274. Інформаційна сфера України: стан, проблеми і перспективи. – К., 2002. – С. 25.
275. Герман Крістіано. Шляхи та манівці до глобального інформаційного суспільства // Сучасна політична культура та мас-медіа. – К., 1998. — С. 17 – 33.
276. Солонская С.А., Недбаевский С.Д. Практика манипулирования массовым сознанием в СМИ и способы ее нейтрализации // Актуальні проблеми міжнародних відносин. – К., 2002. – С. 99 – 109.
277. Політична цензура в Україні: факти, тенденції, коментарі. – К., 2002. – С. 80.
278. Реклама: внушение и манипуляция. – Самара: Издательский дом "БАХРАХ-М", 2001. – С. 634.

279. Матеріали до парламентських слухань "Суспільство, ЗМІ, влада: свобода слова та цензура в Україні". – К., 2002. – С. 15-18.

280. Даниленко С. Комунікаційний чинник формування нової політичної еліти // Журналістика й проблема формування нової політичної еліти у посткомуністичних державах: Матеріали міжнародної науково-практичної конференції / За загал, ред. проф. А.З. Москаленка. – К., 1996. – С. 34 – 35.

281. Фромм Э. Иметь или быть? – М.: Прогресс, 1990. – С. 45.

282. Ортега-и-Гассет Хосе. Этюды об Испании. – С. 65 – 74.

283. Бахтияров О.Г. Манипулятивные технологии воздействия на общество и методы противодействия им. // Актуальні проблеми міжнародних відносин. – К., 2002. – С. 93-98.

284. Dufour Jean-Louis, Les crises internationales de Pŕkin (1900) a Sarajevo (1995), Editions Complexe, 1996.

285. President: Iraqi Regime Danger to America is "Grave and Growing" – http://www.whitehouse.gov

286. President Discusses Growing Danger posed by Saddam Hussein's Regime – http://www.whitehouse.gov

287. President Bush Outlines Iraqi Threat – http://www.whitehouse.gov

288. PM speech: 'Saddam Hussein is a threat that has to be dealt with' –http://www.whitehouse.gov

289. Prime Minister's Iraq statement to Parliament – http://www.number-10.gov.uk

290. PM statement on Iraq following UN Security Council Resolution – http://www.number-10.gov.uk

291. President Delivers "State of the Union" – http://www.whitehouse.gov

292. Prime Minister's statement to Parliament following his meeting with President Bush – http://www.whitehouse.gov

293. Presidential Remarks 2/10/03 – http://www.whitehouse.gov

294. President Discusses the Future of Iraq – http://www.whitehouse.gov

295. Poll: Americans Back Ultimatum – http://www.cbsnews.com

296. America's Image Further Erodes, Europeans Want Weaker Ties – http://people-press.org

297. Пионтковский А. Антиамериканизм по-европейски и по-русски – http://www.vif2.ru

298. Zaharna R.S. Crisis Public Diplomacy: American Public Diplomacy in the Arab World // Foreign Policy in Focus, Volume 8, Number 2, June 2003 – http://www.foreignpolicy-infocus.org/briefs/ vol8/ v8n0diplomacy_body.html

299. Bush Job Approval Edges Back Up – http://www.cbsnews.com

300. Chu J. "Winning The Battle, Losing The War" – http://www.whitehouse.gov

301. Wikipedia: The free encyclopedia "Internet protocol suite"- http://www.whitehouse.gov
302. Старостина Е. Кибертерроризм – подход к проблеме //http://www.crime-research.ru
303. Information Security. A new challenge for the EU. A.Esterlie, H.Rank, B. Schmit/ Chaillot Papper №76, march 2005.
304. Яковенко А.А. Кибертерроризм – угроза информационному обществу//
305. DG Information Society. eEurope 2005// www.europa.eu.int/european society/eeurope
306. Лукацкий А.В. Кибертерроризм: за и против /http://www.crime-research.ru
307. Волковский Н.Л. История информационных войн: В 2 ч.- СПб, 2003.
308. Панарин И.Н. Технология информационной войны. – М.:"КСП+", 2003. – 320 с.
309. Информационные вызовы национальной и международной безопасности. – М.: ПИР-Центр, 2001.
310. Леонов О. В. Кібертероризм як проблема інформаційного суспільства.- http:// www.niisp.gov.ua
311. Гавловський В.Д., Цимбалюк В.С. Кіберзлочинність як чинник державної інформаційної політики України.- http:// www.crime-research.org
312. Wilkinson P. The Laws of War and Terrorism // The Morality of Terrorism / Ed. by D. Rappoport, Y. Alexander. – N.-Y.: Columbia University Press, 1989.
313. Супертерроризм: новый вызов нового века. – М.: Права человека, 2002.
314. CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Dorothy E. Denning Georgetown University May 23,2000.: http://www.cs.georgetown.edu
315. Игнатенко А. Зеленый Internetционал. Экстремизм в компьютерной сети.//НГ-Религии.–1999.–№3/3.–7апр.
316. Комп'ютерна злочинність: Навч. посіб. – К.: Атака, 2004. – 240 с.
317. Джангир Арас Четвертая мировая война.– Баку.: Изд-во"SADA", 2003.
318. Номоконов В.А., Интернет и преступность: криминологические и правовые аспекты взаимосвязи // Организованный терроризм и организованная преступность.– М., 2002.
319. Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime, GIPI, August 2002.
320. Activism, Hacktivism, and Cyberterrorism:The Internet as a Tool for Influencing Foreign Policy by Dorothy E. Denning Georgetown University New-York, 2001.

