Міністерство внутрішніх справ України
Львівський державний університет внутрішніх справ
Центр післядипломної освіти, дистанційного та заочного навчання

Кафедра інформаційного та аналітичного забезпечення діяльності правоохоронних органів

КЕЙС
заняття на тему
«Безпека роботи з інформацією. Основні загрози та заходи безпеки при роботі з інформацією. Робота з програмами шифрування та відновлення інформації»

Підвищення кваліфікації (короткострокове)
поліцейських – дільничні офіцери поліції
Національної поліції України

Інформація про викладача:
к.т.н., доцент ЗАЧЕК
Олег Ігорович
0962102685

Львів -2021

Тема
«Безпека роботи з інформацією. Основні загрози та заходи безпеки при роботі з інформацією. Робота з програмами шифрування та відновлення інформації.»

Годин на тему – 1
Занять – 1 (1 академічна година)

Навчальна мета: надати слухачам знання щодо основних понять технологій захисту інформації, ознайомити із сучасними технічними та програмними засобами захисту інформації, надати практичні навички роботи із програмами шифрування даних.

Міжтематичні зв'язки: права людини; професійна етика; толерантність та недискримінація в роботі поліцейського; протидія торгівлі людьми; охорона місця події.

План лекції

1. Інформаційна безпека в поліцейській діяльності. Основні загрози та заходи безпеки при роботі з інформацією.
2. Сутність та класифікація методів захисту інформації в комп'ютерних системах та мережах.
3. Організаційні (адміністративні) заходи захисту інформації.
4. Апаратні та апаратно-програмні методи та засоби захисту інформації.
5. Робота з програмами шифрування та відновлення інформації.

1. Інформаційна безпека в поліцейській діяльності. Основні загрози під час роботи з інформацією

Діяльність Національної поліції значною мірою пов'язана з отриманням та використанням відомостей обмеженого доступу, розголошення яких може спричинити порушення конституційних прав громадян, а також зниження ефективності роботи правоохоронних органів щодо попередження, розкриття та розслідування злочинів.

У процесі здійснення своєї діяльності співробітники Національної поліції отримують інформацію про режим і характер роботи підприємств, розташованих на території, що обслуговується, відомості, що стосуються особистого життя громадян, а також іншу інформацію (наприклад, службового характеру). Дана інформація, а також відомості про окремі методи, прийоми і результати роботи Національної поліції складають службову таємницю. Розголошення таких відомостей, а також витік інформації про плановані і ті, що проводяться, заходи щодо охорони громадського порядку і боротьби зі злочинністю порушує нормальну їх діяльність і значно знижує її ефективність.

Велика увага сьогодні приділяється нормативно-правовому забезпеченню інформаційної безпеки. Базові засади закладаються Конституцією України (ст. 17, 19, 31, 32, 34, 50, 57 та 64), Закон України «Про інформацію» закладає правові основи інформаційної діяльності. В Законі України «Про інформацію» також введено і класифікацію інформації (рис. 1).

Крім цього ціла низка законодавчих актів регулює відносини у інформаційній сфері. Це, зокрема, Закони України "Про телекомунікації", "Про Національну програму інформатизації", "Про захист інформації в інформаційно-телекомунікаційних системах", а у Кримінальний кодекс України було введено розділ XVI, в якому визначалася відповідальність за злочини в інформаційній сфері.

Цілий ряд нормативно-правових актів, які безпосередньо стосуються питань інформаційної безпеки прийнято Міністерством внутрішніх справ України та Національною поліцією України. Серед цих документів особливу увагу необхідно звернути на:

Доручення МВС України від 19.03.2015 № 13155/Ав «Про заходи із протидії витоку службової інформації»;

Доручення МВС України від 24.04.2015 № 19130/Ав «Про недопущення витоку інформації, що утворюється в службовій діяльності»,

Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів»;

Саме в цих документах встановлено вимоги до парольного захисту, розглянуто питання застосовування у службовій діяльності поштових серверів та роботи з електронною поштою.

Звичайно розглянути всі аспекти питання інформаційної безпеки у рамках курсу «Безпека роботи з інформацією» ми не зможемо. В рамках двох годин це неможливо. Наша задача розібратися у основних небезпеках при роботі з інформацією, саме при використанні сучасної комп'ютерної техніки, та надати рекомендації стосовно того як захистити себе.

Перед початком розгляду загроз під час роботи з інформацією доцільно розглянути основні поняття, які передують вивченню даного питання.

Насамперед це ***предмет захисту***. У якості предмету захисту нами розглядатиметься інформація, що зберігається, оброблюється і передається у комп'ютерних системах. Особливістю цієї інформації є:

- двійкове представлення інформації всередині системи, незалежно від фізичної сутності носіїв вихідної інформації;
- високий ступінь автоматизації обробки і передавання інформації;
- концентрація великої кількості інформації у комп'ютерній системі.

