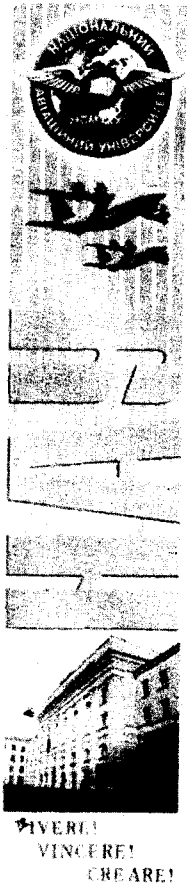
С.В. Толюпа
В.О. Хорошко
Ю.Є. Хохлачова



ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Лабораторний практикум

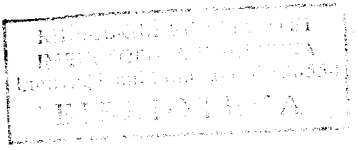
Київ 2014

Міністерство освіти і науки України
Національний авіаційний університет

С.В. Толюпа, В.О. Хорошко, Ю.Є. Хохлачова

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Лабораторний практикум



Київ 2014

УДК 351.863:004.0561(477)

ББК 67.9(4Укр)401+66.4(4Укр)

З-15

Рекомендовано вченою радою Інституту комп'ютерних інформаційних технологій НАУ (протокол № 6 від 23.06.2014р)

Рецензенти:

доктор технічних наук, професор Пархуць Л.Т.
доктор технічних наук, професор Щербак Л.М.

Хорошко В.О. Забезпечення інформаційної безпеки держави. Лабораторний практикум / Толюпа С.В., Хорошко В.О., Хохлачова Ю.Є. – К ПВП "Задруга", 2014. – 68 с.

Лабораторний практикум створено відповідно до програми курса "Забезпечення інформаційної безпеки держави"

Призначається для студентів, що навчаються за усіма спеціальностями освітнього напрямку "Інформаційна безпека"

УДК 351.863:004.0561(477)

ББК 67.9(4Укр)401+66.4(4Укр)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС	автоматизована система
ДМУ	державне та муніципальне управління
ЕОТ	електронно-обчислювальна техніка
ЗІ	захист інформації
ЗМІ	засоби масової інформації
ЗОТ	засоби обчислювальної техніки
ЗП	запам'ятовуючий пристрій
ІАР	інформаційно-аналітична робота
ІБ	інформаційна безпека
ІзОД	інформація з обмеженим доступом
ІС	інформаційна система
ІТС	інформаційно-телекомунікаційна система
КСЗІ	комплексна система захисту інформації
ОС	операційна система
ОТ	обчислювальна техніка
ПЗ	програмне забезпечення
ПЦС	пульт центрального спостереження
ПЗЗУ	пам'ять на зовнішніх запам'ятовуючих пристроях
РЕБ	радіоелектронна боротьба
РКД	рольове керування доступом
СУБД	системи управління базами даних
СЗ	система захисту
СЗІ	система захситу інформації
СОТ	системи обчислювальної техніки
СПТВ	спеціальний програмно-технічний вплив
ТЗІ	технічний захист інформації
ТСЗІ	технічна система захисту інформації

ВСТУП

Революційні зміни останніх років у електронній індустрії, в першу чергу поява цифрових технології і розповсюдження різних новітніх методів зв'язку, створили передумову і призвели до початку фундаментальних перетворень, результатом якого є обєднання інформкомунікаційних і комп'ютерних систем і мереж у єдиний інформаційний простір.

Інформаційний простір, стає сферою і середовищем боротьби, аналогічним суші, воді, повітря, космосу, а також політики, економіці, оборони тощо. Крім того, інформаційний простір став середовищем різноманітних протиправних дій окремих осіб та різноманітних націоналістичних й міжнародних терористичних угрупувань.

Провідні країни світу та міжнародні організації в останні роки різко посилили увагу до проблеми власної безпеки. Критичні елементи національних інфраструктур практично усіх країн світу є вразливими від різних впливів, і поряд із звичними, кібернетичними.

Крім того, слід визначити, що у відкритих джерелах відмічається зростання активності спецслужб у інформаційних ресурсах держав, чимало звинувачень з боку різних країн звучить на адресу США, Китаю та Росії щодо втручання в іформаційний простір держав.

Слід додати, що державна політики багатьох країн спрямована на здійснення національного та глобального моніторингу і впливу, у тому числі через інформаційний простір, на політичні, економічні, військові, екологічні та інші процеси з метою одержання однобічних переваг.

Інформаційний вплив на інформаційний простір держави та суспільство більш ефективний, ніж політичний, економічний і навіть воєнний. Країни з більш розвиненою інформаційною інфраструктурою визначають умови формування і діяльність інформаційних структур в інших країнах, здійснюють суттєвий вплив

на розвиток їхніх інформаційних сфер. При формуванні державної інформаційної політики одним із найбільших пріоритетів стає розвиток і гарантування інформаційної безпеки держави.

Водночас, необхідно чітко бачити і враховувати протиріччя пов'язані із впровадженням в інформаційні ресурси держави та застосуванням у них заходів та засобів захисту. Ці протиріччя пов'язані з тим, що застосування систем захисту, якими б досконалими вони не були, створює певні «незручності» використання захищеного інформаційного простору держави.

При цьому слід враховувати, що однією з найбільш небезпечних загроз для України є порушення та втручання в її інформаційний простір, що дуже важливо для забезпечення інформаційної безпеки держави.

На наш погляд без подальшого вітчизняного стратегічно важливого напрямку – забезпечення інформаційної безпеки держави – можливо втратити всю діяльність і ефективність у цій справі тому, що занадто велика кількість публікацій орієнтована на закордонні видання та їх досвід. Пракичне використання таких видань у нас неможливо, за розбіжністю правових баз.

Цикл лабораторних робіт дозволить познайомитися з принципами та методами забезпечення інформаційної безпеки, а також поглибити свої знання з цієї дисципліни.

Загальні методичні вказівки

Основна мета лабораторних робіт – сприяння засвоєнню набутих знань, умінь і навичок із забезпечення інформаційної безпеки держави.

Навчальні заняття проводяться згідно з навчальним розкладом. Група проходить інструктаж за правилами техніки безпеки, пожежної безпеки та ділить на бригади по 2 або більше студентів. На першому навчальному занятті бригада отримує номер відповідно робочого місця.

До початку навчального заняття студент повинен вивчити порядок виконання роботи, ознайомитися з літературою, яка має відношення до неї.

Ступінь підготовки студента до виконання поточної роботи перевіряється викладачем. З метою самоконтролю при підготовці до виконання роботи, рекомендується відповісти на запитання, які наводяться в кінці кожної лабораторної роботи. Студент, який отримав незадовільну оцінку під час перевірки, до виконання роботи не допускається. Студент, який не здав попередню роботу, до наступної не допускається.

Звіт про лабораторну роботу оформляється на аркушах білого паперу формату А4 (210 х 297 мм) та зброшуровано таким чином, щоб аркуші були щільно стиснуті. Не допускається їх з'єднання скріпкою.

Текст звіту слід оформлювати українською мовою і він повинен мати такі береги: 30мм – лівий; 10мм – правий; 20мм – верхній та нижній.

Текст звіту про роботу виконується за допомогою комп'ютера та перетворений у візуальну форму подання електронного документа. Друкується на одній стороні аркуша через 1,5 міжрядкових інтервали, текст вирівнюється по ширині аркуша. Візуальною формою подання електронного документа є відображення даних, які він містить, на папері у формі, придатній для приймання його змісту людиною.

Сторінки тексту звіту про роботу слід нумерувати арабськими цифрами, додержуючись валової нумерації по всьому тексту. Номер сторінки

проставляється у правому верхньому березі сторінки без крапки в кінці. Титульна сторінка включається до загальної нумерації сторінок тексту звіту. Номер сторінки на титульному аркуші не проставляється.

Текст звіту про роботу повинен бути викладений стисло, грамотно, зрозуміло, без повторів та вживання слів і зворотів, які не несуть смислового навантаження і оформлений у вигляді поєднання суцільного тексту і таблиць при необхідності.

Текст звіту про роботу повинен містити:

- мету роботи;
- суть звіту про роботу;
- висновки.

Суть звіту про роботу – це викладення відомостей про предмет практичної роботи, котрий є необхідним й достатнім для розкриття сутності даної роботи (опис: теорії, методів роботи тощо) та її результатів.

При викладенні **суті звіту** особливу увагу приділяють новизні в роботі, а також питання безпеки інформації тощо.

Висновки вміщують безпосередньо після викладення суті звіту про роботу, починаючи з нової строки.

У висновках наводять оцінку одержаних результатів роботи.

Якщо текст висновків має різні смислові аспекти, або містить декілька висновків його треба розбити на розділи, підрозділи, пункти, підпункти, які нумерують арабськими цифрами і друкують з абзацу.

Зразок оформлення титульної сторінки звіту про роботу наведено нижче.

Національний авіаційний університет

Кафедра безпеки інформаційних технологій

ЗВІТ

про лабораторну роботу №___

_____

(назва роботи)

Роботу виконав студент

_____

(ПІБ)

_____ курс, група _____

"___"_____20___р.

Викладач_____

(підпис)

_____

(звання, ПІБ)

Київ 20___

Лабораторна робота № 1

Інформаційне протиборство

Мета роботи: Поглибити теоретичні знання з наступних питань:

- аналіз основних об'єктів впливу в інформаційному протиборстві;
- аналіз типової стратегії інформаційної війни.

Короткі теоретичні відомості:

В даний час в число сфер ведення бойових дій, крім землі, моря, повітря і космосу, додалася і інформаційна сфера. Як підкреслюють військові експерти, основними об'єктами поразки в нових війнах будуть інформаційна інфраструктура і психологія супротивника (з'явився навіть термін «human network»).

Як основні об'єкти впливу в інформаційній війні виступають:

1. Мережі зв'язку та інформаційно - обчислювальні мережі, використовувані державними організаціями при виконанні своїх управлінських функцій;

2. Військова інформаційна інфраструктура, вирішальне завдання управління військами;

3. Інформаційні та керуючі структури банків, транспортних і промислових підприємств;

4. Засоби масової інформації (ЗМІ) (у першу чергу електронні).

Мартін Лібікі визначив 7 різновидів інформаційної війни:

- командно-управлінська,
- розвідувальна,
- психологічна,
- хакерська,
- економічна,
- електронна
- кібервійна.

Командно-управлінська (Command - and - control) війна в якості основного об'єкта впливу розглядає канали зв'язку між командуванням і виконавцями. Перерізаючи «шию» (канали зв'язку), нападаючий ізолює «голову» від «тулуба». Стверджується, що це краще, ніж просто вбивати «голову». Вважається, що Інтернет народився як оборонний варіант цієї війни.