321. Європейська Конвенція з кіберзлочинності (Будапешт, 23 листопада 2001 р.). – .europa.eu int

322. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євро інтеграції: Навчальний посібник. – К.: КНТ, 2006.– 208 с.

323. Всемирный симпозиум по науке и культуры: Выступление г-на Амаду-Махтара М'Боу, Генерального директора ЮНЕСКО. – Париж, 1981.

324. Дзюба І. Між культурою і політикою. – К.: Сфера, 1998.

325. Діалог культур в глобальному світі / Матеріали круглого столу. – К., 2001.

326. Доклад о развитии человека 2004. Культурная свобода в современном многообразном мире. Издано для Программы развития Организации Объединенных Наций (ПРООН).– М.: «Весь Мир», 2004.

327. Межправительственный комитет по Всемирному десятилетию развития культуры: Заключительный доклад. Вторая внеочередная сессия (Париж, 3-7 апреля 1995 г.). – Париж: ЮНЕСКО, 1995.

328. Пироженко В. О. Гуманітарна складова національної безпеки: предмет дослідження та коло основних проблем // Страт, панорама. – 2005. – № 2.

329. Про основи національної безпеки України: Закон України // Відомості Верховної Ради (ВВР). – 2003. – № 39.

330. Резолюция Генеральной Ассамблеи Организации Объединенных Наций A/RES/60/1, принятая 24 октября 2005 г.; итоговый документ Всемирного саммита 2005 года.

331. Ручка А. „Свої" та „чужі" в багатоскладовому суспільстві // Соціокультурні ідентичності та практики / За ред. А. Ручки. – К.: Ін-т соціології НАН України, 2002.

332. Сідак В., Валько І. Мораль і безпека особи, нації, держави. Історико-філософські нариси. – К., 2001.

333. Феномен нації: основи життєдіяльності. – К.: Знання: КGO, 1998.

334. UNDP (United Nations Development Programme). 2004. "BCPR (Bureua for Crisis Prevention and Recovery) Geneva: Contribution to HDR2004".

335. UNESCO (United Nations Educational, Scientific and Cultural Organization). 1998. World Culture Report: Culture, Creativity and Markets. Paris: UNESCO Publishing.

336. UNESCO (United Nations Educational, Scientific and Cultural Organization). 2000c. World Culture Report: Cultural Diversity, Conflict and Pluralism. Paris: UNESCO Publishing.

337. UNESCO (United Nations Educational, Scientific and Cultural Organization). 2002. "Universal Declaration on Cultural Diversity". Cultural Diversity Series No. 1. Paris.

338. UNESCO (United Nations Educational, Scientific and Cultural Organization). 2004a. "Culture. Trade and Globalization". Paris. March 2004.

339. Rodman Peter W. Drifting Apart? Trends In U.S.-European Relations. – Wash.: The Nixon Center, 1999;

340. Naumann Klaus. Das Bundis von der Aus? Gedanken uber die Zukunft der NATO // Internatinale Politik. – Jahr 57, Nr. 7. – Juli 2002. – Ss. 7 – 14.

341. Спільна декларація НАТО – ЄС щодо Європейської політики безпеки та оборони. 16 грудня 2002 р. // Празький саміт і трансформація НАТО. – Брюссель: NATO/OTAN, 2002. – С. 103-104.

342. Zecchini Laurent. Les nouveaux habits de l'OTAN // Le Monde. – 20 Juin 2003; Riche Pascal. Les craintes europeennes de Washington // Liberation. – 20 Juin 2003.

343. Barnett Thomas P. M. The Pentagon's New Map: War and Peace in the Twenty-first Century. – New York: G.P. Putnam's Sons, 2004.

344. Chubin Shahram, Green Jerrold D., Larrabee F. Stephen. NATO's New Strategic Concept and Peripheral Contingencies: The Middle East. / RAND/GCSP Workshop. – Wash., D.C.: RAND, 1999. – P. 1 – 7.

345. The Financial Times, 22 November 2006.

346. Walt Stephen M. American primacy: its prospects and pitfalls – prominence of United States in economic, international affairs // Naval War College Review. – Vol . 55, No. 2. – Spring 2002.

347. Lucas Edward. Sound alarm – Nato is failing // The Daily Telegraph, 17 November 2006.

348. Телеканал СТБ Світлана Федчун, Володимир Овчаренко,Програма «Вікна», 24 жовтня, 18:10

349. Інформаційно-аналітичний проект «Погляд». Євроатлантична інтеграція України: агітація "ЗА" НАТО з великим рахунком програла агітації "ПРОТИ". 13-06-2006

350. Кремень В.Г. Політична безпека України: концептуальні засади та система забезпечення. – К.: НІСД, 1998.

351. Косевцов В.О., Бінько І.Ф. Національна безпека України: проблеми та шляхи реалізації пріоритетних національних інтересів. – К.: НІСД, 1996. (Серія "Національна безпека"; Вип.1).