Виходячи зі сказаного, ***об'єктом захисту інформації*** є комп'ютерна система або автоматизована система обробки даних, а предметом захисту у комп'ютерних системах є інформація. Матеріальною основою існування інформації в комп'ютерних системах є електронні та електронно-механічні пристрої. За допомогою пристроїв введення чи систем передачі даних

інформація попадає до комп'ютерних систем. В системі інформація зберігається на запам'ятовуючих пристроях різних рівнів і виводиться із системи за допомогою пристроїв виведення інформації чи систем передачі даних. Таким чином, для захисту інформації в комп'ютерних системах необхідно захищати пристрої і машинні носії від несанкціонованого впливу на них. ***Захищеність інформації у інформаційній системі*** – це такий стан усіх компонентів комп'ютерної системи, при якому забезпечується захист інформації від можливих загроз на необхідному рівні. Інформаційні системи, у яких забезпечується безпека інформації, називаються ***захищеними***.

Рис. 1. Класифікація інформації згідно Закону України «Про інформацію»

Захищеність інформації (чи інформаційна безпека) в системі МВС України досягається проведенням керівництвом відповідного рівня ***політики інформаційної безпеки***. По суті, це документ, який визначає основні напрямки вирішення завдань захисту інформації у інформаційно-пошукових системах, а також містить загальні вимоги і принципи побудови систем захисту інформації у комп'ютерних системах.

Таким чином, під ***системою захисту інформації в інформаційних системах*** розуміють єдиний комплекс правових норм, організаційних заходів, технічних програмних і криптографічних засобів, які забезпечують захищеність інформації у інформаційних системах у відповідності до прийнятої політики інформаційної безпеки.

Загрози інформації.

З позиції забезпечення безпеки інформації у інформаційних системах такі системи доцільно розглядати у вигляді єдності трьох компонентів, які здійснюють взаємовплив один на одного:

- інформація;
- технічні і програмні засоби;
- обслуговуючий персонал і користувачі.

Тому забезпечення безпеки інформації в інформаційних системах повинно передбачати захист усіх компонент від зовнішніх і внутрішніх загроз.

Під ***загрозою безпеці інформації*** розуміють потенційно можливу подію, процес чи явище, які можуть призвести до знищення, втраті цілісності, конфіденційності чи доступності інформації.

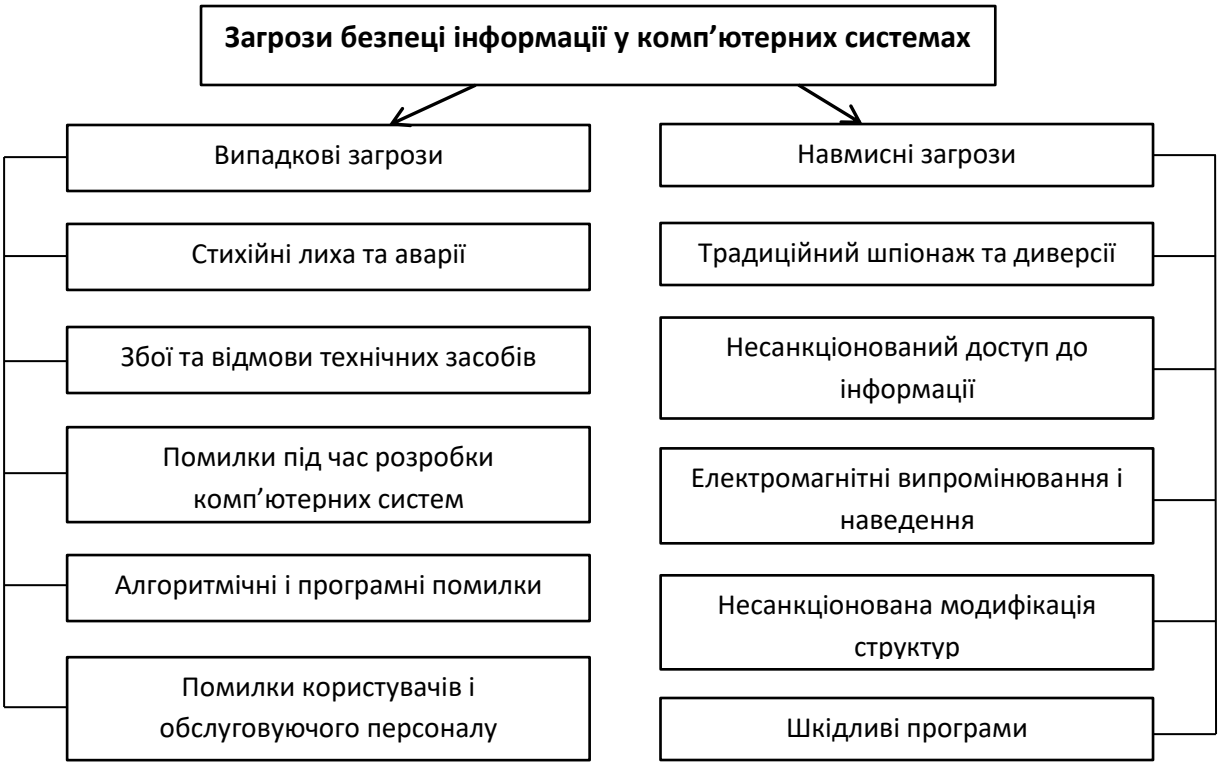

Рис. 2. Загрози безпеці інформації у комп'ютерних системах.

