**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Дніпропетровський державний університет  
внутрішніх справ**

Кафедра економічної та інформаційної безпеки

**КОНСПЕКТ ЛЕКЦІЙ**

**з дисципліни «ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ТА ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НЕДЕРЖАВНИХ СЛУЖБ БЕЗПЕКИ»**

Для здобувачів вищої освіти юридичного факультету,

спеціальності 262 "Правоохоронна діяльність"

що навчаються на бакалаврському рівні вищої освіти

**Дніпро – 2019**

Укладач: Гавриш О.С, старший викладач кафедра економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ.

Конспект лекцій обговорений та схвалений на засіданні кафедри економічної та інформаційної безпеки 27.08.2019р., протокол No14

**ТЕМА 1. ІНФОРМАЦІЙНІ РЕСУРСИ ПІДПРИЄМСТВА**

**ПЛАН ЛЕКЦІЇ:**

1. Класифікації інформаційних ресурсів.

2. Класифікація інформації в інтернеті.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

Конституція України від 28.06.1996 № 254к/95-ВР (Редакція від 21.02.2019).

Закони:

* Закон України «Про інформацію» від 02.10.1992 № 2657-XII
* Закон України «Про захист інформації в інформаційно-телекомунікаційних
* системах» від 05.07.1994 № 80/94-ВР
* Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
* Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Нормативні документи:

* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
* Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
* НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
* НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
* НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

**Навчальні посібники, інші дидактичні та методичні матеріали:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

2. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. –К.: ДУІКТ, 2016.–126с.

3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

4. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак;під ред. В.О. Хорошко.–Луганськ: Ноулідж, 2012.–480 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

**МЕТА ЛЕКЦІЇ:**

Вивчити загальне визначення інформаційного ресурсу, структуру інформаційних ресурсів, основні положення Закону України “Про Національну програму інформатизації”

**ВСТУП**

Загальне визначення інформаційного ресурсу міститься у ст. 1 Закону України “Про Національну програму інформатизації”, де інформаційні ресурси визначаються як “сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо)”.

У більш конкретному вигляді під інформаційними ресурсами розуміють організовану сукупність інформації, інформаційних продуктів та інформаційних технологій, які призначені для інформаційного забезпечення життєдіяльності людини, суспільства та держави. Тому, книги (найперші інформаційні ресурси), музеї, бібліотеки, архіви тощо – все це інформаційні ресурси.

Структуру інформаційних ресурсів складають масиви документів, окремі документи тощо, в яких накопичується та зберігається сформована за певними ознаками або критеріями інформація.

1. **Класифікації інформаційних ресурсів.**

В науковій літературі пропонується безліч засад для **класифікації інформаційних ресурсів**.

Так, за **природою** інформації, яка їх створює, інформаційні ресурси поділяються на такі, що створюються зі штучної інформації та інформації, яка утворюється самостійно, незалежно від людини.

Перший клас інформаційних ресурсів створює інформація, яка утворюється **самостійно**. Наприклад, інформація про чисельність населення в країні, інформація гідрометцентру тощо.

До другого класу інформаційних ресурсів відноситься інформація, яка створюється **штучно** в результаті інтелектуальної діяльності людини. Наприклад, математична, логічна обробка інформації, літературні твори тощо. При цьому процес творчості припускає не тільки переробку вже відомої інформації, а й створення нової інформації – прогнозів, винаходів тощо.

За **сферами** використання інформаційні ресурси поділяються на бібліотеки, архіви, фонди інформації, електронні інформаційні системи тощо. В основі цієї класифікації лежать інтереси споживачів інформації. Споживач відноситься до інформації як до джерела своїх знань, яким він користується у повсякденному житті, під час отримання освіти, професійної підготовки, перепідготовки тощо. При цьому відбувається формування інформаційних ресурсів з урахуванням потреб споживачів.

За **способом** формування інформаційних масивів і розповсюдження інформації з них інформаційні ресурси поділяються на **стаціонарні** і **мобільні**.

Стаціонарні інформаційні ресурси формуються і використовуються, як правило, в спеціалізованих інформаційних організаціях за допомогою їх інформаційних систем і мереж, у том числі й через Інтернет. Основний механізм розповсюдження інформації з таких інформаційних ресурсів реалізується в порядку надання інформаційних послуг, тобто через пошук інформації в інформаційних системах цих організацій при зверненні до них користувачів (споживачів). Причому це може здійснюватися як безпосередньо самим користувачем, якщо такі можливості надаються йому відповідною інформаційною системою, так і через посередника. Споживач повинен знати місце розташування інформаційної організації і умови отримання інформації з її ресурсів. Такий механізм отримання інформації з інформаційного ресурсу заснований на принципі: споживач рухається до ресурсу.

**Пересувні** ( або їх ще називають мобільними) інформаційні ресурси формуються державними і приватними (комерційними) інформаційними організаціями як спеціальні інформаційні продукти, головним чином, у вигляді банків даних. Такі інформаційні продукти тиражуються і розповсюджуються в комплексі - банк даних включає в свій склад і базу даних, і пошуковий апарат до неї. У цьому випадку, купуючи такий банк даних, споживач отримує можливість індивідуального користування ним на власному комп’ютері. Отже, тут використовується принцип: ресурс “рухається” до споживача. Цей принцип не новий. На його основі створювались і розповсюджувались інформаційні продукти на паперових носіях - збірники, енциклопедії, антології тощо. Але вони отримали особливо широке розповсюдження у зв’язку з розвитком нових інформаційних технологій і, зокрема, з появою лазерних дисків. Прикладом такого роду діяльності є інформаційні продукти “Ліга-Закон”, “Законодавств” та ін.