Розвідувальна війна має на меті збір важливої у військовому відношенні інформації та захист власної.

Електронна війна об'єктом свого впливу має кошти електронних комунікацій - радіозв'язку, радарів, комп'ютерних мереж. Її важлива складова - криптографія, що дозволяє здійснювати шифрування і розшифровку електронної інформації.

Психологічна війна здійснюється шляхом пропаганди, «промивання мізків» та іншими методами інформаційної обробки населення.

Лібікі виділяє 4 складові психологічної війни: підрив громадянського духу; деморалізація збройних сил; дезорієнтація командування; війна культур.

Хакерська війна має цілями тотальний параліч мереж, перебої зв'язку, введення помилок у пересилання даних, розкрадання інформації, розкрадання послуг за рахунок несанкціонованих підключень до мереж, їх таємний моніторинг, несанкціонований доступ до закритих даних. Для досягнення цих цілей використовуються різні програмні засоби: віруси, «троянські коні», «логічні бомби», сніффери («нюхалка», «следілкі»).

Економічна інформаційна війна. Лібікі виділяє дві її форми - інформаційну блокаду (спрямована проти США) і інформаційний імперіалізм (метод самих США).

Інформація володіє унікальними властивостями, не властивими іншим секторам економіки. Інформація на відміну від усіх інших ресурсів придатна для багаторазового використання і для численних користувачів, при цьому чим більше вона застосовується, тим цінніше стає. Те ж саме можна сказати про

мережі, що зв'язують різні джерела інформації.

Такий один з підходів до визначення сутності та змісту інформаційної війни.

В умовах, коли час інформаційної протидії між системами малий (наприклад, не перевищує середнього часу життя елемента системи) і система - супротивник має модельованими базовими елементами, можна запропонувати наступний алгоритм, який здавалося б «завжди перемагає»:

1) визначення базових елементів інформаційного простору системи - противника;

2) вивчення індивідуальних особливостей і потенційних можливостей базових елементів;

3) моделювання різних варіантів поведінки базових елементів при різних вхідних впливах;

4) вибір найбільш переважного сценарію ведення базових елементів;

5) підготовка середовища, в якій функціонують базові елементи (громадської думки), і їх самих;

6) реалізація.

З урахуванням вище сказаного загальна схема інформаційної війни могла б виглядати як на рис. 1.

Рис. 1. Типова стратегія інформаційної війни

Наведена схема, безумовно, не відображає всіх можливих підходів і прийомів до організації та проведення операцій з інформаційного впливу. Розум людський більш витончений, ніж будь-яка можлива проекція генеруючих ним думок в площину практичних алгоритмів. У типову стратегію включено лише те, що випливає з доведених раніше теорем, тверджень і наслідків. Звідси випливає: якщо інформаційна система виявляє вплив проти себе комплексу прийомів схеми рис. 1, то це може означати, що дана інформаційна система перебуває в стані інформаційної війни.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Ярочкин В.И. Информационная безопасность / Ярочкин В.И. – М.: Академический проект, 2003. – 640 с.

3. Богуш В.М. Інформаційна безпека держави / Богуш В.М., Юдін О.К. – К.: "МК-Пресс", 2005. – 432 с.

4. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №1 відповідно з номером бригади, наведено в табл. 1.
4. Проаналізувати роботу.
5. Зробити порівняльний аналіз.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 1

Завдання для виконання лабораторної роботи №1

Номер бригади	Завдання
1	Знайти книгу М. Лібікі "Що таке інформаційна війна?" і визначити поняття командно-управлінської та психологічної війни
2	Знайти книгу М. Лібікі "Що таке інформаційна війна?" і визначити поняття електронна війна і кібервійна
3	Знайти книгу М. Лібікі "Що таке інформаційна війна?" і визначити поняття розвідувальної та економічної війни
4	Знайти книгу М. Лібікі "Що таке інформаційна війна?" і визначити поняття хакерська, електронна та кібервійни
5	Знайти книгу Расторгуєва С.П. "Філософія інформаційної війни" і визначити поняття саморуйнівна та самовідроджувальна інформаційні структури
6	Знайти книгу Расторгуєва С.П. "Філософія інформаційної війни" і визначити поняття проблеми початку і наслідки інформаційної війни
7	Знайти книгу Расторгуєва С.П. "Філософія інформаційної війни" і визначити поняття явні інформаційні загрози і приховані інформаційні загрози

Контрольні питання:

1. Що виступає основними об'єктами впливу в інформаційній війні?
2. Які 7 різновидів інформаційної війни визначив Мартін Лібікі?
3. Що таке алгоритм перемоги?
4. Типова стратегія інформаційної війни?

Лабораторна робота № 2

Аналітичне забезпечення інформаційної безпеки

Мета роботи: Поглибити теоретичні знання з наступних питань:

- аналіз методів інформаційно - аналітичної роботи;
- аналіз джерел отримання інформації;
- аналіз методів обробки інформації.

Короткі теоретичні відомості:

Інформаційно-аналітична робота (ІАР) - це визначення необхідної інформації, її пошук, систематизація, складання висновків і їх розповсюдження.

ІАР включає в себе весь процес створення аналітичної інформації, що складається з декількох етапів: організація збору та первинної обробки матеріалу, власне аналіз і виборче поширення інформації.

Етапи ІАР:

• визначення необхідної інформації і напрямків її пошуку;

• збір інформації;

• первинна обробка інформації;

• аналіз (тобто знаходження причинно - слідчих та інших зв'язків між фактами, явищами і т.д.);

• оцінка інформації і виробництво аналітичного продукту (відсів несуттєвих фактів, сортування та визначення достовірності фактів і подій, формулювання висновків);

• дозоване поширення інформації (підготовка аналітичних записок і звітів). На даному етапі пріоритетними є питання переконливості підготовленого документа, встановлення рамок допуску та вміння зацікавити людину (або організацію), на адресу якої спрямований документ.

Функції і завдання ІАР:

1. Збір попереджувальної інформації для виявлення осіб і організацій, що

спеціалізуються на зазіханнях у сфері інтересів підприємства, що охороняється.

2. Відстеження оперативної обстановки, що виникає навколо підприємства, що охороняється, тобто фіксація подій та осіб, дозволяє виявити ознаки підготовки недружніх акцій.

3. Приховані методи розслідування, виявлення розкрадачів серед співробітників підприємства, що охороняється, відстеження каналів витоку конфіденційної інформації.

4. Створення системи взаємовідносин та контактів з офіційними структурами та ЗМІ, дозволяє отримувати попереджуючу інформацію про підготовку недружніх акцій.

5. Аналіз відкритих і конфіденційних джерел на предмет встановлення витоку інформації, забезпечення охорони інтересів підприємства, встановлення та запобігання спроб проникнути в конфіденційну інформацію.

Джерела отримання інформації можна розділити на три категорії: відкриті, напівідкриті, закриті.

Обробка отриманої інформації - справа, що вимагає скрупульозності в обліку найдрібніших деталей і точності в оформленні. Оброблений масив інформаційної документації повинен відповідати кільком вимогам: доступність, інваріантність, коректування.

Під доступністю розуміється можливість роботи з інформацією для людини не створюючи бази даних. Наприклад, директора підприємства, уточнюючого інформацію, або нового аналітика, що прийшов на зміну, наприклад, загиблому в автокатастрофі.

Інваріантність передбачає доступ до інформаційних осередкам, об'єднаним різними класифікаторами. Наприклад, доступ до інформації певного джерела, доступ до інформації з певної справи з різною сортуванням, доступ до джерел з вищою категорією надійності тощо.

Коригування припускає можливість модифікації бази даних. Під

модифікацією можуть розумітися видалення відомостей, що стали непотрібними або небезпечними, відомостей додавання нової інформації, внесення змін до кодуванні і т.п.

Таким чином, інформаційний масив проходить первинну обробку і перетворюється в базу даних або доповнює її.

Виділяють дві основні групи методів: стратегічні і тактичні. Стратегічні методи інакше називають узагальненими. Вони дозволяють розглянути ситуацію цілком. По суті вони є аналітичними. Тактичні методи дозволяють деталізувати картину того, що відбувається і виділити ключові події, тобто - синтетичними методами пізнання.

Основні стратегічні методи аналітичної роботи моделювання і системний аналіз.

Моделювання - створення узагальнених і спрощених моделей ситуацій. Часто подія (набір фактів) складно аналізувати як таке. У випадку підбирається подія, в основному відповідає основним характеристикам, але більш просте для аналізу.

Одним з типових принципів моделювання статистики є числова або математична модель. Статистика дозволяє зробити узагальнюючий висновок по вже відомій ситуації, виходячи з якої можна припускати ситуацію майбутню.

Існує три основних способи аналітичної роботи: одиночний, парний, «мозковий штурм».

Одиночний образ - робота окремого аналітика. Аналітик сам вибирає методи дослідження, проводить необхідну роботу, готує висновок. Виділяють кілька типів аналітичних працівників залежно від використання ними прийомів роботи.

• Художник. На аркуші паперу олівцем графічно відзначаються факти, і між ними шикуються взаємозв'язку. Картинка наочна, її легко виправити (за допомогою ластику і пару штрихів). В результаті малювання такої картинки

досить нескладно відсіяти малозначні факти і ви ділити найбільш важливі. У результаті такого малювання слід центральний факт або прогноз розвитку логічного ланцюжка.

• Комбінатор. На паперових картках надписуються відповідні факти. Після цього картки розкладаються у відповідному порядку, міняються місцями і т. п. У результаті відновлюється вся логічний ланцюжок, яку можна продовжити.

• Лектор. Аналітик каже відомі факти, намагається їх логічно вибудувати, як би читаючи лекцію. У результаті такої промови слідують забуті деталі, передбачаються нові напрямки пошуку, виводяться підсумки дії. Часто після такого варіанту аналізу події зв'язуються в дуже послідовний логічний ланцюжок, висновок стає дуже явним.

• Чертежник (або математик). Такий фахівець любить надавати своїй роботі числовий варіант і переносити її на графіки. Далі йде аналіз функції за графіком.

Парна робота передбачає обговорення проблеми парою аналітиків. При цьому зазвичай йде робота на протилежностях оптиміст - песиміст, синтетик - критик, кореспондент - респондент і т.п. Оптиміст розглядає проблему з точки зору бажаного результату песиміста, припускаючи найгірший варіант. Синтетик створює логічний ланцюжок подій. Критик висловлює зауваження навіть по найдрібніших деталях, кореспонденту задає "незручні" питання, а респондент намагається на них відповісти в результаті формується точка зору влаштовує обох аналітиків.

«Мозковий штурм» є дуже ефективним прийомом роботи злагодженої групи фахівців. «Мозковий штурм» - оперативний метод аналізу проблеми групою фахівців з усіх ракурсів і пошук неадекватних і несподіваних способів її вирішення.