Усі можливі потенційні загрози безпеки інформації в інформаційних системах прийнято розділяти на два класи: ***випадкові*** та ***навмисні.***

Випадковими називають загрози, які не пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу. Реалізація загроз цього типу призводить до найбільших втрат інформації (за статистикою до 80%). При цьому, в основному, відбувається знищення, порушення цілісності і доступності інформації. Рідше порушується конфіденційність інформації, однак, під час цього створюються умови для навмисної дії на інформацію. Розглянемо та охарактеризуємо основні випадкові загрози.

Стихійні лиха та аварії. Дана загроза характеризується найруйнівнівнішими наслідками для комп'ютерних систем, оскільки відбувається фізичне знищення інформаційних систем, інформація втрачається або доступ до неї стає неможливим.

Збої та відмови складних систем є неминучими. В результаті збоїв і відказів порушується робото здатність технічних засобів, знищуються і спотворюються дані та програми, порушується алгоритм роботи засобів. Порушення алгоритмів роботи окремих вузлів та пристроїв системи може також призвести до порушення конфіденційності інформації.

Помилки підчас розробки інформаційних систем, алгоритмічні і програмні помилки призводять до наслідків, які є аналогічними до наслідків. Окрім цього, такі помилки можуть використовуватись зловмисниками для дії на ресурси інформаційної системи. Особливу небезпеку становлять помилки в операційних системах і програмних засобах захисту інформації.

Помилки користувачів і обслуговуючого персоналу. Відповідно до даних Національного Інституту Стандартів і Технологій США (NIST) 65% випадків порушення безпеки інформації відбувається в результаті цієї загрози. Некомпетентне, неохайне чи неуважне виконання функцій них обов'язків працівниками призводять до знищення, порушення цілісності і конфіденційності інформації, а також компрометації механізмів захисту.

Загалом, характеризуючи загрози цього класу, слід зазначити, що, в цілому, механізм їх реалізації на сьогодні вивчений достатньо добре, накопичено значний досвід протидії цим загрозам. Сучасні технології розробки технічних та програмних засобів, ефективна система експлуатації інформаційних систем, яка включає обов'язкове резервування інформації, дозволяють значно знизити втрати від реалізації загроз даного класу.

Навмисні загрози.

Даний клас загроз, на даний час, вивчений не достатньо, окрім цього, він динамічний і постійно поповнюється новими загрозами. Загрози цього класу у відповідності до їх фізичної суті і механізмів реалізації можуть класифікуватися на наступні.

Традиційний шпіонаж та диверсії. У якості джерел небажаної дії на інформаційні ресурси і надалі актуальні методи та засоби шпіонажу та диверсій, які використовувалися і використовуються для отримання та знищення інформації. Найчастіше вони використовуються для отримання

відомостей про систему з метою проникнення, крадіжки та знищення інформаційних ресурсів. До методів шпіонажу та диверсій відносяться:

- підслуховування;
- візуальне спостереження;
- крадіжка документів і машинних носіїв інформації;
- крадіжка програм і атрибутів системи захисту;
- підкуп і шантаж співробітників;
- збір і аналіз відходів машинних носіїв інформації;
- підпали;
- влаштовування вибухів.

Для прослуховування зловмиснику не обов'язково проникати на об'єкт. Сучасні засоби дозволять прослуховувати розмови з відстані декількасот метрів. В міських умовах дальність дії зменшується значно зменшується, що пов'язано з вищим рівнем фонового шуму. Принцип дій таких засобів полягає на аналізі відбитого променя лазера від скла вікна приміщення, яке коливається внаслідок звукових хвиль. Коливання віконного скла від акустичних хвиль у приміщені може зніматися за допомогою спеціальних пристроїв, які закріплюються на склі. Такі засоби перетворюють механічні коливання скла в електричний сигнал з подальшим передаванням по радіоканалу. Поза приміщеннями прослуховування ведеться за допомогою дуже чутливих направлених мікрофонів (до 100 метрів). Розмови у сусідні приміщеннях, за стінами можуть контролюватися за допомогою стетоскопічних мікрофонів (при товщині стіни – 0,5- 1 метр). Одним із можливих каналів втрати звукової інформації може бути прослуховування розмов, які ведуться за допомогою зв'язку. Прослуховування переговорів по провідним та радіоканалам не потребує високовартісного обладнання і високої кваліфікації зловмисника.

Візуальне спостереження для отримання інформації з інформаційних систем малопридатне і носить, як правило, допоміжний характер. Воно організовується в основному для встановлення режимів роботи і розташування механізмів захисту інформації.

Несанкціонований доступ до інформації. Даний термін визначений як доступ до інформації, що порушує правила розмежування доступу з використанням штатних засобів обчислювальної техніки та інформаційних систем. Під правилами розмежування доступу розуміють сукупні сит положень, що регламентують права доступу осіб до інформації. Право доступу до ресурсів інформаційної системи визначається для кожного співробітника у відповідності до його функціональних обов'язків. Виконання правил розмежування доступу реалізуються за рахунок створення системи розмежування доступу.