352. Соснін О.В. Забезпечення інформаційної безпеки держави: теоретичний дискурс // Стратегічна панорама. – 2004. – № 2. – С. 149-154.

353. Іванов В.Ф. Законодавство про засоби масової інформації: український та зарубіжний досвід. — К.: Видавничий центр "Київський університет", 1999.

354. Іванов В.Ф. Медіа та політреклама у дзеркалі закону: Монографія. — К.: ЦВП, 2001.

355. Преса і влада. — К., 2001.
356. СМИ в СНГ: Бюллетень Европейского института средств массовой информации. — 2000-2002.
357. Україна: Інформація і свобода слова. — К., 1997.
358. Українське законодавство: Засоби масової інформації. — К., 2000.
359. Український часопис прав людини. — К., 1994-1999.
360. Гаджиев К.С. Введение в геополитику. – М.: Логос, 2003. – 315 с.
361. Мадіссон В.В., Шахов В.А. Сучасна українська геополітика: Навч. посібник. – К.: Либідь, 2003. – 176 с.
362. Toffler A. Powershift, Wealth and Violence at the Edge the 21st Century. – N.Y.: Bentam, 1990. – 485 p.
363. Fukuyama F. The End of History? // The National Interest. – 1989. – Vol. 16. – P. 3-13.
364. Панарин И.Н. Информационная война и геополитика. – М.: Мир книги, 2006. – 506 с.
365. А. Меркель требует определения окончательных границ Евросоюза.- [Електрон.ресурс]. – Спосіб доступу: URL: http://www.veneportaal.ee/news
366. Единая Европа выдохлась.- [Електрон.ресурс]. – Спосіб доступу: URL: http://www.vremea.net/news
367. Василенко И.А. Геополитика современного мира. – М.: Гардарики, 2006. – 378с.
368. Андрущенко (Гринько) С.В. Україна в сучасному геополітичному середовищі. – К.: Логос, – 2005. – 286 с.
369. Libisky M. The Emerging Primacy of Information // Orbis. – 1996. – №40/2. – P.261-276.
370. Dodds K., Atkinson, D. Geopolitics and geographical imagination of Argentina // Geopolitical traditions: a century of geopolitical thought. – L.: Routledge, 2000. – 150 p.
371. У Tuathail G., Agnew, J. Geopolitics and discourse: practical geopolitical reasoning in American foreign policy // Political Geography. – 1992. – Vol. 11. – P. 190–204.
372. Dodds K. Political geography III: critical geopolitics after ten years // Progress in Human Geography. – 2001. – Vol.25, № 3. – P. 469–484.
373. Кольтюков А.А. Международный терроризм – угроза глобальной и региональной безопасности: особенности проявления и пути противодействия // "Право и безопасность". – 2002. – № 2-3 (3-4). -[Електронний ресурс].- Спосіб доступу: URL: http://dpr.ru.
374. Wallerstein I. Geopolitics and Geoculture: Essays on the Changing World System (Studies on Modern Capitalism). – C.:Cambridge UP, 1991. – 205 p.

375. У Tuathail, G. Problematising geopolitics: survey, statesmanship and strategy // Transactions of the Institute of British Geographers. – 1994. – Vol. 19, №3. – P. 259–272.

376. Heffernan, M. Fin de siecle, fin du monde? On the origins of European geopolitics, 1890–1920 //Geopolitical traditions: a century of geopolitical thought; In Dodds K. and Atkinson D., editors. – L.: Routledge, 1992. – P. 27–51.

377. Atkinson D., Dodds K. Introduction: geopolitical traditions: a century of geopolitical thought //Geopolitical traditions: a century of geopolitical thought; In Dodds K. and Atkinson D., editors. – L.: Routledge, 2000. – P. 1–24.

378. Sharp J. Reel geographies of the new world order: patriotism, masculinity and geopolitics in post-Cold War American movies // Rethinking geopolitics; In У Tuathail G. and Dalby S., editors. – L.: Routledge, 1998. – P. 152–169.

379. Luke T., У Tuathail G. On videocameralistics: the geopolitics of failed states, the CNN International and (UN)governability// Review of International Political Economy. – 1998. – №4. – P. 709–733.

380. McKendrick J. Data for Scotland: reshaping the nation through population statistics // Scottish Geographical Journal. – 1999. – Vol. 115. – P. 211–226.

381. Falah, Ghazi-Walid, Flint, Colin, Mamadouh Virginie War and Extraterritoriality: The Popular Geopolitics of the United States' War on Iraq as Reflected in Newspapers of the Arab World // Annals of the Association of American Geographers. – 2006. – Vol. 96, Issue 1. – P. 142-164.

382. Кудряченко А.І., Рудич Ф.М., Храмов В.О. Геополітика.- К.:МАУП, 2004.– 296 с.

383. Цымбурский В. Геополитика как мировидение и род занятий. [Электронный ресурс] // Русский Архипелаг. Сетевой проект Русского Мира. – Спосіб доступу: URL: http://www.archipelag.ru

384. Гречанінов В. Після розпаду біполярної системи. Новий світовий порядок та глобалізація на початку XXI століття // Політика і час. – 2002. – №1. – С.58-67.

385. Бжезинський З. Велика шахівниця // Всесвіт. – 1999. – №2. – С.75-145.

386. Маклюен М. Понимание медиа: внешние расширения человека. – М.: Канон-Пресс-Ц, 2003. – 464 с.