Інформаційні ресурси ще можна класифікувати за **видами інформації**, з якої вони складаються. З огляду на це існують інформаційні ресурси:

правової інформації;

науково-технічної інформації;

політичної інформації;

фінансово-економічної інформації;

статистичної інформації;

інформації про стандарти і регламенти, метрологічної інформації;

соціальної інформації; інформації про охорону здоров’я; інформації про надзвичайні ситуації; персональної інформації (персональні дані); кадастри (земельний, містобудівний, майновий, лісний, інші);

інформації іншого виду.

Інформаційні ресурси за **способом доступу поділяються** на інформаційні ресурси, які складаються з інформації відкритого доступу (без обмеження); інформації з обмеженим доступом (державна таємниця, конфіденційна інформація, комерційна таємниця, банківська та інші види таємниць, персональні дані).

За **видом** носія інформації інформаційні ресурси формуються на традиційному носії – папері, на комп’ютерних носіях інформації, в пам’яті комп’ютера, на сервері тощо.

За **способом організації зберігання** і використання інформаційні ресурси поділяються на традиційні (масив, фонд документів, архів) та автоматизовані (Інтернет, банк даних, автоматизована інформаційна система (мережа), база знань.

За **формою власності** інформаційні ресурси можуть мати статус загальноукраїнського національного надбання, державної власності, приватної власності, колективної власності.

Ще одну класифікацію інформаційних ресурсів можна провести по **видах джерел інформації та сферами їх використання**. За цими підставами інформаційні ресурси поділяються на **ресурси науково-технічної інформації, соціально-економічної, правової, освітянської, соціально-культурної** тощо.

На **законодавчому рівні** України визначаються тільки інформаційні ресурси науково-технічної інформації та інформаційні ресурси спільного користування.

Згідно зі ст. 1 Закону України “Про науково-технічну інформацію”:

- під інформаційними ресурсами науково-технічної інформації розуміється систематизоване зібрання науково-технічної літератури і документації, зафіксоване на паперових чи інших носіях;

- під інформаційними ресурсами спільного користування розуміється сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових та науково-технічних бібліотек, центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання.

Об’єктом відносин у сфері науково-технічної інформації є документована на будь-яких носіях або публічно оголошувана вітчизняна або зарубіжна науково-технічна інформація.

За допомогою сучасних технологій, інформаційних систем, в тому числі автоматизованих, банків даних, мереж і, в першу, чергу Інтернет, сьогодні забезпечується реалізація процесу обігу інформації у суспільстві, формування інформаційних ресурсів, пошуку і розповсюдження інформації з них.

**Суб’єктами відносин**, що забезпечують реалізацію цих процесів є:

- громадяни, в тому числі іноземці, особи без громадянства; організації: бібліотеки; архіви; музеї;

- інформаційні центри й інші інформаційні структури, інформаційні фонди, центри аналізу інформації;

- інформаційні агентства, інші органи масової інформації;

- інші організації – власники інформаційних ресурсів;

- органи державної влади: Верховна Рада України, Президент України, Адміністрація Президента, Конституційний Суд, Верховний Суд, Кабінет Міністрів України, міністерства, відомства, комітети.

**Власниками інформаційних** ресурсів можуть бути як самостійні інформаційні центри, інформаційні організації, фірми, підприємства, установи, які мають статус юридичної особи (далі - інформаційні організації), так і окремі інформаційні структури (управління, відділи, лабораторії тощо) в складі інших юридичних осіб, а також фізичні особи.

Інформація з інформаційних ресурсів розповсюджується в результаті підготовки інформаційних продуктів і надання інформаційних послуг. Інформаційні продукти і інформаційні послуги також можна певним чином класифікувати.

Так, **інформаційні продукти** можуть бути у вигляді: документів, даних; добірок документів, даних; довідок, аналітичних довідок; баз даних, банків даних тощо.

**Інформаційні послуги** можна представити у вигляді послуг з інформаційного обслуговування: пошук інформації, обробка інформації, видача даних (документів), збереження інформації; послуги з користування Інтернет, автоматизованими інформаційними системами (АІС), банками даних, консультаційні послуги, послуги з передачі інформації, послуги з доступу до Інтернет, послуги з користування електронною поштою і формування особистих сайтів тощо.

Інформаційні продукти і послуги надаються споживачам відповідно до чинного законодавства, договору, запиту та ін. Споживач отримує їх у порядку самообслуговування, або через посередника. Інформація може надаватися як за плату (у тому числі - на пільгових основах), так і безкоштовно. Можливий також обмін інформацією.

При формуванні інформаційних ресурсів, підготовці і наданні користувачам інформаційних продуктів, інформаційних послуг, особливо при включенні таких ресурсів у транскордонні інформаційні мережі, в першу чергу Інтернет, необхідно вирішувати питання їх захисту від несанкціонованого доступу.

У зв’язку з цим повинні захищатися: інформаційні ресурси на всіх видах носіїв, у том числі ті, що містять інформацію обмеженого доступу; інформаційні системи і їх мережі; інформаційні технології і засоби їх забезпечення; комп’ютерні носії з інформацією, наприклад, засобами електронного цифрового підпису чи криптографії; бази даних (знань) у складі автоматизованих інформаційних систем і їх мереж; програмні засоби, мережі тощо.

Одним з видів сучасних інформаційних ресурсів є **веб-ресурси**. Веб-ресурси – це інформаційні ресурси у вигляді одного чи декількох веб-сайтів.

Веб-ресурси, як і будь-які інформаційні ресурси, можуть бути об’єктами усіх форм власності, договірних відносин згідно з цивільним законодавством та законодавством про інтелектуальну власність.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Особливу увагу необхідно приділяти формуванню і використанню державних інформаційних ресурсів в частині, що стосується забезпечення повноти і актуальності інформації, яку вони містять. Основна мета цієї роботи - максимально повне і відкрите надання інформації користувачам у порядку реалізації їх основного конституційного права на пошук і отримання достовірної та повної інформації.