Аналітичний висновок має бути доказовий, що перевірявся, стислий і

необхідний.

1. Показність виводу. Виявляється в тому, що він повинен бути повністю підтверджений кодом аналітичного дослідження. Непідтверджена частина виведення цьому правилу не задовольняє і використовуватися не може.

2. Висновку полягає в можливості перевірити в майбутньому або по інших каналах вірність викладок.

3. Стислість необхідна для керівника. Як говорилося на початку, аналітичний підрозділ стає необхідним тоді, коли керівник не може справлятися з інформаційним потоком. Тому висновки аналітика повинні бути короткими і точними. В іншому випадку аналіз втрачає свою цінність для керівника.

4. Необхідність аналітичного висновку диктується тими ж умовами. Аналітик повинен займатися тільки тим напрямкам аналізу, які перспективні для керівника підприємства. Вимагає високого професіоналізму і максимального рівня аналітичного мислення, систематизації фактів і визначення можливих наслідків безпосередньо. Тому для полегшення роботи часто використовується прийом роботи «з кінця». Спочатку визначається можливий висновок, після цього всі факти підтасовуються під нього. Висновок вважається коректним, коли під нього підійшли всі наявні у аналітика факти.

Правила інформаційно - аналітичної роботи:

1. Правило формулювання ланцюга. Необхідно визначити, в яких цілях будуть використані результати ІАР. Від цього залежить масштаб, методи і спосіб вирішення завдання. Перед аналітиком повинні бути поставлені конкретні зрозумілі ланцюга.

2. Правило визначення понять полягає в точному визначенні сенсу кожного терміна, використовуваного в ІАР. Слід виявити коло термінів, понять, які повинні мати чітке визначення і трактуватися однозначно.

3. Правило використання всіх можливих джерел інформації з даної

тематики. Аналітику доводиться працювати з інформацією, яку він в даний момент. Чекати повноцінної інформації від надійного джерела - значить втрачати час. Необхідно відпрацювати всі можливі джерела, визначити достовірність кожного інформаційного центру та працювати виходячи з даних фактів.

4. Правило інтерпретації фактів. Передбачає розкриття сенсу значення фактів, зіставлення їх з аналогічними, що мали місце раніше.

5. Правило встановлення причинно - наслідкових зв'язків. У будь-якому випадку, необхідно встановити причини розглянутої події і виділити її слідства.

6. Правило визначення тенденції розвитку об'єкта. Необхідно припускати, як дана подія буде розвиватися. Треба визначити можливі шляхи її розвитку, сигнальні події для кожного варіанту розвитку, свої майбутні дії.

7. Правило встановлення ступеня достовірності. Це правило застосовується до всіх аналітичних досліджень. З урахуванням якості отриманої інформації та кваліфікації аналітика, якість (вірогідність) висновку може бути високим, середнім або низьким.

8. Правило коректності висновків. Правило допускає довільності висновків. Важливо пам'ятати, що висновки повинні підтверджуватися базовою інформацією. Інша важлива вимога до висновків - необхідність змісту відповіді на поставлене запитання.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Єжова Л.Ф. Управління інформаційною безпекою. В 2-х томах \ Єжова Л.Ф., Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. – К.: Вид-во НАУ, 2012.

3. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №2 відповідно до нормеру бригади наведено в табл. 2.
3. Знайти інформацію відповідно до завдання.
4. Оформити звіт.
5. Зробити висновки відповідно з оформленням інформаційно - аналітичної довідки.

Таблиця 2.

Завдання для виконання лабораторної роботи №2

Номер бригади	Завдання
1	Знайти матеріали по первинній обробці інформації та охарактеризувати її особливості, недоліки та переваги.
2	Знайти матеріали про відкриті і конфіденційні джерела. Провести їх порівняння і охарактеризувати.
3	Знайти матеріали про стратегічні і тактичні методи. Навести їх порівняння, проаналізувати і охарактеризувати.
4	Знайти матеріали про способи аналітичної роботи: одиночний і "мозковий штурм". Проведіть їх порівняння, охарактеризуйте та проаналізуйте.
5	Знайти матеріали про способи аналітичної роботи: одиночний і парний Проведіть їх порівняння, охарактеризуйте та проаналізуйте.
6	Знайти матеріали про способи аналітичної роботи: парний і "мозковий штурм". Проведіть їх порівняння, охарактеризуйте та проаналізуйте
7	Знайти матеріали про типи одиночних аналітиків. Проведіть їх порівняння між собою, охарактеризуйте та проаналізуйте.

Контрольні питання:

1. Етапи аналітичного забезпечення?
2. Функції та завдання інформаційно-аналітичної роботи?
3. Організація інформаційно-аналітичної роботи?

4. Джерела отримання інформації?
5. Обробка отриманої інформації?
6. Методи аналітичної роботи?
7. Способи аналітичної роботи?
8. Структура аналітичного висновку?
9. Правила інформаційно-аналітичної роботи?

Лабораторна робота № 3

Класифікація технічних засобів забезпечення інформаційної безпеки

Мета роботи: Поглибити теоретичні знання з наступних питань:

- аналіз технічних засобів забезпечення інформаційної безпеки.

Короткі теоретичні відомості:

Визначення потенційної цінності інформації дозволяє подумати в першу чергу про безпеку найбільш важливих секретів, витік яких здатен завдати шкоди. При цьому важливо встановити:

1. Яка інформація потребує захисту?
2. Кого вона може цікавити?
3. Які елементи інформації найбільш цінні?
4. Який "термін життя" цих секретів?
5. У що обійдеться їх захист?

Досвід застосування систем захисту інформації (СЗІ) показує, що ефективною може бути тільки комплексна система захисту інформації (КСЗІ), яка об'єднує такі заходи:

1. Законодавчі. Використання законодавчих актів, що регламентують права та обов'язки фізичних і юридичних осіб, а також держави в області ІБ.

2. Морально - етичні. Створення і підтримка на об'єкті такої моральної атмосфери, у якій порушення регламентованих правил поведінки оцінювалося б більшістю співробітників різко негативно.

3. Фізичні. Створення фізичних перешкод для доступу сторонніх осіб до охоронюваної інформації.

4. Адміністративні. Організація відповідного режиму секретності, пропускного і внутрішнього режиму.

5. Технічні. Застосування електронних та інших пристроїв для СЗІ (див. рис 2).

6. Криптографічні. Застосування шифрування і кодування для приховування інформації, що обробляється і передається від несанкціонованого доступу.

7. Програмні. Застосування програмних засобів розмежування доступу.

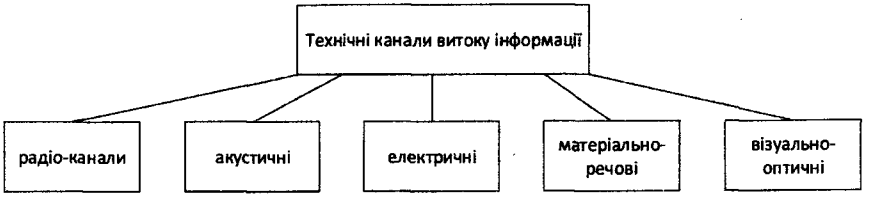


Рис. 2. Класифікація технічних каналів витоку інформації

Обгрунтований вибір необхідного рівня захисту інформації є сістемостворюючім завданням, оскільки як заниження, так і завищення рівня неминуче веде до втрат. При цьому останнім часом роль даного питання різко зросла у зв'язку з тим, що, по-перше, тепер в число захищаються крім військових, державних і відомчих, включені також секрети промислові, комерційні і навіть особисті, а друге, сама інформація всі більше стає товаром.

Таким чином, для оцінки інформації необхідні показники двох видів:

• ті, які характеризують інформацію як ресурс, що забезпечує діяльність товариства;

• ті, які характеризують інформацію як об'єкт праці.

При цьому необхідно враховувати причини утворення каналів витоку інформації (див. рис. 3).

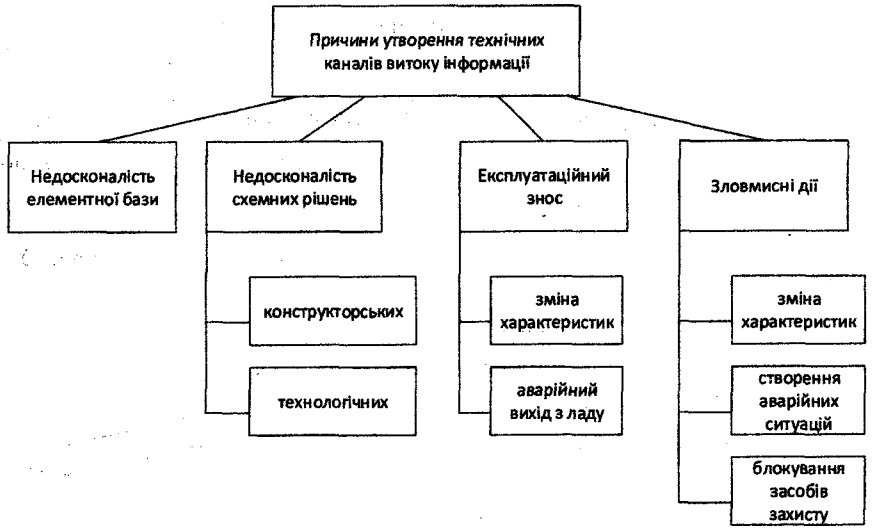


Рис. 3. Причини утворення технічних каналів витоку інформації

Засоби захисту в свою чергу можна розділити на постійно діючі та ті, які включаються при виявленні спроби нападу. За активністю вони діляться на пасивні, напівактивні і активні. За рівнем забезпечення СО засоби захисту діляться на 4 класи: системи слабкого захисту (1 клас), системи сильного захисту, системи дуже сильного захисту, системи особливого захисту.

Класифікація технічних засобів захисту

Технічними називаються такі засоби захисту інформації, в яких основна захисна функція реалізується технічним пристроєм (комплексом або системою).

Безперечними перевагами технічних засобів захисту інформації (ТСЗІ) є:

- досить висока надійність;
- досить широке коло завдань;
- можливість створення комплексних систем захисту інформації (КСЗІ);
- гнучке реагування на спроби несанкціонованого впливу;
- традиційність використовуваних методів здійснення захисних функцій.

Основні недоліки ТСЗІ полягають у наступному:

• висока вартість багатьох засобів;

• необхідність регулярного проведення регламентних робіт і контролю;

• можливість видачі помилкових тривог.

Системну класифікацію ТСЗІ зручно провести за такою сукупністю критеріїв:

• здійснення функції захисту;

• ступінь складності пристрою;

• спряженість із засобами ОТ

Структуризація значень обраних критеріїв наведена на рис. 4.