Несанкціонований доступ до інформації з використанням штатних апаратних і програмних засобів можливий у наступних випадках:

- відсутня система розмежування доступу;
- збій або відмова в інформаційній системі;
- помилкові дії користувачів або обслуговуючого персоналу;
- помилки у системі розмежування доступу;
- фальсифікація повноважень.

Якщо система розмежування доступу відсутня, то зловмисник, який має навики роботи з комп'ютерними системами, може отримати необмежений доступ до будь-якої інформації, що знаходиться в системі. В результаті збоїв та відмов засобів інформаційної системи, а також через помилкові дії обслуговуючого персоналу і користувачів можливий стан системи, за якого спрощується несанкціонований доступ до інформації. Зловмисник може виявити помилки в системі розмежування доступу і використати їх для несанкціонованого доступу до інформації. Фальсифікація повноважень є одним із найймовірніших шляхів (каналів) несанкціонованого доступу до інформації.

Електромагнітне випромінювання і наводки. Процес обробки і передачі інформації технічними засобами інформаційних систем супроводжується електромагнітним випромінюванням в навколишнє середовище і наведенням електричних сигналів у лініях зв'язку, сигналізації, заземленнях тощо. Це явище отримало назву – *побічних електромагнітних випромінювань та наводок*. За допомогою спеціального обладнання. За допомогою спеціального обладнання сигнали приймаються, виділяються, підсилюються і можуть або записуватися, або проглядатися. Наведені в провідниках електричні сигнали можуть виділятися і фіксуватися за допомогою обладнання, яке розташовується за сотні метрів від джерел сигналів. Для отримання інформації зловмисник маже також використовувати «прочісування» інформаційних сигналів в мережі електроживлення технічних засобів інформаційної системи. «Прочісування» інформаційних сигналів в мережі електроживлення можливе за наявності магнітного зв'язку між вихідним трансформатором підсилювача і випрямляючим трансформатором пристрою або за рахунок падіння напруги на внутрішньому опорі джерела живлення під час проходження струмів підсилених інформаційних сигналів. Якщо затухання у фільтрі випрямного пристрою недостатнє, то інформаційні сигнали можуть бути виявлені в мережі живлення.

Несанкціонована модифікація структур. Велику загрозу безпеці інформації в інформаційних системах несе несанкціонована модифікація алгоритмічної, програмної і технічної структур системи. Несанкціонована модифікація структур може здійснюватися будь-якому життєвому циклі інформаційної системи.

Несанкціонована зміна структури інформаційної системи у процесі її розробки чи модернізації отримала назву «закладка». У процесі розробки «закладки» впроваджуються, як правило, в спеціалізовані системи. Їх важко виявити у зв'язку з високою кваліфікацією їх авторів і складності сучасних інформаційних систем. Алгоритмічні, програмні і апаратні «закладки» використовуються або для безпосередньої шкідливої дії на систему, або для забезпечення неконтрольованого входу в систему. Шкідлива дія «закладок» на систему здійснюється під час отримання відповідної команди із зовні і під час настання визначених подій у системі. Такими подіями може бути перехід на визначений режим роботи, прихід встановленої дати, досягнення певного напрацювання тощо.

Програмні і апаратні «закладки», які призначені для неконтрольованого входу до програми, використання привілегійованих режимів роботи (наприклад, режимів операційної системи), обходу засобів захисту інформації отримали назву «люки».

Шкідливі програми. Одним із основних джерел безпеки інформації в інформаційних системах є використання спеціальних програм, які отримали загальну назву «шкідливі програми».

В залежності від механізму дії шкідливі програми поділяють на чотири класи:

- «логічні бомби»;
- «черв'яки»;
- «троянські коні»;
- «комп'ютерні віруси».

«Логічні бомби» - це програми або їх частини, які постійно знаходяться в комп'ютері або в обчислювальних системах і виконуються лише при дотриманні певних умов. Прикладом таких умов може бути: настання відповідної дати, перехід інформаційної системи в певний режим роботи, настання окремих подій задане число разів тощо.

«Черв'яками» називають програми, які виконуються кожен раз під час завантаження системи, володіють властивістю переміщатися в системі чи мережі і само відтворювати копії. Лавиноподібне розмноження програм призводить до перенавантаження каналів зв'язку, пам'яті і, в кінцевому випадку, до блокування системи.

«Троянські коні» - це програми, отримані шляхом явної зміни чи додавання команд в користувацькі програми. Під час наступного виконання цих програм, поряд із заданими функціями, виконуються несанкціоновані, змінені чи будь-які нові функції.

«Комп'ютерні віруси» - це невеликі програми, які після провадження в ПК самостійно розповсюджуються шляхом створення своїх копій, а при виконанні певних умов здійснюють негативний вплив на інформаційну систему.

Оскільки вірусам притаманні властивості усіх класів шкідливих програм, то усі шкідливі програми в побуті часто називають вірусами.