**2.** **Класифікація інформації в інтернеті.**

Класифікація електронних інформаційних ресурсів була б абсолютно неповною, якщо б не порушувалися питання інтернету, оскільки сьогодні більшість електронних документів доступно саме там. Тут представлено кілька основних критеріїв:

 форма подання (веб-сторінки, інформаційні і файлові сервери, бази даних, телеконференції);

 мовний і територіальна ознака;

 зміст і т. д.

**Типи інтернет-ресурсів**

Види та класифікація інформаційних освітніх ресурсів у навчальному процесі розглядаються досить докладно. Проте можна навести і деякі доповнення, включивши в розподіл ІР на класи поняття додаткових типів інтернет-ресурсів.

Як правило, серед критеріїв виділяють наступні:

 повнота і функціональний зміст;

 принцип взаємодії з користувачем (інформативне, інтерактивне);

 ступінь доступності. У змістовній частині сайти розподіляють на візитки (лаконічні сторінки з основною інформацією), блоги (персональні сторінки), промоушн-сайти (реклама товарів і послуг), електронні магазини і сервіси, інформаційні сайти з певною тематикою, веб-портали (великі ресурси або інтернет-спільноти), корпоративні представництва (системи автоматизації діяльності компаній), системи управління підприємствами, інтегровані в інтернет і інтранет (зовнішні та внутрішні мережі). При взаємодії з користувачем можна виділити такі типи ІР, як інформаційні (мережеві видання, ЗМІ, телебачення, радіо), прикладні (онлайн-бібліотеки і бази даних, сховища з можливістю скачування, пошукові системи), безпосередньо-комунікаційні (соціальні мережі, інтернет-спільноти), розважальні (ігри, музика, відео, анекдоти і т. д.), комерційні (сайти з платними послугами та інтернет-магазини), презентаційні ІР рекламного характеру. Якщо говорити про ступінь доступності, цей критерій дозволяє розділити ІР на публічні (відкриті всім користувачам без винятку), внутрішньомережеві (доступ мають тільки співробітники будь-якої організації всередині мережі інтернет), екстра-мережеві (розміщуються в інтернеті, але має доступ обмежене коло користувачів).

Згідно з законодавством, веб-сайти загального інформаційного змісту не повинні містити персональні дані або інформацію, що становить державну таємницю, та іншу інформацію, що обмежена у поширенні.

При розміщенні інформації на веб-ресурсі власник повинен:

не розміщувати на своєму веб-сайті інформацію насильницького, фашистського або іншого антилюдського змісту;

поважати релігійні, національні, культурні, політичні, професійні та інші права громадян, не розповсюджувати інформацію, яка може спровокувати національну або релігійну ворожнечу;

не розміщувати інформацію, що може зашкодити честі, гідності та репутації окремих осіб;

не розголошувати конфіденційну інформацію, а також персональні дані без згоди на це суб’єкту даних;

дотримуватись норм культури і моралі та інше.

Забороняється використання веб-ресурсів для:

втручання в особисте життя громадян;

розміщення персональних даних в базах даних загального інформаційного призначення;

поширення спотвореної інформації.

Власник інформації, у випадку нанесення йому моральної чи матеріальної шкоди в результаті поширення інформації на веб-сайті має право на повне відшкодування, згідно з чинним законодавством України на підставі рішення суду.

Власник веб-ресурсу може зареєструвати належний йому інформаційний ресурс як засіб масової інформації, що поширює відомості у телекомунікаційних мережах, у випадку, коли метою створення цього ресурсу або змістом його діяльності є розповсюдження масової інформації.

**Захист ІР**

І, само собою зрозуміло, будь ІР повинні захищатися на найвищому рівні, причому абсолютно без різниці, до якого типу вони належать, незалежно від носія, на якому вони зберігаються.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Крім того, під захистом можна розуміти і юридичний аспект (авторське право, законодавство, ліцензування, атестація), і програмні засоби у вигляді антивірусів або міжмережевих екранів (файрволів – програмних або "залізних"), криптографічних технологій шифрування даних або з'єднання і т. д.

**ВИСНОВКИ З ТЕМИ**

Як видно з усього вищесказаного, класифікацій інформаційних ресурсів можна навести досить багато, особливо якщо враховувати величезну кількість різноманітних критеріїв, які можна застосовувати в кожному конкретному випадку. Само собою зрозуміло, що деякі умовні поділу ІР на відповідні класи в різних варіантах можуть і не збігатися. Тим не менш у загальних рисах всі вони дуже схожі і мають багато спільного. Нарешті, всі класи ІР в більшості своїй тісно взаємопов'язані, а тут була приведена лише мала частина всього того, що можна розглянути, якщо конкретизувати якийсь певний тип ІР.

**ТЕМА 3. СИСТЕМАТИЗАЦІЯ ТА ЗБЕРІГАННЯ ІНФОРМАЦІЇ**

**ПЛАН ЛЕКЦІЇ:**

1. Умови безпеки інформації, державна політика та система технічного захисту інформації в Україні

2. Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

Конституція України від 28.06.1996 № 254к/95-ВР (Редакція від 21.02.2019).

Закони:

* Закон України «Про інформацію» від 02.10.1992 № 2657-XII
* Закон України «Про захист інформації в інформаційно-телекомунікаційних
* системах» від 05.07.1994 № 80/94-ВР
* Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
* Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Нормативні документи:

* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
* Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
* НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
* НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
* НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

**Навчальні посібники, інші дидактичні та методичні матеріали:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

1. Інформаційне забезпечення юридичної діяльності: підручник / кол. авт.; ред. В.Б. Вишня. - Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. - 245 с.

3. Інформатика і комп’ютерна техніка : навч. посіб. / Л.М.Дибкова. – 3-тє вид., доп. –.К.: Академвидав, 2011. – 464 с.

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.