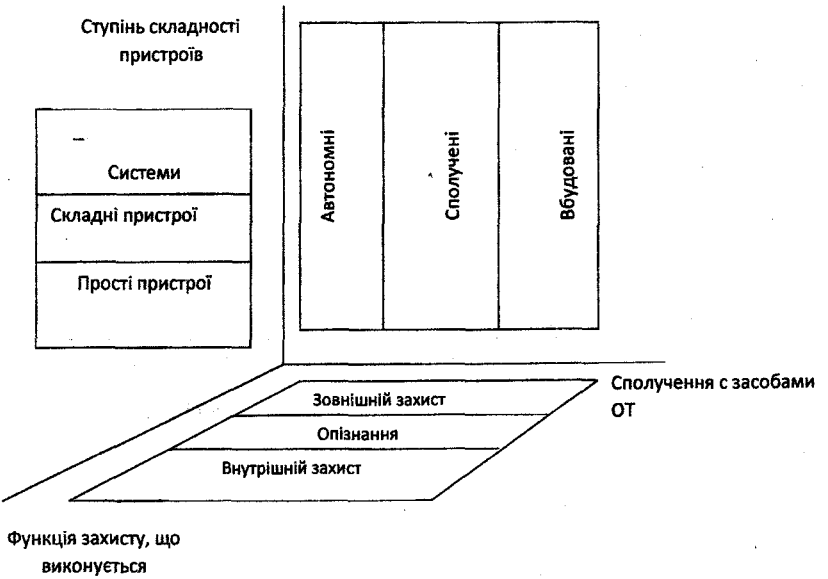


Рис. 4. Класифікація технічних засобів захисту

Наведені значення критеріїв інтерпретуються наступним чином:

• Спряженість із засобами ОТ.

• Автономні - засоби, що виконують свої захисні функції незалежно від функціонування засобів ОТ, тобто повністю автономно.

• Парні - кошти, виконані у вигляді самостійних пристроїв, але виконують захисні функції в поєднанні (спільно) з основними засобами ОТ

• Вбудовані - кошти, які конструктивно включені до складу апаратури ОТ

• Виконувана функція захисту.

• Зовнішній захист - захист від впливу дестабілізуючих факторів, що виявляються за межами зони ресурсів.

• Розпізнавання - специфічна група засобів, призначених для розпізнавання людей з різних індивідуальних характеристик.

• Внутрішній захист - захист від впливу дестабілізуючих факторів, що виявляються безпосередньо в засобах обробки інформації.

• Ступінь складності пристрою.

• Прості пристрої - нескладні прилади і пристосування, які виконують окремі процедури захисту.

• Складні пристрої - комбіновані агрегати, що складаються з деякої кількості простих пристроїв, здатні до здійснення складних процедур захисту.

• Системи - закінчені технічні об'єкти, здатні здійснювати деяку комбіновану процедуру захисту, має самостійне значення.

Якщо кожен елемент класифікаційної структури представити в якості групи ТСЗІ, то повний арсенал цих коштів буде включати 27 відносно самостійних груп.

Відповідно до класифікації у функціональному відношенні, головне значення має класифікація за виконуваної функцією. Класифікація ж за критеріями спряженості і ступеня складності відображає, головним чином, тільки особливості конструктивної та організаційної реалізації ТСЗІ.

Як вже було сказано, виділяють три макрофункції захисту, що виконуються ТСЗІ: зовнішній захист, розпізнавання та внутрішній захист. Подальша деталізація функціональної класифікації ТСЗІ призводить до виділення 11-ти груп. ТСЗІ, які входять у ці групи, можуть бути різної складності і різного виконання. До теперішнього часу розроблено велику кількість різних ТСЗІ, багато з яких випускаються серійно.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов В.А., Хорошко В.А. – К.: Арий, 2008.

3. Пановский В.В. Защита информации в телекомуникационных сетях. В 2-х томах. – Харьков: ООО "Компания СМИТ", 2006.

4. Емельянов С.Л. Проблемы защиты информации от утечки и пути ее решения / Емельянов С.Л., – Одесса: Феникс, 2011. – 624 с.

5. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №3 відповідно з номером бригади приведено в табл. 3.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3

Завдання для виконання лабораторної роботи №3

Номер бригади	Завдання
1	Знайдіть матеріали про акустичні та електричні канали витоку інформації. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.
2	Знайдіть матеріали про електричні та радіотехнічні канали витоку інформації. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.
3	Знайдіть матеріали про автономні складні системи захисту, що забезпечують внутрішній захист і вбудовані складні системи. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.
4	Знайдіть матеріали про прості сполучені пристрої впізнання і складні вбудовані пристрої впізнання. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.
5	Знайдіть матеріали про складну вбудовану зовнішню систему захисту і складну сполучену зовнішню систему захисту. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.
6	Знайдіть матеріали про систему вбудованого внутрішнього захисту і систему сполученого внутрішнього захисту. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.
7	Знайдіть матеріали про складні пристрої автономного зовнішнього захисту і системи автономного зовнішнього захисту. Проведіть їх порівняння, охарактеризуйте, проаналізуйте, визначте переваги і недоліки.

Контрольні питання:

1. Заходи КСЗІ?
2. Класифікація технічних каналів витоку інформації?
3. Причини утворення технічних каналів витоку інформації?
4. Класифікація технічних засобів захисту інформації?
5. Переваги та недоліки технічних засобів захисту інформації?
6. Критерії ТСЗІ?

Лабораторна робота № 4

Класифікація програмних та криптографічних засобів забезпечення інформаційної безпеки

Мета роботи:

- аналіз програмних засобів забезпечення інформаційної безпеки;
- аналіз криптографічних засобів забезпечення інформаційної безпеки.

Короткі теоретичні відомості:

Програмними СЗІ називаються спеціальні програми, що входять до складу програмного забезпечення АС для вирішення в них (самостійно або в комплекті з іншими засобами) завдань захисту. Програмні СЗІ є неодмінною і важливою частиною механізму захисту сучасних АС. Така їх роль визначається наступними перевагами: універсальністю, гнучкістю, простий реалізацією, надійністю, можливістю модифікації і розвитку.

Загальноприйнятої класифікації програмних СЗІ в даний час не існує. Однак при описі програм захисту зазвичай дотримуються розподілу їх за функціональною ознакою, тобто по виконуваних функцій захисту. При цьому в міру розвитку форм і способів використання обчислювальної техніки функції програмного захисту розширюються.

З урахуванням названих принципів можна використовувати класифікацію, наведену на рис. 5.

Рис. 5. Класифікація програмних СЗІ

При цьому під зовнішнім захистом розуміється сукупність засобів, методів і заходів, спрямованих на захист території, на якій розташовані будівлі обчислювальних центрів і приміщень, в яких розташовані їхні елементи. Поняття внутрішнього захисту охоплює сукупність засобів, методів і заходів, спрямованих на СО, оброблюваної в АС. До складу ядра системи безпеки входять програми, що забезпечують захист самої СЗІ.

В даний час не існує закінченої і загальноприйнятої класифікації криптографічних методів, так як багато хто з них знаходяться в стадії розвитку і становлення.

Під шифруванням в даному випадку розуміється такий вид криптографічного закриття, при якому перетворенню піддається кожен символ захищається повідомлення. Всі відомі способи шифрування розбиті на п'ять груп: підстановка (заміна), перестановка, аналітичне перетворення, гамування і комбіноване шифрування. Кожен з цих способів може мати кілька різновидів.

Під кодуванням розуміється такий вид криптографічного закриття, коли деякі елементи даних, що захищаються (не обов'язково окремі символи)

замінюються заздалегідь вибраними кодами (цифровим, літерними, буквено - цифровими поєднаннями тощо. Цей метод має два різновиди: смислове та символьне кодування. При смисловому кодуванні кодуються елементи, які мають цілком певний сенс (слова, пропозиції, групи пропозицій). При символьному кодуванні кодується кожен символ захищається тексту. Символьне кодування по суті збігається з підстановлювальний шифруванням.

До окремих видів криптографії належать методи розсічення - рознесення і стиснення. Розсічення - рознесення полягає в тому, що масив даних, що захищаються ділиться (розтинають) на такі елементи, кожен з яких окремо не дозволяє розкрити зміст інформації, що захищається. Виділені таким чином елементи даних розносяться по різних зонах пам'яті або розташовуються на різних носіях. Стиснення даних являє собою заміну часто зустрічаються однакових рядків даних або послідовностей однакових символів деякими заздалегідь вибраними символами.

Оскільки криптографічні методи СО застосовуються давно, то вже є сформульовані основні вимоги до них.

1. Метод повинен бути надійним, тобто відновлення відкритого тексту при володінні тільки шифротекста, але не ключем повинно бути практично нездійсненною завданням.

2. Через труднощі запам'ятовування обсяг ключа не повинен бути більшим.

3. Через труднощі, пов'язані зі складними перетвореннями, процеси шифрування повинні бути простими.

4. Через можливість появи помилок передачі дешифрування шифротекста, що містить окремі помилки, не повинно привести до нескінченного збільшення помилок в отриманому передбачуваному відкритому тексті.

5. Через труднощі передачі обсяг шифротекста не повинен бути значно

більше відкритого тексту.

Перераховані вимоги були розроблені для традиційної криптографії.

При сучасному розвитку техніки необхідність задоволення перерахованим вимогам зазнає істотні зміни.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Задруга", 2013. – 170 с.

2. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

3. Горбенко І.Д. Прикладна криптологія: теорія, практика, застосування / Горбенко І.Д., Горбенко Ю.І. – Харків: Вид. "Форт", 2012. – 880 с.

4. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №4 відповідно з номером бригади приведено в табл. 4.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 4

Завдання для виконання лабораторної роботи №4

Номер бригади	Завдання
1	Знайти матеріали про програми зовнішнього захисту. Охарактеризувати їх, визначити переваги і недоліки
2	Знайти матеріали про програми внутрішнього захисту. Охарактеризувати їх, визначити переваги і недоліки
3	Знайти матеріали про програми ядра системи безпеки. Охарактеризувати їх, визначити переваги і недоліки
4	Знайти матеріали про методи шифрування і методи кодування. Охарактеризувати їх, визначити переваги і недоліки. Проведіть їх порівняльний аналіз.
5	Знайти матеріали про кодування та інші види криптографії. Охарактеризувати їх, визначити переваги і недоліки
6	Знайти матеріали про шифрування та інші види криптографії. Охарактеризувати їх, визначити переваги і недоліки
7	Знайти матеріали про комбіновані методи та інші види криптографії. Охарактеризувати їх, визначити переваги і недоліки

Контрольні питання:

1. Що таке програмні СЗІ?
2. Класифікація програмних СЗІ?
3. Класифікація криптографічних методів ЗІ?
4. Вимоги до криптографічних методів ЗІ?