387. Lonsdale D. Information Power: Strategy, Geopolitics, and the Fifth Dimension // Geopolitics, geography and Strategy; ed. by Grey C., Sloan G. – London: frank Cass, 1999. – P. 137-157.

388. Ивашов Л.Г. Россия или Московия? Геополитическое измерение национальной безопасности России. – М.: Эксмо, 2002. – 199 с.

389. Шевченко М. Можливості подолання дестабілізуючого впливу геополітичного фактора: Україна і Балканський досвід, http://www.fleet.sebastopol.ua.

390. Андреев В. Г. Оружие и война: новые тенденции развития//Военная мысль. - 1999, №3.

391. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії. – К., 2000.

392. Соснін О. В. Стратегічний ресурс суспільства. Розвиток високих технологій – запорука індустріального статусу держави // Політика і час. – 2002.–№ 11.

393. М.Шевченко Можливості подолання дестабілізуючого впливу геополітичного фактора: Україна і Балканський досвід, http://www.fleet.sebastopol.ua.

394. Lonsdale D. Information Power: Strategy, Geopolitics, and the Fifth Dimension // Geopolitics, geography and Strategy /ed. by Grey C., Sloan G. – London: frank Cass, 1999. – P. 139.

395. Kraemer, Eric A. The Great Debate. Competing Grand Strategies for America. – Washington: National Defense University, 2000, May 4. – 26 p.

396. Podhoretz, John. Bush Country. – New York: St. Martin's Press, 2004. –276 p.

397. Bush, George. A Charge to Keep. – William Morrow, 1999.

398. Toward a New Grand Strategy for U.S. Foreign Policy Edited by Tom Barry // IRC Strategic Dialogue, 2004, No. 3, December 13, 2004. – 2 p.

400. Lippman, Walter. U.S. Foreign Policy: Shield of the Republic. – Boston: Little, Brown, 1943.

401. Krauthammer, Charles. Democratic Realism: An American Foreign Policy for a Unipolar World. – Washington: American Enterprise Institute, 2004. – aei.org

402. Kennedy, David M. Freedom from Fear. – http://www.futurecasts.com

403. Zoelick, Robert B. Countering Terror with Trade // Washington Post, 2001, September 20.

404. Rice, Condoleezza. Remarks on Foreign Policy Issues. Federal Document Clearing House Political Transcripts. – 2000, November 17. Accessed on LEXIS–Nexis, 2001, March.

405. Gaffney, Frank. Worldwide Value // National Review Online, November 5, 2004. – P. 233.

406. Ikenberry, G. John and Charles A. Kupchan. Liberal Realism: The Foundations of a Democratic Foreign Policy // National Interest, 2004, Fall.

407. Kupchan, Clifford. Real Democratik // National Interest, 2004? Fall. – .

408. Posen, Barry R. and Andrew L. Ross. Competing Visions for U.S. Grand Strategy // International Security, 1996-97, Vol. 21, No. 3. – P. 5-53.

409. Gershman, John. A Secure America in a Secure World // Foreign Policy In Focus, 2004.

410. Lind, William S. Strategic Defense Initiative // The American Conservative, 2004, November 22.

411. Gaddis, John Lewis. Grand Strategy in the Second Term // Foreign Affairs, January/February 2005.

412. Фукуяма Ф. Конец истории и последний человек. – М.: "Издательство АСТ", 2004.– 592 с.

413. Huntington S. The Lonely Superpower // Foreign Affairs. – 1999. – Vol. 78, № 2 (March/ April). – P. 35-49.

414. Schneider C. P. Diplomacy that works: 'best practices' in cultural diplomacy / http://www.culturalpolicy.org/pdf/Schneider.pdf

415. Шаклеина Т.А. Современные американские концепции мирового лидерства. – М.: ИСКРАН, 2000. – 54 с.

416. Панарин А.С. Искушение глобализмом. – М.: Алгоритм-книга, Эксмо, 2003. – 416 с.

417. Roach C. Cultural imperialism and resistance in media theory and literary theory. // Media, Culture and Society. – 1997. – № 19. – P. 47-66.

418. Boyd-Barrett O. Cultural dependency and the mass media // Gurevitch M., Bennett T., Curran J., Woollacott J. Culture, Society and the Media. – New York: Methuen & Co., 1982. – 320 p.

419. Багацький В.В. Культурний імперіалізм у світі і в Україні // Актуальні проблеми політики. Випуск 8. – Одеса: Юридична література, 2000. – С. 341-344.

420. Fejes F. Media imperialism: An assessment // Media, Culture and Society. – 1981. – №3. – P. 281-289.

421. Lee S.-N. P. A case against the thesis of communication imperialism: The audience's response to foreign TV in Hong Kong // Australian Journal of Communication. – 1995. – № 22. – P. 63-81.

422. Tomlinson J. Cultural Imperialism: A Critical Introduction. – London: Pinter Publishers, 1991. – 200 p.

423. Mattleart A. Mapping world communication. – Minneapolis: University of Minnesota Press, 1994. – 294 p.

424. Galtung J. A structural theory of imperialism // Modelski G. Transnational corporations and world order: Readings in international political economy. – San Francisco: W.H. Freeman and Company, 1979. – P. 155-171.