**МЕТА ЛЕКЦІЇ:**

Познайомити студентів з державною політикою та системою технічного захисту інформації в Україні. Знати порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.

**ВСТУП**

Для здійснення обґрунтованого розподілу документів, встановлення єдиної системи формування справ, їх обліку, швидкого відшукування документів за змістом та різновидом, відбору документів для державного зберігання у процесі діловодства в установі мусить бути створена номенклатура справ**.**

1. **Умови безпеки інформації, державна політика та система технічного захисту інформації в Україні**

На сучасному етапі серед основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ до інформації, яка обробляється та циркулює на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також витік інформації технічними каналами.

Саме з метою протидії зазначеним загрозам в Україні створена та функціонує система технічного захисту інформації, яка дозволяє вирішувати практично весь комплекс завдань з технічного захисту інформації на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах державних органів, підприємств, установ та організацій.

Система являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Функції органу державного управління у сфері технічного захисту інформації виконує Департамент спеціальних систем та захисту інформації Служби безпеки України, який реалізує державну політику, здійснює управління захистом інформації в інформаційно-телекомунікаційних системах та на об’єктах інформаційної діяльності, а також державний контроль за функціонуванням системи технічного захисту інформації.

На відомчому рівні в центральних органах виконавчої влади, інших державних органах, підпорядкованих ним підприємствах, установах та організаціях створюються або визначаються підрозділи, на які покладаються завдання із забезпечення технічного захисту інформації.

На сьогодні в країні створено відповідну нормативно-правову базу, яка визначає основні принципи технічного захисту інформації, норми та вимоги з технічного захисту інформації, порядок проведення робіт та здійснення контролю його ефективності (більшість актів, що стосуються питань технічного захисту інформації, розміщено у мережі Інтернет на офіційному сайті Департаменту).

Функціонування системи технічного захисту інформації здійснюється з урахуванням необхідності забезпечення гарантії відповідності рівня захищеності інформації вимогам нормативних документів. При цьому необхідну якість робіт з технічного захисту інформації можна забезпечити за умови залучення спеціалістів, які мають відповідну фахову підготовку та досвід роботи, при відповідному технічному оснащенні.

З урахуванням зазначеного та відповідно до “Положення про технічний захист інформації в Україні”, затвердженого Указом Президента України від 27 вересня 1999 року №1229, для здійснення розроблення, впровадження, атестації та експлуатації комплексів (систем) технічного захисту інформації необхідно отримати відповідні дозволи або ліцензії.

Суб’єкти господарської діяльності отримують ліцензію відповідно до Закону України “Про ліцензування певних видів господарської діяльності” та затверджених Ліцензійних умов.

Державні органи, які мають намір проводити роботи з технічного захисту інформації для власних потреб, отримують відповідний дозвіл Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Як позитивний момент хочу відзначити, що на сьогодні дозволи на проведення робіт з технічного захисту інформації для власних потреб отримали 11-ть державних органів.

Обов’язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об’єктах інформаційної діяльності, є одержання об’єктивної оцінки рівня захищеності інформації. Це здійснюється через систему державної експертизи та атестації.

Ефективність робіт з технічного захисту інформації може бути досягнуто за умови застосування захищених засобів обробки інформації та засобів її захисту, які мають відповідні сертифікати та експертні висновки.

Для цього зазначені засоби, які надходять на український ринок і споживачі яких належать до сфери державного управління, проходять перевірку на відповідність вимогам технічного захисту інформації в Українській державній системі сертифікації продукції УкрСЕПРО, а також через державну експертизу у сфері технічного захисту інформації.

У державі створено систему підготовки, перепідготовки та підвищення кваліфікації фахівців з питань захисту інформації. В цій системі сформовано структуру необхідних спеціальностей та спеціалізацій, підготовка спеціалістів здійснюється у 20 вищих навчальних закладах, перепідготовка та підвищення кваліфікації спеціалістів здійснюється чотирма навчальними центрами. Забезпечується розроблення методичних основ науково обґрунтованої системи підготовки спеціалістів захисту інформації.

Важливе місце в системі технічного захисту інформації відіграє державний контроль за її функціонуванням, який здійснюється Інспекцією Департаменту шляхом проведення контрольно-інспекторських перевірок виконання вимог нормативно-правових актів у сфері технічного захисту інформації.

Значна увага приділяється проведенню аналізу стану технічного захисту інформації.

Серед напрямків підвищення ефективності технічного захисту інформації в державних органах Департаментом вбачається:

- створення дієво здатних підрозділів технічного захисту інформації та укомплектування їх фахівцями з відповідною підготовкою;

- розробка та впровадження відомчих нормативно-правових актів з питань технічного захисту інформації;

- визначення доцільності отримання дозволу на право провадження робіт з технічного захисту інформації для власних потреб залежно від обсягів робіт з захисту інформації та економічної доцільності;

- розробка органами, які мають дозвіл на право провадження робіт з технічного захисту інформації для власних потреб, та погодження з Департаментом документів, які дозволяють оптимізувати проведення робіт з захисту інформації в інформаційно-телекомунікаційних системах, в тому числі роботи з оцінки захищеності інформації.

Сьогодні серед основних робіт, які проводяться та супроводжуються Департаментом для забезпечення подальшого розвитку системи технічного захисту інформації, можна відзначити роботи з:

- визначення шляхів упорядкування та оптимізації заходів щодо створення, експертизи та впровадження в експлуатацію інформаційно-телекомунікаційних систем державних органів та установ, в першу чергу, призначених для обробки секретної інформації;

- підвищення безпеки вітчизняних інформаційних ресурсів шляхом розроблення та впровадження в автоматизованих системах державних органів та установ вітчизняної захищеної операційної системи;

- розробки сучасних нормативних документів з питань захисту інформації від витоку технічними каналами, створення та впровадження комплексів технічного захисту інформації на об’єктах інформаційної діяльності”.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Під час складання номенклатури справ слід керуватися положенням про орган, службу чи підрозділ установи, його штатним розкладом, планами і звітами про роботу, переліком документів із зазначенням строків їх зберігання, номенклатурами справ за попередні роки. При цьому вивчаються документи, що створюються в діяльності підрозділу, їх види і склад.