Лабораторна робота № 5

Загрози безпеки

Мета роботи: Поглибити теоретичні знання з наступних питань:

- класифікації загроз;
- аналіз найбільш застосовуваних загроз.

Короткі теоретичні відомості:

Загроза - це потенційна можливість певним чином порушити інформаційну безпеку.

Спроба реалізації загрози називається атакою, а той, хто здійснює таку спробу - зловмисником. Потенційні зловмисники називаються джерелами загроз.

Найчастіше загроза є наслідком наявності вразливих місць в захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки в програмному забезпеченні).

Проміжок часу від моменту, коли з'являється можливість використовувати слабке місце, і до моменту, коли пробіл ліквідується, називається вікном небезпеки, асоційованим з даними вразливим місцем. Поки існує вікно небезпеки, можливі успішні атаки на ІС.

Уразливі місця і засоби їх використання з'являються постійно; це означає, по-перше, що майже завжди існують вікна небезпеки і, по-друге, що відстеження таких вікон повинно проводитися постійно, а випуск і накладення латок - якомога оперативніше.

Відзначимо, що деякі загрози не можна вважати наслідком якихось помилок чи прорахунків; вони існують в силу самої природи сучасних ІС.

Розглянемо найбільш поширені загрози, яким піддаються сучасні інформаційні системи. Мати уявлення про можливі загрози, а також про вразливі місця, які ці загрози зазвичай експлуатують, необхідно для того, щоб

вибирати найбільш економічні засоби забезпечення безпеки. Занадто багато міфів існує в сфері інформаційних технологій, тому незнання в цьому випадку веде до перевитрати коштів і, що ще гірше, до концентрації ресурсів там, де вони не дуже потрібні, за рахунок ослаблення дійсно вразливих напрямків.

Підкреслимо, що саме поняття "загроза" в різних ситуаціях часто трактується по-різному. Наприклад, для підкреслено відкритої організації погроз конфіденційності може просто не існувати - вся інформація вважається загальнодоступною; проте в більшості випадків нелегальний доступ є серйозною небезпекою. Іншими словами, загрози, як і все в ІБ, залежать від інтересів суб'єктів інформаційних відносин (і від того, який збиток є для них неприйнятним).

Ми спробуємо подивитися на предмет з точки зору типової (на наш погляд) організації. Втім, багато загроз (наприклад, пожежа) небезпечні для всіх.

Загрози можна класифікувати за кількома критеріями:

- за аспектом інформаційної безпеки (доступність, цілісність, конфіденційність), проти якого загрози спрямовані в першу чергу;
- за компонентами інформаційних систем, на які загрози націлені (дані, програми, апаратура, підтримуюча інфраструктура);
- за способом здійснення (випадкові/навмисні дії природного/техногенного характеру);
- за розташуванням джерела загроз (всередині/поза розглянутим ІС).

В якості основного критерію будемо використовувати перший (по аспекту ІБ), залучаючи при необхідності інші.

Поширені загрози доступності

Частими і небезпечними (з погляду розміру шкоди) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи.

Іноді такі помилки і є власне погрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (такі помилки адміністрування). За деякими даними, до 65% втрат - наслідок ненавмисних помилок.

Пожежі та повені не приносять стільки бід, скільки безграмотність і недбалість у роботі.

Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками - максимальна автоматизація і строгий контроль.

Інші загрози доступності класифікуємо за компонентами ІС, на які націлені загрози:

- відмова користувачів;
- внутрішня відмова інформаційної системи;
- відмова підтримуючої інфраструктури.

Звичайно, щодо користувачів розглядаються наступні загрози:

- небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості і при розбіжності між запитами користувачів і фактичних можливостей і технічних характеристик);
- неможливість працювати з системою в результаті відсутності відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і т.п.);
- неможливість працювати з системою в результаті відсутності технічної підтримки (неповнота документації, недолік довідкової інформації тощо).

Основними джерелами внутрішніх відмов є:

- відступ (випадковий або навмисний) від встановлених правил експлуатації;

• вихід системи з штатного режиму експлуатації внаслідок випадкових або навмисних дій користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації тощо);

• помилки при переконфігуруванні системи;

• відмови програмного та апаратного забезпечення;

• руйнування даних;

• руйнування або пошкодження апаратури.

Щодо підтримуючої інфраструктури рекомендується розглядати наступні загрози:

• порушення роботи (випадково чи навмисно) систем зв'язку, електроживлення, водо-та / або теплопостачання, кондиціонування;

• руйнування або пошкодження приміщень;

• неможливість або небажання обслуговуючого персоналу та / або користувачів виконувати свої обов'язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк і т.п.).

Досить небезпечні так звані "скривджені" співробітники - нинішні і колишні. Як правило, вони прагнуть завдати шкоди, організації - "кривднику", наприклад:

• зіпсувати обладнання;

• вбудувати логічну бомбу, згодом зруйнує програми та / або дані;

• видалити дані.

Небезпечні, зрозуміло, стихійні лиха та події, які сприймаються як стихійні лиха: пожежі, повені, землетруси, урагани. За статистикою, на частку вогню, води і тому подібних "зловмисників" (серед яких найнебезпечніший - перебій електроживлення) припадає 13% втрат, завданих інформаційним системам.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов В.А., Хорошко В.А. – К.: Арий, 2008.

3. Пановский В.В. Защита информации в телекомуникационных сетях. В 2-х томах. – Харьков: ООО "Компания СМИТ", 2006.

4. Емельянов С.Л. Проблемы защиты информации от утечки и пути ее решения / Емельянов С.Л., – Одесса: Феникс, 2011. – 624 с.

5. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №5 відповідно з номером бригади приведено в табл. 5.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 5

Завдання для виконання лабораторної роботи №5

Номер бригади	Завдання
1	Знайти матеріал про критерії, за якими здійснюється класифікація. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.
2	Знайти матеріал про загрози доступності. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.
3	Знайти матеріал про загрози користувачам. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.
4	Знайти матеріал про загрози підтримуючої інфраструктури. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.
5	Знайти матеріал про шкідливе програмне забезпечення. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.
6	Знайти матеріал про загрози цілісності інформації. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.
7	Знайти матеріал про загрози цілісності та доступності інформації. Оцінити їх достоїнства і недоліки, провести їх порівняльний аналіз.

Контрольні питання:

1. Поняття та види загроз?
2. Класифікація загроз?
3. Шкідливе програмне забезпечення?
4. Загрози цілісності?
5. Загрози конфіденційності?
6. Основні джерела внутрішніх відмов?

Лабораторна робота № 6

Системна класифікація та характеристики технічних засобів забезпечення інформаційної безпеки

Мета роботи: Поглибити теоретичні знання з наступних питань:

- аналізу класифікації ТСЗІ;
- аналізу вимог до систем захисту інформації;
- аналізу підсистем всій СЗІ.

Короткі теоретичні відомості:

Для управління доступом в приміщення широкого поширення набули замки з кодовим набором. Крім того, для захисту приміщень широко використовуються датчики, які можуть бути розділені на три групи:

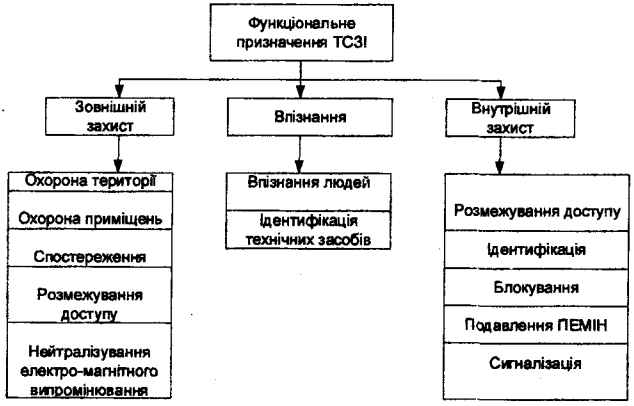


Рис. 6. Класифікація ТСЗІ за функціональним призначенням

• датчики для виявлення спроб проникнення на територію об'єкта або в приміщення, що контролюється;

• датчики для виявлення присутності людини в приміщенні;

• датчики для виявлення переміщення предмета, що охороняється.

Відповідно до вимог з технічного захисту на кожному об'єкті, що охороняється, встановлюються такі типи пожежно-захисних систем:

• зовнішні системи сигналізації проникнення;

• внутрішні системи сигналізації проникнення;

• системи сигналізації пожежної охорони.

Внутрішні системи сигналізації проникнення діляться на однорубіжні, дворубіжні і багатозонні.

Структурна схема однорубіжної охоронної системи сигналізації передбачає побудову шлейфу сигналізації з сповіщувачами, дають інформацію на пульт центрального спостереження (ПЦС) про порушення шлейфу або його обрив, а також можливість керувати виносними світловими і звуковими сигналізаторами.

Дворубіжна охоронна система сигналізації передбачає організацію двох рубіжах охорони об'єкта.

Для першого рубіжу доцільно використовувати сповіщувачі, що забезпечують розмикання контактів, а для другого - охоронні сповіщувачі об'ємної дії. Перевага другого варіанта полягає в уточненій селекції сигналів спрацьовують охоронних сповіщувачів на другому рубіжі охорони.

Структурна схема організації багатозонної системи захисту дозволяє здійснювати охорону до шістнадцяти зон всередині об'єкта. Використовується дворубіжна охоронна система сигналізації з можливістю виключення деяких зон, причому охорона інших міститься в робочому стані.

Зовнішні системи сигналізації проникнення служать для надійної сигналізації про проникнення через зони, забезпечені огородженнями (на особливих об'єктах таких огорож може бути дві).

Зазвичай зона ділиться датчиками системи сигналізації на ділянки довжиною 100-300 м. Як датчики зазвичай використовуються: гідравлічний сигналізатор шуму, датчик магнітного поля УКХ, мікрохвильовий сигналізатор

та інфрачервоні шлагбауми.

Датчики сигналізації фіксують і перетворюють сигнал проникнення через ділянки в електричний сигнал, який подається по кабелю до пульта обробки сигналів, який знаходиться в приміщенні ПНЦ. Часто до пульта підключаються ПЕОМ та друкувальний пристрій, автоматично реєструють час і ділянка проникнення.

Системи внутрішнього сигналізації класифікуються за способом підключення датчиків до ПКП. Виділяють провідні і бездротові системи. Бездротові системи зручніші при монтажі та використанні, але характеризуються більшою ймовірністю помилкових спрацьовувань.

Пристроями охоронної сигналізації обладнуються вхідні двері, запасні виходи і ворота, вікна і вітражі, приміщення та їх елементи (стіни, стелі, підлоги), проходи, окремо розташовані шафи і сейфи.