425. Link J.H. Test of the cultural dependency hypothesis // Stevenson R., Shaw D. Foreign news and the new world information order. – Ames: Iowa State University Press, 1984. – P. 186-199.

426. Mohammadi A. Cultural imperialism and cultural identity // Downing J., Mohammadi A., Sreberny-Mohammadi A. Questioning the media: A critical introduction. – London: Sage, 1995. – P. 362-378.

427. McPhail T.L. Electronic colonialism: The future of international broadcasting and communication. – Newbury Park, CA: Sage, 1987. – 314p.

428. Said E. W. Culture and imperialism. – New York: A.A. Knopf, 1993. – 416 p.

429. Ogan C. Media imperialism and the video cassette recorder: The case of Turkey // Journal of Communication. – 1988. – № 38. – P. 93-106.

430. Liebes T., Katz E. The export of meaning: Cross-cultural readings of "Dallas" –Oxford: Oxford University Press, 1990. – 200 p.

431. Ang I. Watching "Dallas": Soap opera and the melodramatic imagination. – London: Methuen, 1985. – 160 p.

432. Sinclair J., Jacka E., Cunningham S. New patterns in global television: Peripheral vision. – New York: Oxford University Press, 1996. – 258 p.

433. Lake E. Pop Psychology. How Lionel and J. Lo Can Help Bridge the Gap Between Us and the Arabs' // Washington Post. – 2002. – August 4. – P. 803.

434. Nye J. Soft Power: the means to success in World Politics. – N.Y.: Perseus Publishing, 2004 – 191 p.

435. Smith S. U.S. Democracy Promotion: Critical Questions // American Democracy Promotion. Impulses, Strategies, and Impacts / Michael Cox, G. John Ikenberry, Takashi Inoguchi (eds.) / http://www.oup.co.uk

436. Холмс К.Р. Американский интернационализм: поощрение свободы, демократии и развития // Электронный журнал Государственного департамента США. – 2003. – № 1 / http://usinfo.state.gov

437. Cultural diplomacy. The Linchpin of Public Diplomacy. Report of the Advisory Commitee on Cultural Diplomacy. U.S. Department of State. September 2005/ http://www.maxwell.syr.edu

438. Keison J. Public diplomacy and U.S. foreign policy – http://www.greatdecisions.org

439. Киссинджер Г. Дипломатия. – М.: Ладомир, 1997. – С. 32.

440. Schneider C. P. Culture Communicates: US Diplomacy that Works. Discussion Papers in Diplomacy – http://www.clingendael.nl/publications

441. Психологическая война. / Под редакцией А.Н. Николаева. – М.: Прогресс, 1972. – 352 с.

442. Сардар З., Дэвис В.М. Почему люди ненавидят Америку? – М.: Изд-во Проспект, 2003. – 240 с.

443. Волкогонов Д.А. Психологическая война: подрывные действия в области общественного сознания. – М.: Воениздат, 1984. – 375 с.

444. Кашлев Ю.Б. Информационный взрыв: международный аспект. – М.: Международные отношения, 1981. – 256 с.

445. Fox R. Cultural diplomacy at the crossroad: Cultural Relations in Europe and the Wider. Worlda report on a conference organised jointly by the British Council and Wilton Park at Wiston House (24 – 28 November 1997). – Published by British Council, – 1999. – 38 p.

446. Cummings M.C. Cultural Diplomacy and the United States Government: a Survey. Center for Arts and Culture, 2003 – http://www.culturalpolicy.org

447. Соединенные Штаты в 2005 году: кто мы, как мы осознаем и понимаем себя // Электронный журнал Государственного департамента США. – 2000. – № 2.

448. К единой Америке: общенациональная дискуссия по расовым вопросам // Электронный журнал Государственного департамента США. – 1997. – № 3.

449. Свобода вероисповедания как право человека //Электронный журнал Государственного департамента США. – 2001. – № 2 – http://usinfo.state.gov

450. На пути к сообществу демократических государств // Электронный журнал Государственного департамента США. – 2000. – № 1 – http://usinfo.state.gov

451. Формирование внешней политики США // Электронный журнал Государственного департамента США. – 2000. – № 1. – http://usinfo.state.gov

452. Feigenbaum H.B. Globalization and cultural diplomacy. Center for Arts and Culture. Art, Culture & National Agenda. Issue Paper – http://www.culturalpolicy.org

453. Sablosky J. A. Recent Trends in Department of State Support for Cultural Diplomacy: 1993-2002. – http://www.culturalpolicy.org/pdf/JASpaper.pdf

454. White House 2000 Conference on Cultural diplomacy: Final Report – http://ics.leeds.ac.uk

455. Уткин А.И. США – ЕС: Два полюса, два взгляда // США–Канада: экономика, политика, культура. – 2005. – №7. – С. 26-44.

456. Жинкина И.Ю. Глобальное лидерство США и его влияние на международные отношения // США–Канада: економика, политика, культура. – 1999. – № 7.– С.39-49.

457. Кременюк В.А. Две модели отношений США с окружающим миром // США–Канада: економика, политика, культура. – 2004. – № 11. – С. 69-78.

458. Шаклеина Т.А. Время выбора: имперское искушение. // США и Канада: экономика, политика, культура. – 2003. – № 12. – С. 3-14

459. Хоффман С. Опасности империи // Internationale Politik. –2004. – № 5. – С. 31-42.