1. **Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.**

Технічний захист інформації (ТЗІ) є невід'ємною складовою частиною системи забезпечення національної безпеки України в інформаційній сфері і представлений як діяльність, що спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації в інформаційно-телекомунікаційних, інформаційних, телекомунікаційних, автоматизованих системах і на об'єктах інформаційної діяльності.

Економічно обґрунтовані комплекси і системи захисту інформації будуються адекватно загрозам її безпеки, що описуються у відповідних моделях.

На конкретних об’єктах інформаційної діяльності (ОІД) створюються комплекси ТЗІ - комплекси захисту інформації з обмеженим доступом (ІзОД) від витоку по технічних каналах.

При створенні комплексів ТЗІ досліджуються й аналізуються елементи ОІД, що можуть впливати на показники ефективності ТЗІ.

Суб’єктами створення комплексу захисту можуть бути:

- установа, яка є замовником створення комплексу захисту (далі - замовник або установа-замовник);

- структурний підрозділ установи, що обґрунтовує необхідність і заявляє створення комплексу захисту (далі – заявник);

- фахівець (фахівці), підрозділ, якому доручено організацію і супроводження робіт з ТЗІ в установі;

- суб'єкти господарської діяльності, що мають відповідні ліцензії на провадження діяльності у галузі ТЗІ.

1. Підготовчі роботи

Для підготовки пропозицій щодо організації проведення (в межах певної споруди) робіт із створення комплексу захисту (робіт з ТЗІ) заявник готує дані про необхідність використання в інформаційній діяльності ІзОД та її перелік. При цьому повинні бути враховані інформаційні потоки, технологічні та виробничі особливості, вимоги документів, що містять затверджені (рекомендовані) зведені (розгорнуті) відомості, які за режимом доступу віднесені до ІзОД. Також описується інженерно-технічна споруда, де буде створюватися комплекс (приналежність, склад, дислокація, архітектурно-будівельні границі і т.п.).

Основою для створення комплексу захисту є рішення керівника установи-замовника щодо:

- надання споруді, де планується це створення, статусу ОІД, та призначення відповідальної особи для організації, супроводження та координації робіт на всіх етапах цього створення;

- обов'язкового оформлення результатів створення комплексу згідно з встановленим порядком;

- затвердження програми для проведення обстеження ОІД (відповідно до п.4.2 ДСТУ 3396.1) та термінів виконання інших робіт з ТЗІ.

При цьому враховуються:

- пропозиції від заявників щодо організації створення комплексів захисту;

- відомості про діючі ОІД та створені в установі комплекси захисту;

- перспективу подальших робіт з ТЗІ в установі;

- технічні та економічні можливості установи щодо впровадження інженерно-технічних заходів з ТЗІ.

Зміст програми обстеження (перелік і обсяги робіт, терміни їхнього виконання, виконавці, співвиконавці обстеження) залежить від технічного стану спорудження і від того діюче (існуюче) воно чи заново будується (дані про стан спорудження, що заново будується, готує проектна організація цього будівництва).

2. Основні положення

Створення комплексів ТЗІ це:

1. Процес, пов'язаний з вивченням, дослідженням, конструктивними змінами і т.п. об'єкта, його елементів, оточення, що можуть бути можливим середовищем поширення носіїв ІзОД (складові частини технічних каналів витоку інформації).

2. Збір вихідних даних та оформлення (узгодження й затвердження) необхідних документів:

- протоколів, актів досліджень, вимірів технічних засобів, розпоряджень на експлуатацію технічних засобів, призначених для оброблення ІзОД;

- переліку загроз для безпеки ІзОД (модель загроз);

- результатів категорування на ОІД;

- технічних завдань на розробку і впровадження заходів для ТЗІ і т.п.

3. Прийняття рішень з ТЗІ, їх реалізація й оформлення (узгодження чи затвердження) необхідної документації, а саме:

- техніко-економічних обґрунтувань (ТЕО), проектно-кошторисної, робочої, конструкторської, іншої документації;

- програми і методики приймальних і атестаційних випробувань;

- протоколів випробувань;

- актів приймання й атестації комплексу.

4. Оформлення документації для введення в експлуатацію ОІД з урахуванням вимог з ТЗІ:

- технічного паспорта на комплекс ТЗІ і паспорта на кожне приміщення ОІД;

- наказів, розпоряджень (на підставі позитивних результатів атестації), що дозволяють обробляти чи озвучувати, працювати з ІзОД (для АС готують окремі дозвільні документи).

На ОІД досліджують складові комплексу, що можуть впливати на ефективність захищеності ІзОД і бути середовищем поширення носіїв ІзОД за межу контрольованої зони.

Складовими комплексу захисту на ОІД можуть бути розміщені на ньому засоби оброблення ІзОД, засоби ТЗІ, інженерні комунікації, обладнання, системи зв’язку, радіофікації, телебачення, сигналізації, автоматизації, керування, заземлення, електро-, газо-, водопостачання (холодного, гарячого), опалення, вентиляції, кондиціонування повітря, водостоку, каналізації, технологічне обладнання, огороджувальні будівельні конструкції, світлопроникнені отвори приміщень, будинків, споруд, салонів транспортних засобів тощо.

Створення комплексу ТЗІ здійснюється як під час нового будівництва, так і при розширенні, реконструкції, капітальному ремонті, пристосуванні інженерно-технічної споруди, де передбачається здійснювати діяльність, пов'язану з використанням ІзОД (далі – будівництво ОІД), у т.ч. під час створення АС.