2. Сутність та класифікація методів захисту інформації в комп'ютерних системах та мережах

Практичне застосування систем захисту інформації показує, що ефективною може бути лише побудова комплексної системи захисту інформації, яка буде включати у себе максимально можливі способи чи методи захисту. Відповідно до розглянутих вище загроз, розроблено та класифіковано методи захисту інформації в інформаційних системах. Усі дані методи можна розподілити на наступні категорії:

- морально-етичні – створення і підтримання на об’єкті де організовується захист інформації, такої моральної атмосфери, у якій порушення правил, які регламентують поведінку працівників, оцінювалось колективом різко негативно;
- нормативно-правові – використання законодавчих актів, які регламентують права та обов’язки фізичних і юридичних осіб, а також держави в галузі захисту інформації;
- організаційні (адміністративні) – організація відповідного режиму секретності, пропускного та внутрішнього порядку;
- фізичні – створення фізичних перешкод для доступу сторонніх осіб до інформації, яка підлягає захисту;
- технічні (апаратні) – застосування електронних та інших засобів для захисту інформації;
- криптографічні – застосування шифрування і кодування для укриття інформації, що обробляється і передається, від несанкціонованого доступу;
- програмні – застосування програмних засобів розмежування доступу, антивірусні програми тощо.

У літературі можна знайти відмінні від приведеної класифікації методів захисту інформації, однак сутності даних методів вони не змінюють.

3. Організаційні (адміністративні) заходи захисту інформації

Закони і нормативно-правові акти виконуються у тому випадку, якщо вони підкріплені правильною організаційною діяльністю відповідних структур. Під час розгляду питань безпеки інформації така діяльність відноситься до організаційних методів захисту інформації.

Організаційні методи захисту інформації включають в себе заходи і дії, які повинні виконувати посадові особи у процесі створення і експлуатації інформаційних систем для забезпечення заданого рівня безпеки інформації.

Організаційні методи захисту інформації тісно пов’язані з правовим регулюванням в галузі безпеки інформації. У відповідності із законами та нормативними актами в МВС створюються спеціальні служби, які організовують створення і функціонування систем захисту інформації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в інформаційних системах:

- організація робіт з розробки системи захисту інформації;
- обмеження доступу на об’єкт і до ресурсів інформаційної системи;
- розмежування доступу до ресурсів інформаційної системи;
- планування заходів;
- розробка документації;
- навчання обслуговуючого персоналу та користувачів;
- сертифікація засобів захисту інформації;
- ліцензування діяльності зі захисту інформації;
- атестація об’єктів захисту;

- удосконалення системи захисту інформації;
- оцінка ефективності функціонування системи захисту інформації;
- контроль за виконанням встановлених правил роботи в інформаційній системі.

4. Апаратні та апаратно-програмні методи та засоби захисту інформації

Перші операційні системи для ПК не мали власних засобів захисту, у зв'язку із чим і виникла потреба розробки додаткових систем захисту. Актуальність цієї проблеми не зменшилась і з появою потужніших операційних систем, оскільки дані системи не здатні захистити дані, які знаходяться за її межами , наприклад під час використання інформаційного обміну у мережах.

Апаратно програмні засоби можна розбити на 5 основних груп (рис. 3).

Рис. 3. Апаратно-програмні засоби захисту інформації.

1. Системи ідентифікації і аудентифікації користувачів.

Такі системи застосовуються для обмеження доступу випадкових і незаконних користувачів до ресурсів комп'ютерної системи. Загальний алгоритм роботи цих систем полягає у тому, щоб отримати від користувача інформацію, яка підтверджує його особистість, перевірити її достовірність, після чого надати (чи не надати) цьому користувачу можливість роботи із системою. Під час побудови таких систем виникає проблема вибору інформації, на основі якої виконується процедура ідентифікації користувача. У загальному можна виділити наступні типи:

- таємна інформація, якою володіє користувач (пароль, персональний ідентифікатор, ключ тощо). Цю інформацію користувач повинен запам’ятати або можуть бути застосовані спеціальні засоби зберігання такої інформації;
- фізіологічні параметри людини (відбитки пальців рук, малюнок райдужної оболонки ока тощо чи особливості поведінки людини (наприклад, особливості роботи на клавіатурі).
- Системи ідентифікації першого типу прийнято рахувати традиційними. Системи ідентифікації другого типу називають *біометричними*.

2. Системи шифрування дискових даних.

Основне завдання таких систем полягає забезпечення захисту від несанкціонованого використання даних, які знаходяться на носіях інформації.

Забезпечення конфіденційності даних забезпечується шляхом їх шифрування з використанням симетричних алгоритмів шифрування. Основною класифікаційною ознакою для комплексів шифрування служить рівень їх впровадження у комп’ютерну систему.

Робота прикладних програм з дисковим накопичувачем складається з двох етапів – *логічного* і *фізичного*.

Логічний етап відповідає рівню взаємодії прикладної програми з операційною системою (наприклад, виклик сервісних функцій читання/запису даних). На цьому етапі основним об’єктом є файл.

Фізичний етап відповідає рівню взаємодії операційної системи і апаратури. У якості об’єктів цього рівня виступають структури фізичної організації даних , наприклад, сектори жорсткого диску.

В результаті системи шифрування даних можуть здійснюватися криптографічні перетворення даних на рівні файлів (захищаються окремі файли) і на рівні дисків (захищається диск повністю).

До програм першого типу можна віднести програму-архіватор rar, до другого типу можна віднести програму шифрування Diskreet.