У цих системах використовуються датчики наступних типів: пасивні інфрачервоні датчики тиску, фотоелектричні датчики, мікрохвильові датчики, ультразвукові датчики, магнітні датчики, датчики розбиття скла і вібродатчики.

Останнім часом промисловість налагодила випуск спеціальних технічних засобів охорони: оптоелектронних, ультразвукових, ємнісних, радіохвильових т.д., що дозволяють організувати багаторубіжними охоронну сигналізацію з селективної передачі сигналів про спрацювання конкретного охоронного сповіщувача на ПЦС.

Для захисту приміщень широко застосовуються також лазерні та оптичні системи, датчики яких спрацьовують при перетині порушником світлового променя.

Пристрої та системи розпізнавання застосовуються, в основному, в системах управління доступом в захищаються приміщення. Це завдання вирішується з використанням не тільки фізичних, а й апаратних і програмних засобів.

Вимоги до ПЗ визначаються власником інформації та узгоджуються з виконавцем робіт з проектування і створення СЗІ.

Згідно ДСТУ 3396.0-96 і ГОСТ 3396.1-96 визначено основні положення та порядок робіт зі створення СЗІ. Ці стандарти встановлюють об'єкт захисту, мету, основні організаційно - технічні положення СЗІ, неправомірний доступ до якої може завдати шкоди громадянам, організаціям, державі, а також категорії нормативних документів з СЗІ та вимоги до порядку проведення робіт з технічного захисту.

Виходячи з цих документів, метою СЗІ є запобігання витоку або порушення цілісності інформації з обмеженим доступом (ІзОД).

Мета КСЗІ може бути досягнута побудовою СЗІ, яка є організованою сукупністю методів і засобів забезпечення СЗІ.

Зміст і послідовність робіт з протидії загрозам або їх нейтралізації повинні відповідати зазначеним у ГОСТ 3396.0-96 етапи функціонування систем захисту інформації, відповідно до ГОСТ 3396.1-96, і полягати в:

- проведенні обстеження об'єкта (підприємства, установи, організації);

- розробці реалізації організаційних, первинних технічних, основних технічних з заходів з використанням засобів забезпечення ТЗІ;

- прийому робіт з ТЗІ;

- атестації засобів (систем) забезпечення інформаційної діяльності на відповідність вимогам нормативних документів системи ТЗІ.

У процесі формування вимог до СЗІ доцільно знайти відповіді на наступні питання:

- Заходи безпеки пропонується використовувати?

- Яка вартість доступних програмних і технічних заходів захисту?

- Наскільки ефективні доступні заходи захисту?

- Наскільки уразливі підсистемі СЗІ?

- Є можливість провести аналіз ризику?

Сукупність вимог до СЗІ наведена на рис. 7.

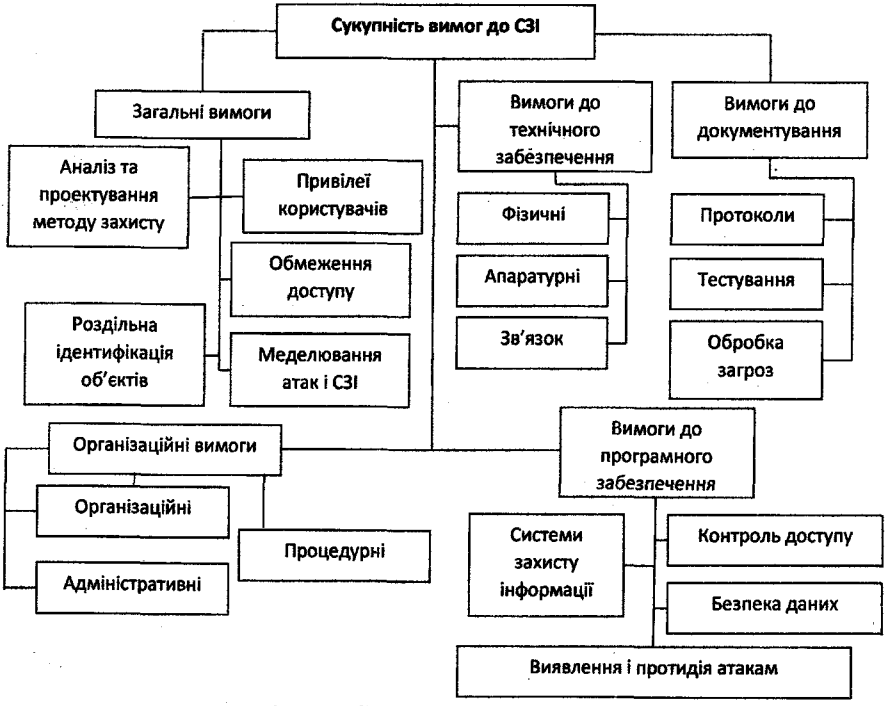


Рис. 7. Сукупність вимог до СЗІ

У загальному випадку доцільно виділити наступні групи вимог до СЗІ:

- Загальні вимоги;

- Організаційні вимоги;

- Конкретні вимоги до підсистем захисту, технічного та програмного забезпечення, документування, способів і методів захисту.

Загальні вимоги. Перш за все, необхідна повна ідентифікація користувачів, терміналів, програм, а також основних процесів і процедур, що відбуваються на об'єкті захисту. Крім того, слід обмежити доступ до інформацій, використовуючи сукупність таких способів:

- Ієрархічна класифікація доступу;

- Класифікація інформації за важливістю і місцем виникнення;

- Вказівки обмежень до інформаційних об'єктів;

- Визначення програм і процедур, наданих тільки конкретному користувачем

СЗІ повинна гарантувати, що будь - рух інформації ідентифікується, авторизується, виявляється і документується.

Зазвичай формулюються загальні вимоги до СЗІ, які відповідають наступним характеристикам:

- Способам побудови СЗІ або її окремих компонентів;

- Архітектурі засобів обчислювальної техніки та інформаційних систем (в клас і мінімальній конфігурації ЕОМ, операційного середовища, орієнтації на ту чи іншу програмну і апаратну (технічна) платформи);

- Застосування стратегії захисту;

- Витрат ресурсів на забезпечення СЗІ;

- Надійності та живучості функціонування СЗІ;

- Числа ступенів секретності підтримуваних СЗІ;

- Забезпеченню швидкості обміну інформацією на об'єкті, в тому числі з урахуванням використовуваних криптографічних вимог;

- Кількості підтримуваних СЗІ рівнів повноважень;

- Можливості СЗІ обслуговувати певну кількість користувачів;

- Тривалість процедури генерації програмної версії СЗІ;

- Тривалість процедури підготовки СЗІ до роботи після подачі живлення на компоненти об'єкта;

- Можливість СЗІ реагувати на спроби несанкціонованого доступу або атаки ззовні;

- Наявності і забезпечення автоматизованого робочого місця адміністратора СО;

- Склад використовуваного програмного та лінгвістичного забезпечення, до його сумісності з іншими програмними платформами, до можливості модифікації і т.п.;

- Використовуваних компонентів СЗІ, що купуються (наявність ліцензії, сертифіката тощо).

Організаційні вимоги до системи захисту передбачають реалізацію сукупності адміністративних і процедурних заходів.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов В.А., Хорошко В.А. – К.: Арий, 2008.

3. Конеев И.Р. Информационная безопасность предприятия / Конеев И.Р., Беляев А.В. – СПб.: БХВ-Петербург, 2003. – 752 с.

5. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №6 відповідно з номером бригади приведено в табл. 6.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 6

Завдання для виконання лабораторної роботи №6

Номер бригади	Завдання
1	Знайти матеріал про загальні вимоги до СЗ, проаналізувати їх і провести порівняльний аналіз.
2	Знайти матеріал про організаційні вимоги до СЗ, проаналізувати їх і провести порівняльний аналіз.
3	Знайти матеріал про технічні вимоги до СЗ, проаналізувати їх і провести порівняльний аналіз.
4	Знайти матеріал про вимоги до програмного забезпечення, проаналізувати їх і провести порівняльний аналіз.
5	Знайти матеріал про вимоги до документування, проаналізувати їх і провести порівняльний аналіз.
6	Знайти матеріал про підсистему забезпечення цілісності та достовірності, проаналізувати їх і провести порівняльний аналіз.
7	Знайти матеріал про підсистему управління доступом, проаналізувати їх і провести порівняльний аналіз.

Контрольні питання:

1. Класифікація ТСЗІ за функціональним призначенням?
2. Типи пожежно-захисних систем?
3. Вимоги до технічних засобів інформаційної безпеки?
4. Сукупність вимог до систем захисту інформації?
5. Організаційні заходи, що підвищують ефективність захисту інформації?
6. Основні положення за створення СЗІ?

Лабораторна робота № 7

Електронна ідентифікація користувачів

Мета роботи: Поглибити теоретичні знання з наступних питань:

- ідентифікація та аутентифікація;
- аналіз важливих заходів щодо дозволу на отримання інформації;
- аналіз рішень про надання доступу до інформації;
- аналіз біометричних методів надання доступу до інформації.

Короткі теоретичні відомості:

Ідентифікація та аутентифікація

Ідентифікацію та аутентифікацію можна вважати основою програмно - технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація та аутентифікація - це перша лінія оборони, "прохідна" інформаційного простору організації.

Ідентифікація дозволяє суб'єкту (користувачеві процесу, що діє від імені певного користувача, або іншому апаратно - програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка справжності".

Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність сервера) і двосторонньої (взаємної). Приклад односторонньої аутентифікації - процедура входу користувача в систему.

У мережевому середовищі, коли сторони ідентифікації / аутентифікації територіально рознесені, у розглянутого сервісу є два основних аспекти:

- службовець аутентифікатором (тобто використовується для підтвердження автентичності суб'єкта);
- як організовано (і захищений) обмін даними ідентифікації / аутентифікації.

Суб'єкт може підтвердити свою дійсність, пред'явивши принаймні одну з наступних сутностей:

• щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ тощо);

• щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);

• щось, що є частиною його самого (голос, відбитки пальців і т.п., тобто свої біометричні характеристики).

Надійна ідентифікація та аутентифікація ускладнена не тільки через мережеві загрози, але і з цілої низки причин. По-перше, майже всі аутентіфікаційні суті можна дізнатися, вкрасти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача і системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційні інформацію (адже на його місце міг сісти інша людина), а це не тільки клопітно, але і підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніше засіб захисту, тим він дорожчий.

Сучасні засоби ідентифікації / аутентифікації повинні підтримувати концепцію єдиного входу в мережу. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежне звернення, то багаторазова ідентифікація / аутентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід в мережу став нормою, домінантні рішення поки не сформувалися.

Головна перевага парольної аутентифікації - простота і звичність. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Однак, за сукупністю характеристик їх слід визнати найслабшим засобом перевірки аутентичності.