При будівництві ОІД повинні бути впроваджені відповідні організаційні та інженерно-технічні заходи для таких видів ІзОД:

- мовної ІзОД, яка озвучується в приміщеннях ОІД, де можливе проведення нарад, показів із звуковим супроводженням кіно- і відеофільмів тощо, а також у приміщеннях, де встановлені кінцеві пристрої систем спеціального зв’язку, засоби обчислювальної техніки тощо;

- ІзОД, яка обробляється на ОІД технічними засобами (формування, збирання, введення, записування, накопичення, підсилення, перетворення, відтворення, зчитування, зберігання, копіювання, множення, знищення, реєстрація, приймання, отримання, передавання, відображення тощо);

- виробничої ІзОД, що має місце при виробництві й експлуатації продукції спеціального призначення.

Організаційні та інженерно-технічні заходи, що застосовуються при створенні комплексу захисту на ОІД, повинні відповідати вимогам нормативних документів з питань ТЗІ та містять:

- архітектурно-будівельні заходи захисту;

- інженерно-технічні заходи пасивного захисту інформації (оптичне, акустичне, електромагнітне, радіаційне екранування, технічні засоби із захистом, спеціальні засоби захисту інформації в телефонних та інших проводових лініях тощо);

- технічні заходи активного захисту інформації (генератори віброакустичного, просторового акустичного та електромагнітного зашумлення, лінійного електромагнітного зашумлення).

Як правило, в технічних рішеннях при створенні комплексу захисту на ОІД перевага повинна надаватися заходам пасивного захисту інформації.

Засоби забезпечення ТЗІ загального призначення застосовують у складі комплексу на ОІД державних органів за наявності сертифіката відповідності системи УкрСЕПРО вимогам нормативних документів з питань ТЗІ чи позитивного експертного висновка державної експертизи у сфері ТЗІ. Застосування імпортних засобів можливо лише за умови відсутності вітчизняних аналогів, за наявності відповідних техніко-економічних обґрунтувань і у випадку їх сертифікації чи одержання позитивного експертного висновка.

3. Етапи створення комплексу ТЗІ на ОІД

Створення комплексу ТЗІ на ОІД включає такі основні етапи:

1 – передпроектні роботи;

2 – розроблення та впровадження заходів з ТЗІ;

3 – випробування комплексів захисту.

3.1. На етапі виконання передпроектних робіт (1 етап):

 організовують проведення обстеження ОІД;

 організовують оформлення моделі загроз для ІзОД;

 розробляють завдання на виконання робіт зі створення комплексу;

 готують звіт про виконання передпроектних робіт;

 розробляють технічні вимоги із захисту ІзОД чи ТЗ на виконання робіт зі створення комплексу.

У ході обстеження необхідно:

- провести аналіз умов функціонування ОІД, його розташування на підприємстві, в організації, дослідити інформаційні потоки і технологічні процеси обробки інформації, об'єкти захисту;

- дослідити засоби забезпечення інформаційної діяльності, комунікації яких мають вихід за межі контрольованої зони (КЗ);

- провести аналіз схем засобів і систем життєзабезпечення ОІД (електроживлення, заземлення, пожежна й охоронна сигналізація і т.д.), а також інженерних комунікацій і металоконструкцій;

- визначити наявність і технічний стан засобів забезпечення ТЗІ;

- виявити наявність транзитних, незадіяних комунікацій, заставних пристроїв в архітектурно-будівельних конструкціях, що можуть створювати технічні канали витоку інформації;

- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтажу;

- провести аналіз зведень, приведених в організаційних, проектних, інших документах, розроблених у частині ТЗІ для існуючих об'єктів.

Звіт про виконання передпроектних робіт може містити:

а) результати обстеження ОІД, оформлення моделі загроз, розробки завдань (технічних вимог);

б) час і умови проведення категорування на ОІД, а саме встановлення категорій для кожного приміщення, де озвучується мовна ІзОД, кожного об'єкта обробки ІзОД технічними засобами і для інших об'єктів (порядок проведення категорування встановлюється діючими НД з питань ТЗІ);

в) обґрунтування необхідності:

- застосування інженерно-технічних заходів захисту (у т.ч. застосування засобів обробка ІзОД у захищеному виконанні);

- залучення до виконання робіт суб'єктів господарської діяльності в галузі ТЗІ, проектно-дослідних, будівельно-монтажних організацій;

- розробка проектно-кошторисної документації в частині ТЗІ;

г) пропозиції про порядок подальшого виконання робіт зі створення комплексу, їхній склад, обсяг, виконавців і т.п.

Під час підготовки звіту та прийняття рішень повинні бути враховані фінансові можливості замовника, особливості, обсяг і характер інформаційної (виробничої) діяльності, результати аналізу можливості здійснення загроз, співвідношення витрат на захист і наслідків здійснення загроз і т.п.

Для комплексу ТЗІ, що буде створюватися під час нового будівництва, реконструкції інженерно-технічної споруди, повинно бути розроблено:

- технічне завдання (ТЗ) на виконання робіт зі створення комплексу на ОІД, а також, у разі потреби, завдання на проектування заходів захисту відповідно до вимог ДБН А.2.2-2;

- проектно-кошторисну документацію в частині ТЗІ відповідно до вимог ДБН.

Для особливо важливих ОІД ТЗ і результати атестації комплексу узгоджуються з Департаментом спеціальних телекомунікаційних систем і захисту інформації СБ України.

3.2. На етапі розробки і впровадження заходів щодо ТЗІ (2 етап):

Розробляється “План заходів щодо захисту ІзОД на ОІД”.

У "Плані заходів..." повинно бути зазначено:

- роботи зі створення комплексу, перелік, зміст, терміни виконання, відповідальні, головні виконавці цих робіт;

- перелік технічної документації, яку необхідно розробити (у т.ч. програма і методики іспитів, технічний паспорт на комплекс;

- терміни придбання (закупівлі) технічних засобів забезпечення ТЗІ, іншого устаткування.