Іншою класифікаційною ознакою систем шифрування дискових даних є спосіб їх функціонування. За способом функціонування системи шифрування дискових даних поділяють на два класи:

- системи *прозорого* шифрування;
- системи, які спеціально викликаються для виконання шифрування.

У системах прозорого шифрування криптографічні перетворення проводяться у режимі реального часу, непомітно для користувача. Наприклад,користувач записує підготовлений текстовий документ на диск, а система захисту у процесі запису проводить його шифрування.

Системи другого класу, як правило, представляють собою утиліти, які необхідно спеціально викликати, які необхідно спеціально викликати для виконання шифрування. До них наприклад відносяться архіватори зі вбудованими засобами парольного захисту.

3. Системи шифрування даних, що передаються по комп'ютерних мережах.

Розрізняють два основних способи такого шифрування: *канальне* шифрування і *кінцеве (абонентське)* шифрування.

У випадку канального шифрування захищається уся інформація, яка передається каналами зв'язку, включаючи службову. Процедура такого шифрування реалізується за допомогою протоколу канального рівня. Цей спосіб шифрування має наступну перевагу – вбудовування процедури шифрування на канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи.

Однак у даного методу є суттєві недоліки:

- шифруванню на даному рівні підлягає уся інформація, включаючи службові дані транспортних протоколів. Це ускладнює механізм маршрутизації мережевих пакетів і потребує розшифрування даних в пристроях проміжної комутації (шлюзах, ретрансляторах тощо);
- шифрування службової інформації може призвести до появи статистичних закономірностей у шифруванні даних. що впливає на надійність захисту і накладає обмеження на використання криптографічних алгоритмів.

Кінцеве (абонентське) шифрування дозволяє забезпечити конфіденційність даних, що передаються між об'єктами (абонентами). Кінцеве шифрування реалізується за допомогою відповідного прикладного протоколу. У цьому випадку захищеним залишається лише повідомлення , а уся службова інформація залишається відкритою.

4. Системи аутентифікації електронних даних.

Під час обміну даними по мережах виникає проблема аутентифікації автора документа і самого документа, тобто встановлення особистості автора і перевірка відсутності змін у документі.

Для аутентифікації електронних даних застосовують код аутетифікації повідомлення (імітовставку) або електронний цифровий підпис. Під час формування коду коду аутентифікації повідомлення і електронного цифрового підпису використовують різні типи систем шифрування.

Код аутентифікації повідомлення формують за допомогою симетричних систем шифрування даних. Імітовставка виробляється з відкритих даних за допомогою спеціального перетворення з використанням секретного ключа і передається по каналу зв'язку у кінці зашифрованих даних. Імітовставка перевіряється отримувачем повідомлення, що має секретний ключ, шляхом повторення процедури, що виконувалась попередньо відправником, на отриманими відкритими даними.

Електронний цифровий підпис представляє собою відносно невелику кількість додаткової аутентифікаційної цифрової інформації, що передається разом із текстом. Для реалізації електронного цифрового підпису використовують принципи асиметричного шифрування.

5. Засоби управління ключовою інформацією.

Під ключовою інформацією розуміють сукупність усіх криптографічних ключів, що використовуються в інформаційній системі.

Основним класифікатором засобів управління ключовою інформацією є вид функції управління ключами. Розрізняють наступні основні види функцій управління ключами: генерація ключів, зберігання ключів і розподіл ключів.

Способи генерації ключів розрізняють для симетричних і асиметричних криптосистем. Для генерації ключів симетричних криптосистем використовуються апаратні і програмні засоби генерації випадкових чисел, зокрема схеми із застосуванням блочного симетричного алгоритму шифрування. Генерація ключів для асиметричних криптосистем являє складніше завдання у зв'язку із необхідністю отримання ключів з певними математичними властивостями.

Функція зберігання ключів передбачає організацію безпечного зберігання, обліку і видалення ключів. Для забезпечення безпечного зберігання і передачі ключів застосовують їх шифрування за допомогою інших ключів. Такий підхід призводить до концепції ієрархії ключів. До ієрархії ключів, як правило входить головний ключ (майстер ключ), ключ шифрування ключів і ключ шифрування даних. Необхідно зазначити, що генерація і зберігання ключів є критичними питаннями криптографічного захисту.

Розподіл ключів є самим відповідальним процесом в управлінні ключами. Цей процес повинен гарантувати скритність розподілу ключів, а також оперативність і точність їх розподілу. Розрізняють два основних способи розподілу ключів між користувачами комп'ютерної мережі:

- застосування одного або декількох центрів розподілу ключів;
- прямий обмін сеансовими ключами між користувачами.

5. Робота з програмами шифрування та відновлення інформації

Програмними засобами захисту інформації називають спеціальні програми. Які входять до складу програмного забезпечення інформаційних систем для вирішення в них завдань захисту інформації.

Програмні засоби захисту є невід'ємною частиною механізму захисту інформаційних систем.

В організаційному плані побудова програм захисту інформації визначається розробкою комплексу програм, що виконують захисні функції:

- визначення користувачів;
- розмежування доступу до масивів даних;
- боротьбу з комп'ютерними вірусами;
- шифрування даних тощо.

Переваги таких програм зрозумілі: кожна з них забезпечує вирішення певних важливих завдань захисту.