460. Ливен А. Борьба за душу Америки // Internationale Politik. – 2004. – № 5. – С. 4-17.

461. Лалл Дж. Мас-медіа, комунікація, культура: глобальний підхід /Пер. з англійської.– К: "К.І.С.", 2002. – 264 с.

462. Баннов Б.Г., Вачнадзе Г.Н. Чужие голоса в эфире. – М.: Молодая гвардия, 1981. – 287 с.

463. The United State of Television // Financial Times. – 2003. – July 21. – P. 3.

464. Всемирный доклад по культуре 2000+ ЮНЕСКО "Культурное разнообразие, конфликт и плюрализм". – М.: Издательский Дом МАГИСТР-ПРЕСС, 2002. – 416 с.

465. Suleiman E. Dйbats GATT: Pourquoi la France intйresse si peu l'Amйrique // Le Monde. – 1993. – Decembre 8. – P. 2.

466. What the World Thinks in 2002. How Global Publics View: Their Lives, Their Countries, The World, America. Report – http://news.ft.com

467. Hanley D.C. Secretary Open Forum Examines Public Diplomacy // Washington Report on Middle East Affairs. – 2004. – Vol. 23. – P. 75-76.

468. Perlez J. U.S. is Trying to Market Itself to Young, Suspicious Arabs. // New York Times. – 2002. – September 16. – P. 4.

469. Lake E. Pop Psychology. How Lionel and J. Lo Can Help Bridge the Gap Between Us and the Arabs' // Washington Post. – 2002. – August 4. – P. 803.

470. Kralev N. Cultural diplomacy pays off, envoys say. America's other Army: Inside the Foreign Service // The Washington Times. – 2004. – March 22. – P. 3.

471. Murphy C. How to brand the EU.– http://news.ft.com

472. White Paper on a European communication policy. Brussels, 1.2.2006

473. Bounds A. Brand experts study EU identity crisis // Financial Times. – http://news.ft.com

474. Peter van Ham. I "heart" Europe. 16.11.2005. – http://news.ft.com

475. Peter van Ham. Branding European Power. – http://news.ft.com

476. White L., Purdy M., Padmore E. Europe, Inc. – Re-branding Europe.– http://news.ft.com

477. Kunzru H. Rebranding NATO: A SpinMute consultation document.– http://news.ft.com

478. Алани М. Взгляды арабского мира на НАТО // Вестник НАТО, 2005 г.

479. Ким В. Аллергия на НАТО // Зеркало недели, № 24 (552), 25 Июня – 1 Июля 2005 – http://news.ft.com

480. Матеріали конференції «Євроатлантична інтеграція України: регіональний вимір» (20 -21 березня 2003 р., м. Львів) –

481. Латвия и Эстония организовали в Пскове день НАТО. 24.05.2006. [RTF bookmark start: }OLE_LINK1[RTF bookmark start: }OLE_LINK2– [RTF bookmark end: }OLE_LINK1[RTF bookmark end: }OLE_LINK2

482. Marchese L., Simmons R. The United Nations is experiencing a brand crisis. 01.08.2005. – http://news.ft.com

483. Егорова-Гантман Е., Плешаков К. Политическая реклама. – М.: Никколо, 1999. – 240 с.

484. Полохало В. Рейтинг как оружие кандидата // Вечерние вести. – 2003. – 24-30 октября.

485. Стратегія планування виборчої кампанії / К. Пейн, К. Хед, Ш. О'Коннел. – К., 1997.

486. Головатий М. Мистецтво політичної діяльності. – К., 2002. – С. 22.

487. Старовойтенко Р. Імідж політичної партії як чинник електорального вибору // Нова політика. – 2001. – № 2. – С. 57.

488. Политическая имиджелогия (под ред.. Е. Перелыгиной). М., 2006

489. J. Grinder, R.Bandler. Patterns. – N.-Y.: Realist, 2004. – 207 p.

490. Роббинс Э. Беспредельная власть. – М.: Попурри, 2003. – 592 с.

491. Ситников А.П. Тезисы выступления на региональной научно-практической конференции "Культура и проблемы межэтнической коммуникации". – Н-Новгород, 21 мая 2002.

492. Почепцов Г. Г. Як стають президентами. Виборчі технології XX століття. – К., 1999. – 380 с.

493. Бебик В. Менеджмент виборчої кампанії: ресурси, технології, маркетинг: Навч.-метод. посіб. – К., 2001. – С. 55.

494. Pratkanis A., Aronson E. Age of propaganda: The Everyday Use and Abuse of Persuasion. N-Y.: W.H. Freeman and company, 2001. – 384 p.

495. Вердербер Р., Вердербер К. Психология общения. – М.: Олма-Пресс, 2003. – 384 с.

496. О'Коннор Дж., Сеймор Дж. Введение в НЛП. – Челябинск: Версия, 1997. – 256 с.

497. Ковалевська Т. Ю. Комунікативні аспекти нейролінгвістичного програмування. – Одеса: Астропринт, 2001. – 344 с.

498. Власти не хватает доверия и авторитета (ред.) // Вечерние вести. – 2003. – 30 мая – 5 июня.

499. Черепанова И. Клич Гамаюн. Научная магия суггестивного влияния языка. – М.: Профит Стайл, 2006. – 464 с.