Відповідно до затвердженого "Планом заходів..." чи з проектними рішеннями замовник організовує:

- придбання (закупівлю) технічних засобів забезпечення ТЗІ та іншого устаткування;

- впровадження на ОІД заходів з ТЗІ;

- здійснення (у разі потреби) відповідних будівельних і монтажних робіт та післяопераційного технічного контролю їх виконання.

3.3. На етапі випробування комплексів ТЗІ (3 етап):

Комісія, що створює замовник здійснює приймання комплексу, а виконавець відповідно до затвердженої програми і методик іспитів проводить атестацію комплексу. При цьому аналізують і враховують вимоги акта категорування.

Приймання комплексу може бути об’єднане з його атестацією. Атестацію комплексу здійснюють тільки ті виконавці робіт, що мають відповідну ліцензію чи дозвіл на проведення робіт з ТЗІ. Протоколи й акт атестації комплексу також враховуються при проведенні державної експертизи КСЗІ в АС.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Після завершення атестації комплексу оформляється технічний паспорт на комплекс ТЗІ і готується наказ (розпорядження) керівника установи щодо готовності ОІД до озвучення та (або) оброблення ІзОД технічними засобами (крім оброблення ІзОД в АС: дозвіл на обробку ІзОД в АС готується за результатами проведення державної експертизи КСЗІ в АС).

**ВИСНОВКИ З ТЕМИ**

Незалежно від наявності типової чи примірної номенклатури справ кожна установа мусить мати власну, індивідуальну номенклатуру справ, в якій встановлено конкретний перелік справ, що утворюються за час її діяльності. Залежно від обсягів документного масиву, включеного до систематизованого переліку, виокремлюють індивідуальну номенклатуру справ структурного підрозділу та зведену номенклатуру справ.

**ТЕМА 4. ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ**

**ПЛАН ЛЕКЦІЇ:**

1. Апаратні засоби захисту інформації.
2. Основні групи технічних засобів ведення розвідки.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с.

2. Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації -Харків: ХНУРЕ, 2004 -368 с.

3. Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. –Львів : Видавництво Львівської політехніки, 2013. –96 с

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2014.

**МЕТА ЛЕКЦІЇ:**

Розуміти різницю між програмними та апаратними засобами захисту інформації. Знати класифікацію технічних засобів зняття інформації, системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації.

**ВСТУП**

Проблема захисту даних стала актуальною з самого початку використання обчислювальної техніки. Втрата недокументованих електронних даних спричиняла необхідність повторного виконання необхідної обробки інформації. В деяких випадках втрата вихідних даних робила неможливою повторну обробку інформації, а отже, і втрату важливих результатів.

Саме проблема захисту даних під час передачі їх між комп'ютерами (поряд із завданням збільшення швидкості їх обробки) стала поштовхом до створення комп'ютерних мереж.

Можливо, що закономірним є той факт, що саме розвиток комп'ютерних мереж став причиною надзвичайного загострення проблеми захисту даних.

1. **Апаратні засоби захисту інформації.**

Захист даних, а, отже, і захист інформації - комплексна проблема, яка є частиною національної безпеки. Необхідність вирішення проблеми захисту інформації на державному рівні викликала включення цієї проблеми до стратегії національної безпеки та прийняття Закону "Про електронний підпис". Це не останній законодавчий акт в цьому напрямі, оскільки комплексне вирішення проблеми передбачає створення єдиної правової, організаційної та матеріально-технічної бази.

На державному рівні мова йде про захист інформації державної ваги. Але і на рівні органів державного управління та місцевого самоврядування ця проблема на сьогодні стоїть досить гостро.

Чи є вашій організації організована система захисту даних?

Коли говорять про захист даних, то мають на увазі дві основних небезпеки втрати даних: пошкодження даних і несанкціонованого доступу до них. Боротьба з обома небезпеками ведеться апаратними і програмними засобами та організаційними заходами. Нижче ми розглянемо основні засоби захисту даних, які можна використовувати у своїй практичній діяльності.

До апаратних засобів захисту від пошкодження даних слід віднести використання джерел неперервного живлення, а також резервування та архівування даних.

Раптове зникнення напруги може спричинити втрату тих файлів, з якими в момент зникнення напруги працював комп'ютер. Так, наприклад, як операційна система Windows, так і програми з пакету MS Office під час роботи створюють багато тимчасових файлів, які постійно використовуються програмами. Раптове зникнення напруги може спричинити втрату цих файлів і, як наслідок, "розвал" системи і втрату файлів з даними. Найгіршим випадком є вихід з ладу жорсткого диску. Хоча відновлення інформації з цього диску ще здебільшого можливе, але це може бути не в повному обсязі і коштуватиме досить дорого.

Чому коректне вимкнення комп'ютера є важливим для збереження цілості операційної системи?

Використання джерел неперервного живлення (UPS) дає можливість у випадку пропадання напруги в мережі підтримувати роботу системи ще протягом 20 хв. За цей час завершиться виконання всіх програм і комп'ютер можна буде вимкнути без втрати всіх даних. У відповідальніших випадках використовують резервне живлення або з мережі, або від автономного джерела.

Резервування інформації дає можливість у випадку втрати даних повернути стан системи на момент її резервування. При цьому резервні копії можна зберігати у захищених місцях (приміщеннях чи сейфах). Для резервування використовують або засоби постійної пам'яті (компакт-диски, стримери, переносні жорсткі диски), або жорсткі диски на іншому комп'ютері в мережі.

Для інформації невеликого обсягу цілком придатний спосіб зберігання даних у вигляді архіву на тому ж комп'ютері, на автономному носії або на іншому комп'ютері. Принципово - це те ж саме резервування даних, але в трансформованому (стисненому) вигляді. Для архівування використовують програми WinZIP або WinRAR. Доречі, в архівованому вигляді дані легше передавати засобами електронного зв'язку в мережі. При цьому бажано користуватись архіватором ZIP.