Загальноприйнятої класифікації програмних засобів захисту не існує, однак, під час їх розгляду, зазвичай притримуються критерію

функціональності, тобто функціям захисту, для яких вони написані. При цьому, з розвитком форм і способів обчислювальної техніки функції програмного захисту лише розширюються.

У зв'язку із названими критеріями, зокрема можна використовувати наступну класифікацію:

- програми впізнавання користувача
- програми паролі;
- розмежування доступу
- програми захисту програм
- захист від копіювання;
- антивірусні програми;
- програми контролю стану компонентів захисту;
- програми криптографічного захисту.

Що стосується останнього, то під криптографічними захистом інформації розуміють таке перетворення вихідної інформації, в результаті якого вона стає недоступною для ознайомлення і використання особами, які не мають на це повноважень.

Загалом, відомі різні підходи до класифікації методів криптографічного перетворення інформації. Однак, найчастіше розглядають поділ методів за дією на вихідну інформацію. У такому випадку методи криптографічного захисту інформації поділяють на 4 групи

Процес **шифрування** полягає у проведенні зворотних математичних, логічних, комбінаторних та інших перетворень вихідної інформації, в результаті яких зашифрована інформація являє собою хаотичний набір букв, цифр, інших символів і двійкових кодів.

Для шифрування інформації використовують алгоритм перетворення і ключ.

Рис. 4. Методи криптографічного перетворення інформації

Сучасні методи шифрування повинні відповідати наступним вимогам:

- стійкість шифру протистояти крипто аналізу (криптостійкість) повинна бути такою, щоб розшифрування могло бути здійснене шляхом вирішення завдання повного перебору ключів;
- криптостійкість повинна забезпечуватися не секретністю алгоритму шифрування, а секретністю ключа;
- шифротекст не повинен суттєво перевищувати за обсягом вихідну інформацію;
- помилки, що виникли під час шифрування, не повинні призводити до спотворення і втрати інформації;
- час шифрування не повинен бути довгим;

- вартість шифрування повинна бути співставлень з вартістю інформації, яка зашифровується.

Криптостійкість є основним показником ефективності, і визначається часом чи вартістю засобів, які необхідні криптоаналітику для розшифрування інформації. Єдиний шлях до розшифрування – перебір комбінацій ключа і виконання алгоритму шифрування. Таким чином, вартість розшифрування залежать від довжини ключа і складності алгоритму шифрування.

Методи шифрування можна класифікувати за різними ознаками. Один із варіантів такої класифікації приведено на рис._

Симетричне шифрування – це шифрування при якому для шифрування і для розшифрування використовують один і той же ключ.

Метод заміни – полягає у заміні символів вихідної інформації, записаних у одному алфавіті, символами із іншого алфавіту у певному порядку за певним правилом.

Метод перестановки – полягає у розділені тексту на блоки фіксованої довжини з наступною перестановкою символів у кожному блоці за певним алгоритмом.

Аналітичні методи – це методи, які для шифрування використовують аналітичні перетворення (найчастіше матричні).

Адитивні методи – суть даних методів полягає у послідовному сумуванні цифрових кодів відповідних кодів вихідної інформації з послідовністю кодів ключа, який часто називають гамою. Тому адитивні методи часто називають гамуванням.

Рис. 5. Методи шифрування

Асиметричне шифрування – це шифрування під час якого для шифрування використовують відкритий і відомий ключ, а для розшифрування інший (закритий) ключ.

Стеганографія – це метод захисту інформації, який дозволяє скрити не лише зміст інформації, але й сам факт її передачі. В основі усіх методів стеганографії лежить маскування закритої інформації серед відкритих файлів.

Кодування – це метод захисту інформації, суть якого полягає у заміні змістовних конструкцій вихідної інформації (слів, речень) кодами. У якості кодів можуть використовуватися послідовності цифр чи букв. Для розкодування використовуються спеціальні таблиці або словники. Даний метод доцільно застосовувати з обмеженим набором змістовних конструкцій.

Стиснення інформації може бути віднесене до методів криптографічного захисту з певними застереженнями. Метою стиснення є зменшення обсягу інформації. У той же час стиснена інформація не може бути прочитана або використана без зворотного перетворення.

План практичного заняття (1 год.)

1. Створення захищеного з'ємного носія даних шляхом створення зашифрованого тому засобами програми TrueCrypt.
2. Робота з даними у зашифрованому розділі.

ВИСНОВКИ

Сьогодні, коли сучасні інформаційні технології інтенсивно впроваджуються в усі сфери життя і діяльності суспільства, національна і, як її частина, економічна безпека держави починає прямо залежати від забезпечення інформаційної безпеки.

Засоби комп'ютерної техніки, новітні інформаційні технології почали активно використовувати організовані злочинні угруповання. Їх інтереси в першу чергу спрямовані на отримання конфіденційної комерційної інформації, фінансових махінацій, поширення неправдивої інформації тощо.

Злочинці у кіберпросторі використовують свої знання для промислового шпигунства, політичних цілей, тероризму. Перелік комп'ютерних злочинів можна продовжити, згадавши й атаки на військові, космічні комп'ютерні системи, промислове шпигунство, використання компромату в політичних цілях і т. д.