500. Королько В. Г. Основи паблик рилейшнз: Учебник для студ. ВУЗов /Отв. ред. Удовик С. Л. – М.: Рефл-бук; – К.: Ваклер, 2000. – 528 с.

501. Дилигенский Г. Г. Социально-политическая психология: Учебное пособие. Изд. 2-е, исправ. и доп. – М.: Новая школа, 2000. – 352 с.

502. Максимов А. А. "Чистые" и "грязные" технологии виборов: российский опыт. – М., 2000. – С. 50.

503. Проект Концепції (Основ державної політики) інформаційної безпеки України. //Національна безпека і оборона, 2001.– №1. – С. 30.

504. Галумов Э.А. PR в международных отношениях. //Информация. Дипломатия. Психология. – М.: Известия, 2002. – С. 174-175.

505. Хачатуров К.А. Роль международной информации в формировании репутации государства. //Информация. Дипломатия. Психология. – М.: Известия, 2002. – С. 115.

506. Black J., Bryant J. Introduction to media communication. – Madison: Brown&Benchmark, 1995. – P. 465.

507. Тарашвили Е. Связи с общественностью в государственных структурах. –http://www[RTF bookmark start: }_Hlt28060273.[RTF bookmark end: }_Hlt28060273pressclub.host.ru/PR.Li[RTF bookmark start: }_Hlt28060320b[RTF bookmark end: }_Hlt28060320/Terashvili.htm.

508. Wilson Stan Le Roy. Mass media/mass culture. An introduction. – N.Y.etc.: McGraw-Hill Inc., 1993. – P. 334.

509. Почепцов Г.Г. Коммуникативные технологии двадцатого века. – М.: Рефл-бук; Ваклер, 2000. – С. 71.

510. The spin doctors get serious. –http://www.prfirms.org

511. Harrigan J.J. Politics and the American future: dilemmas of democracy. – 4 ed. – N.Y.etc: McGraw-Hill Companies, 1996. – P. 259.

512. Serfaty Simon. The media and foreign policy. – Houndmills, Basingstoke, Hampshire, Macmillan Academic and professional Ltd., 1990. – P. 6,12, 68, 72.

513. Хэмпсон Кит Правительство Великобритании. Координация связей с общественностью. – http://www.polit.spb.ru/art.phpз?rub228&id10867.

514. Чумиков А.Н. Связи с общественностью. – М.: Дело, 2001. – С. 80-82.

515. Тульчинський Г.Л. PR фирмы: технология и эффективность. – СПб: Алетейя, 2001. – С.112.

516. Связи с общественностью в политике и государственном управлении. // Под общ. Ред. В.С. Комаровского. – М.: Изд-во РАГС, 2001. – С. 230-231.

517. Бабенко Ю. „Інформаційна війна – зброя знищення!", Інститут масової інформації – http://www.pravda.com.ua

518. Политология. Хрестоматия под ред. М. А. Василика.– М., 2000.

519. Політичний маркетинг та електоральні технології. – Київ-Запоріжжя: Ін-т соціології НАНУ, Гарт, 2002.

520. Конотопов П. Політичні технології – зміна поколінь. – http://www.polit-dumka.kiev.ua

521. Горбач В. На західному фронті – українські вибори, 2005 р. – http://www.kontrakty.com.ua

522. Малкін Є., Сучков Є. Які виборчі технології є брудними. Приклад Росії – http://www.politdumka.kiev.ua

523. Сулакшин С.С. Избиратель, осторожно! – М., 1998.

524. Макітра Я. "Маніпуляція свідомістю" – http://www.pravda.com.ua 06.02.2006.

525. Макітра Я. " Маніпуляція свідомістю та політична телереклама 2006" – http://www.pravda.com.ua.

526. Гарань О. ""Маніпуляція свідомістю-2", або Чи існує межа, яку не можуть переходити політтехнологи?" – http://www.pravda.com.ua

527. Коліушко І.Б., Демкова М.С. Електронне урядування – шлях до ефективності та прозорості державного управління. Фонд „Інформаційне суспільство України" 2004.

528. Баранов О. Цифрове законодавство. // Дзеркало тижня. – 2005. – № 20 (395).

529. Непомящий Б. Український освітній Інтернет: Удень з вогнем // Дзеркало тижня. –2004. – № 33 (408).

530. Пронин А.; Несколько слов об электронном правительстве. PCWeek. – М.: Профиль.–2004 г. – №3. – С. 12-15.

531. Угода про партнерство та співробітництво між Європейським співтовариством і Україною. № 998-012.