Тема логічного керування доступом - одна з найскладніших в області інформаційної безпеки. Справа в тому, що саме поняття об'єкта (а тим більше видів доступу) змінюється від сервісу до сервісу. Для операційної системи до об'єктів відносяться файли, пристрої та процеси. Щодо файлів і пристроїв зазвичай розглядаються права на читання, запис, виконання (для програмних файлів), іноді на видалення і додавання. Окремим правом може бути можливість передачі повноважень доступу іншим (так зване право володіння). Процеси можна створювати і знищувати. Сучасні операційні системи можуть підтримувати й інші об'єкти.

Контроль прав доступу проводиться різними компонентами програмного середовища - ядром операційної системи, сервісами безпеки, системою управління базами даних, програмним забезпеченням проміжного шару (таким, як монітор транзакцій) і т.д. Однак, можна виділити загальні критерії, на підставі яких вирішується питання про надання доступу, і загальні методи зберігання матриці доступу.

При прийнятті рішення про надання доступу звичайно аналізується наступна інформація:

• ідентифікатор суб'єкта (ідентифікатор користувача, мережевий адресу комп'ютера тощо). Подібні ідентифікатори є основою довільного (або дискреційного) управління доступом;

• атрибути суб'єкта (мітка безпеки, група користувача тощо). Мітки безпеки - основа примусового (мандатного) управління доступом.

Рольове управління доступом оперує такими основними поняттями:

• користувач (людина, інтелектуальний автономний агент тощо);

• сеанс роботи користувача;

• роль (зазвичай визначається відповідно з організаційною структурою);

• об'єкт (сутність, доступ до якої розмежовується; наприклад, файл ОС або таблиця СУБД);

• операція (залежить від об'єкта, для файлів ОС - читання, запис, виконання тощо, для таблиць СУБД - вставка, видалення і т.п, для прикладних об'єктів операції можуть бути більш складними);

• право доступу (дозвіл виконувати певні операції над певними об'єктами).

Ролям приписуються користувачі і права доступу; можна вважати, що вони (ролі) іменують відносини "багато до багатьох" між користувачами і правами. Ролі можуть бути приписані багатьом користувачам; один користувач може бути приписаний декільком ролям. Під час сеансу роботи користувача активізується підмножина ролей, яким він приписаний, в результаті чого він стає власником об'єднання прав, приписаних активним ролям. Одночасно користувач може відкрити кілька сеансів.

Також необхідно враховувати, що існує специфікації трьох категорій функцій, необхідних для адміністрування рольового керування доступом:

1. Адміністративні функції (створення і супровід ролей та інших атрибутів рольового доступу): створити / видалити роль / користувача, приписати користувача / право ролі або ліквідувати існуючу асоціацію, створити / видалити ставлення успадкування між існуючими ролями, створити нову роль і зробити її спадкоємицею / попередницею існуючої ролі, створити / видалити обмеження для статичного / динамічного поділу обов'язків.

2. Допоміжні функції (обслуговування сеансів роботи користувачів): відкрити сеанс роботи користувача з активацією подразумеваемого набір ролей; активувати нову роль, деактивувати роль; перевірити правомірність доступу.

3. Інформаційні функції (одержання відомостей про поточну конфігурації з урахуванням відносин спадкування). Тут проводиться поділ на обов'язкові і необов'язкові функції. До числа перших відносяться отримання списку користувачів, яким приписані ролі, і списку ролей, яким приписаний користувач.

Всі інші функції віднесені до розряду необов'язкових. Це отримання інформації про права, яких приписані ролі, про права заданого користувача (якими він володіє як член певної сукупності), про активні на даний момент сеансу ролі і права, про операції, роль / користувач можуть зробити з заданим об'єктом, про статичних / динамічних розподілах обов'язків.

Біометричний контроль доступу - автоматизований метод, за допомогою якого шляхом перевірки (дослідження) унікальних фізіологічних особливостей або поведінкових характеристик людини здійснюється ідентифікація особи. Філологічні особливості, наприклад, такі як капілярний малюнок пальця, геометрія долоні або малюнок райдужної оболонки ока, є постійними фізичними характеристиками людини. Даний тип вимірювань (перевірки) практично незмінний також як і самі фізіологічні характеристики. Поведінкові ж характеристики, такі як підпис, голос або клавіатурний почерк, знаходяться під впливом як керованих дій так і менш керованих психологічних чинників. Оскільки поведінкові характеристики можуть змінюватися з часом, зареєстрований біометричний зразок повинен оновлюватися при кожному його використанні. Хоча біометрія, заснована на поведінкових характеристиках, менш дорога і представляє собою меншу загрозу для користувачів, фізіологічні риси допомагають досягти більшу точність ідентифікації особи та її безпеки. У будь-якому випадку обидва методи і забезпечують значно вищий рівень ідентифікації, чим ідентичні карти.

Біометрична система - це система розпізнавання шаблона, яка встановлює справжність конкретних фізіологічних або поведінкових характеристик користувача. Логічно біометрична система може бути розділена на два модулі: модуль реєстрації та модуль ідентифікації.

Схема функціонування біометричних пристроїв

Основними елементами біометричної системи є:

- Зчитувач (сканер);

- Програмне забезпечення ідентифікації, яке формує ідентифікатор користувача;

- Програмне забезпечення аутентифікації, що виробляє порівняння зразка з тими ідентифікаторами користувачів, які є в базі даних.

Найбільш поширені зараз біометричні системи захисту інформації засновані на перевірці (дослідженні) наступних функціональних поведінкових особливостей людини:

- Відбиток пальця;
- Геометрія руки;
- Райдужна оболонка ока;
- Сітківка ока;
- Голосова ідентифікація;
- Геометрія особи;
- Почерк, напис.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Задруга", 2013. – 170 с.

2. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

3. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / Соколов А.В., Шаньчин В.Ф. – М.: ДМК Прес, 2002. – 656 с.

4. Андреєв В.І. Основи інформаційної безпеки / Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. – К.: Вид-во ДУІКТ, 2009. – 292 с.

5. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання на виконання лабораторної роботи №7 відповідно з номером бригади приведено в табл. 7.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 7

Завдання для виконання лабораторної роботи №7

Номер бригади	Завдання
1	Знайти матеріали з біометричних систем криптографії, проаналізувати їх, оцінити достоїнства і недоліки і провести порівняльний аналіз.
2	Знайти матеріали з односторонньох і двосторонньої аутентифікації, проаналізувати їх, оцінити достоїнства і недоліки і провести порівняльний аналіз.
3	Знайти матеріали про надійність і зручність користувачів при аутентифікації, проаналізувати їх, оцінити достоїнства і недоліки і провести порівняльний аналіз.
4	Знайти матеріали про парольну аутентифікацію, проаналізувати їх, оцінити достоїнства і недоліки і провести порівняльний аналіз.
5	Знайти матеріали про прийняття рішення про надання доступу, проаналізувати їх, оцінити достоїнства і недоліки і провести порівняльний аналіз.
6	Знайти матеріали про рольове управління, проаналізувати їх, оцінити достоїнства і недоліки і провести порівняльний аналіз.
7	Знайти матеріали про категорії функцій необхідних для адміністрування рольового керування доступом, проаналізувати їх і провести порівняльний аналіз.

Контрольні питання:

1. Ідентифікація і аутентифікація?
2. Парольна аутентифікація?
3. Керування доступом?
4. Рольове керування доступом?
5. Ідентифікація за біометричними ознаками?
6. Основні елементи біометричної системи?
7. Біометричні системи ідентифікації?

Лабораторна робота № 8

Вивчення стандартів України щодо забезпечення інформаційної безпеки

Мета роботи: Поглибити теоретичні знання нормативно - правової бази України.

Короткі теоретичні відомості:

Державні стандарти являють собою важливу ступінь організації відносин у сфері інформаційної безпеки. Цими документами є:

• ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення.";

• ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт.";

• ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення.";

• ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірки".

• ДСТУ 3918-1999 (ISO / IEC 1207:1995) "Інформаційні технології. Процеси життєвого циклу програмного забезпечення".

• ДСТУ ISO / IEC TR 13335-1:2003 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій.".

• ДСТУ ISO / IEC TR 13335-2:2003 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 2. Управління та планування безпеки інформаційних технологій.".

• ДСТУ ISO / IEC TR 13335-3:2003 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 3. Методи управління захистом інформаційних технологій".

• ДСТУ ISO / IEC TR 13335-4:2005 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 4. Вибір засобів захисту".

• ДСТУ ISO / IEC TR 13335-5:2005 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 5. Керівництво з управління мережею безпеки".

Далі слід розглянути Положення та Постанови Кабінету Міністрів України:

• Положення про технічний захист інформації в прикордонних військах.

• Концепція технічного захисту інформації в Україні.

• Положення про порядок здійснення криптографічного захисту інформації в Україні.

• Положення про технічний захист інформації в Україні.

• Положення про контроль за функціонуванням системи технічного захисту інформації.

• Постанова КМ України "Про деякі питання щодо захисту інформації, охорона якої забезпечується державою".

• Розпорядження Президента України "Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв'язку".

• Державна програма інформаційно - телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / Головань С.М., Петров О.С., Хорошко В.О., Щербак Л.М. – Луганск: Вид-во "Ноулідж", 2012. – 480 с.

3. Сердюков В.В. Правові основи охорони інформації / Сердюков В.В., Стаднік О.М., Живко З.Б., Хорошко В.О. – К.: Вид-во ДУІКТ, 2009. – 355 с.

4. Артемов В.Ю. Нормативно-правовий довідник з охорони інформації в Україні / Артемов В.Ю., Лєнков О.С., Пашков А.С., Стадник О.М., Хорошко В.О. – К.: Вид-во ДУІКТ, 2010.

5. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №8 відповідно з номером бригади наведено в табл. 8.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.

6 Оформити звіт.

7. Зробити висновки.

Таблиця 8

Завдання для виконання лабораторної роботи №8

Номер бригади	Завдання
1	Знайти матеріали з ДСТУ 3396.0-96 та ДСТУ 3396.1, проаналізувати їх і сформулювати недоліки та переваги.
2	Знайти матеріали з ДСТУ 4145-2002, проаналізувати їх і сформулювати недоліки та переваги. Провести порівняльний аналіз з існуючими стандартами інших країн.
3	Знайти матеріали з ДСТУ ISO / IEC TR 13335-TR, проаналізувати групу цих стандартів і оцінити їх недоліки та переваги.
4	Знайти матеріали з ДСТУ 3918-1999 (ISO / IEC 1207:1995), проаналізувати групу цих стандартів і оцінити їх недоліки та переваги.
5	Знайти матеріали з ДСТУ ISO / IEC TR 13335-3:2003 та ДСТУ ISO / IEC TR 13335-5:2005, проаналізувати їх, сформулювати їх відмінності і спільність.
6	Знайти матеріали з ДСТУ ISO / IEC TR 13335-2:2003 та ДСТУ ISO / IEC TR 13335-4:2005, проаналізувати їх, сформулювати їх відмінності і спільність.
7	Знайти матеріали про Концепцію про технічний захист інформації в Україні, Положення про ТЗІ в Україні та Положення про контроль за функціонуванням СТЗІ, проаналізувати їх, провести порівняльний аналіз, відзначити недоліки і переваги.