Отже, протидія комп'ютерним злочинам на всіх рівнях має дуже важливе значення, тому ви повинні знати правове забезпечення захисту інформації в Україні, основні загрози інформації в інформаційних системах, види комп'ютерних злочинів, методи захисту від несанкціонованого доступу, а також види руйнуючих програмних засобів та методи захисту від їх дії.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

І. Нормативно-правові акти:

1. Конституція України: Закон від 28.06.1996 року № 254к/96-ВР. URL: http://zakon5.rada.gov.ua/laws/show/254к/96-вр
2. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 80731-X. Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст. 1122.
3. Конвенція про захист прав людини і основоположних свобод: з поправками, внесен. відповідно до положень Протоколів №№ 11 та 14 з Протоколами №№ 1, 4, 6, 7, 12 та 13). Право України. 2010. № 10. С. 215–233.
4. Конвенція про захист прав людини і основоположних свобод: Міжнародний документ від 04.11.1950. Редакція від 02.10.2013. URL: http://zakon.rada.gov.ua/laws/show/995_004.
5. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. // Відомості Верховної Ради України. 2001. № 25-26. Ст. 131.
6. Кримінальний процесуальний кодекс України від 13 квітня 2012 р. URL: http://zakon4.rada.gov.ua/ laws/show/4651-17.
7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.1999 № 22.
8. Правила забезпечення захисту інформації в інформаційно-телекомунікаційних системах: Постанова Кабінету міністрів України від 29.03.2006 № 373.
9. Про встановлення єдиного порядку створення комплексної системи захисту інформації в автоматизованих системах класу 1 та проведенні її державної експертизи: Наказ МВС України від 15.03.2007 № 84 дск.
10. Про дозвільну систему: Постанова Верховної Ради України від 12.10.1992 № 576.
11. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України. 2011. № 32. Ст. 314.
12. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.
13. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481
14. Про заходи із протидії витоку службової інформації. Доручення МВС України від 19.03.2015 № 13155/Ав.
15. Про недопущення витоку інформації, що утворюється в службовій діяльності. Доручення МВС України від 24.03.2015 № 19130/Ав.
16. Про інформацію: Закон України від 02.10.1996 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. ст. 650.

ІІ. Спеціальна література:

1. Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки: підруч. для студ. вищ. навч. закл., які навчаються за напрямом "Інформаційна безпека" / Державний ун-т інформаційно-комунікаційних технологій / Володимир Олексійович Хорошко (ред.). – Вид. 2-ге, допов. і переробл. – К. : ДУІКТ, 2009. – 293с.

2. Інформатика та інформаційні технології / [Б.В. Щур, І.С. Керницький, В.В. Сеник та ін.]; за ред. Б.В. Щура. – Львів: ЛьвДУВС, 2010. – 536 с.

3. Кулешник Я.Ф. Інформатика / Я.Ф. Кулешник, Т.В. Рудий, В.В. Сеник. – Львів: Львівський державний університет внутрішніх справ, 2015. – 251 с.

4. Магеровська Т.В., Сеник В.В. Інформатика: навчальний посібник / Т. В. Магеровська, В. В. Сеник. – Львів: ЛьвДУВС, 2014. – 348 с. йні технології / [Б.В. Щур, І.С. Керницький, В.В. Сеник та ін.]; за ред. Б.В. Щура. – Львів: ЛьвДУВС, 2010. – 536 с.

5. Рудий Т.В., Керницький І.С., Штангрет М.Й., Кулишник Я.Ф., Рудий А.Т. Іформаційна безпека організацій. Курс лекцій. – Львів: ЛьвДУВС, 2010. – 194 с.

6. Рудий Т. В. Організаційно-технічні засади захисту інформації в інформаційних системах слідчих підрозділів МВС України: посібник для працівників слідчих підрозділів органів внутрішніх справ України / Т. В. Рудий, О. В. Захарова, Я. Ф. Кулешник, В. В. Сеник. – Львів: ЛьвДУВС, 2013. – 240 с.

7. Сучасні інформаційні технології та їх використання у науково-педагогічній діяльності: практикум. – Л. ЛьвДУВС, 2010. – 316 с.

ІІІ. Інформаційні ресурси:

1. Офіційний веб-сайт Президента України. URL: http://www.president.gov.ua/

2. Офіційний сайт Верховної Ради України. URL: www.rada.gov.ua

3. Урядовий портал. Єдиний веб-потал органів виконавчої влади. URL: http://www.kmu.gov.ua/control/

4. Офіційний веб-потал Міністерства внутрішніх справ України. URL: http://www.mvs.gov.ua/

5. Офіційний веб-сайт Міністерства юстиції України. URL: http://www.minjust.gov.ua/

6. Офіційний веб-потал Міністерства освіти і науки України. URL: http://www.mon.gov.ua/

7. Інформаційно-пошукова правова система «Нормативні акти України (НАУ)». URL: http://www.nau.ua/

8. Вікіпедія Вільна енциклопедія. URL: http://uk.wikipedia.org

9. Електронна бібліотека Львівського державного університету внутрішніх справ. URL: http://www.lvduvs.edu.ua