ЗМІСТ

Антологія

Андреев А., Давыдович С. Об информационном противоборстве в ходе вооруженного конфликта в Косово

Воронков Д.А., Богуш Д.А. Манипулятивные составляющие информационных операций

Гриняев С.Н .Особенности информационной войны во время агрессии НАТО против Югославии (по материалам открытой печати)

Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива. Немного истории

Желтов А. Информационная безопасность в международных отношениях

Леваков А. Новые приоритеты в информационной безопасности США

Лейті М. Боротьба на інформаційному фронті

Леонов О. В. Кібервійни постіндустріального світу

Лупаций В.С. Постинформационные технологии в условиях тотальной и глобальной манипуляции

Минихэн К. А. Оборона страны от кибернетической атаки: защита информации в глобальной среде

Мюнклер Х. Терроризм как стратегия коммуникации. Послание 11 сентября

Най Дж. С., Оуэнс У. А. Главная сила Америки — ее информационные возможности

Ожеван М.О. Двогостра зброя

Ожеван М.О. Фронти й тили великих інформаційних війн

Панарин И.Н. Проблемы обеспечения информационной безопасности России в современных условиях

Панарин И.Н. Кондолиза Райс: дипломатия информационной экспансии

Панарин И.Н. Слухи как технология информационной войны

Пахомов Ю.Н. Манипулятивные технологии в рыночно-реформаторском контексте

Печоров С. Дезинформация как метод психологической войны (практика США)

Почепцов Г.Г. Информационные действия и противодействия: основные характеристики

Сменковский А.Ю. Методы двойного воздействия в межгосударственных экономических отношениях

Хант Ч., Зартарьян В. Разведка – нерв экономической войны. Экономическая война

Хэмри Дж. Защита информации – главная задача новейшего периода в обеспечении безопасности

Чинники ескалації загроз інформаційній безпеці України. Аналітична доповідь УЦЕПД

Шафрански Р. Теория информационного оружия

Шимілл Т., Уїльямс Ф., Данлеві К. Протидія електронній війні

Шпиро Ш. Средства массовой информации и терроризм

Документи

Резолюция Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности» (57/239)

Резолюция Генеральной Ассамблеи ООН «Борьба с преступным использованием информационных технологий» (56/121)

Резолюция Генеральной Ассамблеи ООН «Роль науки и техники в контексте международной безопасности и разоружения» (53/73)

Резолюция Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» (53/70)

Резолюция Генеральной Ассамблеи ООН «Меры по ликвидации международного терроризма» (57/27)

Резолюція Ради ЄС «Про законне перехоплення телекомунікацій» (17 січня 1995 р.)

Резолюція Ради ЄС «Про Європейський підхід до культури мережі та інформаційної безпеки» (18 лютого 2003 р.)

Директива Європейського парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (24 жовтня 1995 р.)

Директива Європейського парламенту і Ради ЄС «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі?» (15 грудня 1997 р.)

Резолюція Ради ЄС «Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL)» (20 червня 2001 р.)

Європейська Конвенція про кіберзлочинність (2001 р.)

Соглашение о взаимном обеспечении сохранности межгосударственных секретов в области правовой охраны изобретений (4 июня 1999 г.)

Концепция национальной безопасности Российской Федерации (10 января 2000 г.)

Доктрина национальной безопасности Российской Федерации (9 сентября 2000 г.)

Концепція (основи державної політики) інформаційної безпеки України (Проект УЦЕПД)

Проект Закону України «Про інформаційну безпеку України»

Угода між Урядом України та Урядом Французької Республіки про взаємну охорону таємної інформації та матеріалів

Наукове видання

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ

Автори розділів: 1 розділ: Головченко В.І. (§ 1.6.), Гондюл В.П. (§ 1.3.), Зернецька О.В. (§ 1.4.), Литвиненко О.В. (§ 1.5.), Макаренко Є.А. (§1.1., 1.2.), Ожеван М.А. (§1.7.), Піскорська Г.А. (§ 1.4.), Яковець А.В. (§ 1.8.); **2 розділ:** Бахтіяров О.Г. (§ 2.4.), Богуш Д.А. (§ 2.4.), Гуцал А.Ф. (§ 2.1., 2.2.), Даниленко С.І. (§ 2.7.), Запорожець О.Ю. (§ 2.8.), Недбаєвський С.Л. (§ 2.1., 2.6.), Ожеван М.А. (§ 2.3.), Романенко Ю.В. (§ 2.5.), Солонська С.А. (§ 2.6.); **3 розділ:** Білоусова Н.Б. (§ 3.6.), Даниленко С.І. (§ 3.5.), Іванов В.Ф. (§ 3.9.), Камінський Є.Є. (§ 3.8.), Ожеван М.А. (§ 3.7.), Піскорська Г.А. (§ 3.2.), Сербіна Н. Ф. (§ 3.3.), Толстов С.В. (§ 3.4.), Фролова О.М. (§ 3.1.), **4 розділ:** Кучмій О.П. (§ 4.3.), Панченко Ж.О. (§ 4.1.), Рижков М.М. (§ 4.2.), Тихомирова Є.Б. (§ 4.6), Швець О.В. (§ 4.5.), Шевченко О. В. (§ 4.4.))

Художнє оформлення — Микола Мельник
Комп'ютерна верстка — Микола Мельник
Технічний редактор — Ірина Миколаєнко
Коректор — Ірина Кисарець

Підписано до друку 12.12.2006 р.
Формат 60x84/16. Друк офсетний. Папір офсетний.
Ум. друк. 53,24. Обл.-вид. арк. 71,88.
Наклад 1000 прим. Зам. № 1794.

Віддруковано в ТОВ "Видавництво "Аспект-Поліграф"
Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи серія ДК № 1115, від 12.11.2002 р.

16600, Чернігівська обл., м. Ніжин, вул. Шевченка, 109 а,
факс: (04631) 3-11-08, тел. (04631) 3-18-03,
e-mail: aspekt@ne.cg.ukrtel.net