Контрольні питання:

1. ДСТУ 3396.0-96?
2. ДСТУ 3396.1-96?
3. ДСТУ 3396.2-97?
4. ДСТУ 4145-2002?
5. ДСТУ 3918-1999 (ISO / IEC 1207:1995)?
6. ДСТУ ISO / IEC TR 13335-1:2003?
7. ДСТУ ISO / IEC TR 13335-2:2003?
8. ДСТУ ISO / IEC TR 13335-3:2003?
9. ДСТУ ISO / IEC TR 13335-4:2005?

10. ДСТУ ISO / IEC TR 13335-5:2005?
11. Положення та Постанови Кабінету Міністрів України:

Лабораторна робота № 9

Міжнародні вимоги щодо забезпечення інформаційної безпеки

Мета роботи: Вивчення вимог щодо забезпечення безпеки в провідних країнах світу.

Поглибити знання з наступних питань:

- аналіз вимог щодо забезпечення безпеки в США;

- аналіз вимог щодо забезпечення безпеки в Російській Федерації;

- аналіз вимог щодо забезпечення безпеки у Франції.

Короткі теоретичні відомості:

Вимоги щодо забезпечення інформаційної безпеки в США

Вимоги розділені на три групи: стратегія, підзвітність, гарантії. В кожній групі по дві вимоги такого змісту:

1. Стратегія

Вимога 1 - стратегія забезпечення безпеки: необхідно мати явну і добре певну стратегію забезпечення безпеки.

Вимога 2 - маркування: керуючі доступом мітки повинні бути пов'язані з об'єктами.

2. Підзвітність

Вимога 3 - ідентифікація: індивідуальні суб'єкти повинні ідентифікуватися.

Вимога 4 - підзвітність: контрольна інформація повинна зберігатися окремо і захищатися так, щоб з боку відповідальної за це групи була можливість відслідковувати дії, що впливають на безпеку.

3. Гарантії

Вимога 5 - гарантії: обчислювальна система в своєму складі повинна мати апаратні / програмні механізми, що допускають незалежно оцінку на предмет достатнього рівня гарантій того, що система забезпечує виконання викладених вище вимог з 1-ої по 4-у.

Вимога 6 - постійний захист: гарантовано захищені механізми, що реалізують перераховані вимоги, повинні бути постійно захищені від «виламування» та / або несанкціонованого внесення змін.

У частині стандартизації апаратних засобів інформаційних систем та телекомунікаційних мереж в США розроблені правила стандарту Transient Electromagnetic Pulse Emanations Standart (TEMPEST).

Цей стандарт передбачає застосування спеціальних заходів захисту апаратури від паразитних випромінювань електромагнітної енергії, перехоплення якої може привести до оволодіння охоронюваними відомостями.

Стандарт TEMPEST забезпечує радіус контрольованої зони перехоплення порядку 1м. Це досягається спеціальними схемотехнічними, конструктивними та програмно-апаратними рішеннями, у тому числі:

• застосуванням спеціальної низько яка споживає малошумящий елементної бази;

• спеціальним конструктивним виконанням плат і розводкою сигнальних і земляних електричних ланцюгів;

• використанням екранів і RC-фільтрів, що обмежують спектри сигналів в ланцюгах інтерфейсних з'єднань;

• застосуванням спеціальних заходів, що забезпечують захист від НСД (знімний жорсткий диск, магнітні парольні карти, спеціальні замкові пристрої, програмно-апаратні засоби захисту інформації та шифрування).

Зниження потужності побічних електромагнітних випромінювань і наведень (ПЕМВН) монітора досягається поруч конструктивно-технологічних рішень, застосованих в ПЕОМ:

Вимоги до безпеки інформаційних систем в Росії

Аналогічний підхід був реалізований і в керівному документі Державної технічної комісії при Президентові РФ «Класифікація автоматизованих систем і вимоги щодо захисту інформації», випущеному в 1992 р. Вимоги всіх

наступних документів є обов'язковими для виконання тільки тих державних або комерційних організацій, обробляють інформацію, що містить державну таємницю. Для інших комерційних структур документи носять рекомендаційний характер. У даному документі виділено 9 класів захищеності автоматизованих систем від несанкціонованого доступу до інформації, а для кожного класу визначений мінімальний склад необхідних механізмів захисту та вимоги до змісту захисних функцій кожного з механізмів в кожному з класів систем.

Класи систем розділені на три групи, причому основним критерієм розподілу на групи прийнято специфічні особливості обробки інформації, а саме:

третя група - системи, в яких працює один користувач, допущений до всієї оброблюваної інформації, розміщеної на носіях одного рівня конфіденційності, до групи віднесені два класи, позначені 3Б і 3А;

друга група - системи, в яких працює декілька користувачів, які мають однакові права доступу до всієї інформації, оброблюваної та / або зберігається на носіях різного рівня конфіденційності; до групи віднесені два класи, позначені 2Б і 2А;

перша група - багато користувачів системи, в яких одночасно обробляється і / або зберігається інформація різних рівнів конфіденційності, причому різні користувачі мають різні права на доступ до інформації; до групи віднесені 5 класів: 1Д, 1Г, 1В, 1Б і 1А.

Вимоги до захисту ростуть від систем класу 3Б до класу 1А.

Всі механізми захисту розділені на 4 підсистеми наступного призначення:

- управління доступом;
- реєстрації та обліку;
- криптографічного закриття;
- забезпечення цілісності.

Саботаж в нематеріальній сфері дуже поширений, починаючи з фальсифікації програм і даних до тотального саботажу шляхом застосування логічних бомб і різних вірусів. Цей вид загроз відзначається в усіх обстежених центрах. Збитки головним чином стосуються знищення змісту та форми даних, втрати цілісності, програм і документів.

В основному ці погрози направлені на дезорганізацію захисту: атаки на операційну систему, модифікація даних, зміна мови управління даними, стирання даних на магнітних носіях тощо. Дії здійснює в основному в обчислювальних центрах внутрішній персонал, а іноді спостерігаються і поза ОЦ піратські дії в мережі теледоступу.

Фізичні загрози визначаються як конфігурацією, так і розташуванням будівель і ускладнюються їх рассредоточением, поділом приміщень на окремі кабінети, розосередження засобів пожежогасіння та захисту. Заходи з відновлення залежать від наявності резерву.

Що стосується загроз зовнішнього середовища, то вони є фізично небезпечними в частині необхідності створення штучного клімату та захисту електромереж. Наслідки в основному обмежені, проте часто відзначаються досить значні затримки у відновленні поставок деякими матеріалами, особливо для електрообладнання великої потужності, що використовує незвичайні електричні частоти.

Загрози телекомунікаційних засобів стосуються внутрішнього телекомунікаційного обладнання: щитів, кабелів, автоматичних комутаторів, з'єднувальних коробок, концентраторів, контролерів ліній зв'язку, модемів і т. п. Серйозну небезпеку становить вихід з ладу вузлів зв'язку. Відзначено максимальну перерву у зв'язку до трьох тижнів. Відновлення визначається можливостями перемикання на інші центри, наявністю резервних ліній і засобів.

Література:

1. Іванченко І.С. Забезпечення інформаційної безпеки держави / Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Чирков Д.В. – К.: ПВП "Загроза", 2013. – 170 с.

2. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / Головань С.М., Петров О.С., Хорошко В.О., Щербак Л.М. – Луганск: Вид-во "Ноулідж", 2012. – 480 с.

3. Сердюков В.В. Правові основи охорони інформації / Сердюков В.В., Стаднік О.М., Живко З.Б., Хорошко В.О. – К.: Вид-во ДУІКТ, 2009. – 355 с.

4. Артемов В.Ю. Нормативно-правовий довідник з охорони інформації в Україні / Артемов В.Ю., Лєнков О.С., Пашков А.С., Стадник О.М., Хорошко В.О. – К.: Вид-во ДУІКТ, 2010.

5. Вивчити лекцію.

Порядок виконання лабораторної роботи:

1. Включити ПК.
2. Отримати доступ до Internet.
3. Завдання для виконання лабораторної роботи №9 відповідно з номером бригади наведено в табл. 9.
4. Знайти інформацію відповідно до завдання.
5. Обробити інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 9

Завдання для виконання лабораторної роботи №9

Номер бригади	Завдання
1	Знайти матеріали щодо вимог до забезпечення безпеки в США, проаналізувати їх і сформулювати недоліки та переваги.
2	Знайти матеріали щодо вимог до забезпечення безпеки в Росії, проаналізувати їх і сформулювати недоліки та переваги.
3	Знайти матеріали щодо вимог до забезпечення безпеки у Франції. Проаналізувати їх і відзначити недоліки та переваги.
4	Знайти матеріали щодо вимог до забезпечення безпеки в США та Росії. Проаналізувати їх і провести порівняльний аналіз.
5	Знайти матеріали щодо вимог до забезпечення безпеки в США та Франції. Проаналізувати їх і провести порівняльний аналіз.
6	Знайти матеріали щодо вимог до забезпечення безпеки в Росії та Франції. Проаналізувати їх і провести порівняльний аналіз.
7	Знайти матеріали щодо вимог до забезпечення безпеки в США, Франції та Росії. Проаналізувати їх і провести порівняльний аналіз.

Контрольні питання:

1. Вимоги щодо забезпечення інформаційної безпеки в США?
2. Стандарт TEMPEST?
3. Вимоги щодо забезпечення інформаційної безпеки в Росії?
4. Вимоги щодо забезпечення інформаційної безпеки во Франції?

Навчальне видання

Сергій Васильович Толюпа
Володимир Олексійович Хорошко
Юлія Євгеніївна Хохлачова

Забезпечення інформаційної безпеки держави

Лабораторний практикум

(українською мовою)

Видається у авторській редакції
Надруковано з оригіналу макета замовника

Підписано до друку 26.06.2014 Формат 60x84/16
Друк офсет. Папір офсет. Гарнітура Таймс
Ум. друк. арк. 5,67 Наклад 350 прим.
Замовлення № 11/14

Видавництво ПВП "Задруга"
м. Київ вул. Верхній Вал, 40, оф. 23
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру серія ДК 5158 від 26.06.2006 р.
Надруковано в ТОВ "Поліграф Консалтинг"
м. Київ, вул. Волинська, 60.