Чи використовується у вашій організації централізована система архівування даних?

До апаратних засобів захисту від несанкціонованого доступу найкраще використовувати засоби постійної пам'яті - компакт-диски і переносні жорсткі диски. В цьому випадку дані будуть захищені навіть при пошкодженні чи втраті комп'ютера. Ні в якому випадку для тривалого зберігання даних не слід використовувати дискети. Для цього їх надійність занадто низька.

До апаратних засобів захисту даних від несанкціонованого доступу належать також :

**криптографічні плати**, за допомогою яких дані можна зашифрувати, створити електронний підпис та аутентифікувати користувача;

**магнітна картка SmartCard** для зберігання секретного ключа та шифрування паролів;

**пристрої ActiveCard** для введення паролів, в яких паролі обчислюються на підставі уведених даних (динамічні паролі), та **SmartReader** для зчитування цих паролів. Чотиризначний пароль, що вводиться користувачем, перераховується в цих пристроях у спеціальний код.

**До технічних засобів** можна віднести і біометричні засоби, тобто: зчитування візерунку сітчатки ока, відбитків пальців, геометрії рук, динаміки підпису. Крім цього використовують також комплекси технічних засобів захисту від несанкціонованого доступу до даних, які можна згрупувати наступним чином:

*захист* від електромагнітного випромінювання, куди відносяться: використання оптоволоконних кабелів, захисної плівки на вікнах, захищених дисплеїв;

*захист* від поновлення знищених даних;

*захист* від підслуховування шляхом: встановлення фільтрів на лініях зв'язку, попередження встановлення підслуховуючих пристроїв, використання звукопоглинаючих покрить, протипідслуховувального зашумлення.

Бурхливий розвиток техніки, технології, інформатики в останні десятиліття викликав ще більш бурхливий розвиток технічних пристроїв і систем розвідки. Справді, занадто часто виявлялося вигідніше витратити N-у суму на добування, наприклад, технології, що вже існує, чим у кілька разів більшу на створення власної. А в політиці чи у військовій справі виграш іноді виявляється просто безцінним.

У створення пристроїв і систем ведення розвідки вкладалися і вкладаються величезні кошти у всіх розвинених країнах. Сотні фірм багатьох країн активно працюють у цій галузі. Серійно виробляються десятки тисяч моделей "шпигунської" техніки. Ця галузь бізнесу давно і стійко зайняла своє місце в загальній системі економіки Заходу і має міцну законодавчу базу.

У західній пресі можна знайти дуже захоплюючі документи про існування і роботу міжнародної організації промислового шпигунства "Спейс Інкорпорейтед", а заодно і познайомитися зі спектром послуг, пропонованих цією компанією. Так, англійська газета "Піпл" повідомляє, що серед клієнтів компанії є не тільки промисловці, але й організовані злочинні угруповання. Як і будь-який бізнес, коли він вигідний, торгівля секретами розширює область діяльності, знаходячи для свого процвітання вигідний ґрунт.

Тематики розробок на ринку промислового шпигунства охоплюють практично всі сторони життя суспільства, безумовно, орієнтуючись на найбільш фінансово-вигідні.

У СРСР після 1917 року ведення комерційної розвідки знаходилося під строгим контролем держави. У Радянському Союзі в цій галузі були зосереджені чудові, якщо не сказати кращі, фахівці. Видатним досягненням було і залишиться на багато років чудо технічної розвідки — будинок посольства США в Москві, перетворене у величезне "вухо", у якому кожен подих, кожен шерех був доступний для запису й аналізу. Датчики знаходили навіть у зварених сталевих конструкціях будинку, причому по щільності матеріалу вони відповідали навколишньому металу і були недоступні для рентгенівського аналізу. Ці системи були здатні функціонувати автономно десятки років. Американці змушені були відмовитися від використання цього будинку, навіть незважаючи на те, що колишній глава КДБ Вадим Бакатін передав їм схему побудови цієї системи.

Катастрофа СРСР і розвиток вільної ринкової економіки відродило попит на техніку подібного роду. Фахівці військово-промислового комплексу, що залишилися без роботи, не сповільнили запропонувати свої послуги й у цій області. Спектр послуг широкий: від примітивних радіопередавачів до сучасних апаратно-програмних комплексів ведення розвідки. Звичайно, у нас немає ще великих фірм, що роблять техніку подібного роду, немає і такого достатку моделей, як на Заході, але техніка наших виробників цілком порівнянна по своїм даним з аналогічної західною, а іноді краще і дешевше. Зрозуміло, мова йде про порівняння техніки, що мається у відкритому продажі.

Природно, апаратура, використовувана спецслужбами (її кращі зразки) набагато перевершує по своїх можливостях техніку, використовувану комерційними організаціями. Як приклад можна привести самий маленький і самий дорогий у світі радіомікрофон, габарити якого не перевищують чверті олівцевої гумки для стирання . Цей мініатюрний передавач живиться від ізотопного елемента і здатний протягом року сприймати і передавати на прийомний пристрій, розташований за півтора кілометра, розмову, що ведеться в приміщенні пошепки. Крім того, уже зараз виробляються радіо закладки, що можуть записувати перехоплену інформацію, зберігати її протягом доби чи тижня, передати в режимі швидкодії за мілісекунду, стерти запис і почати процес знову.

Сучасні злочинні угрупування мають на озброєнні новітні технічні засоби отримання, обробки та захисту інформації. Частину таких засобів, як вітчизняного, наприклад радіокапсула Р1 - Р9, приймачі RH-03, RA-05, RA-07, конвертори CO-01 та інші, так і імпортного виробництва, наприклад лазерний мікрофон HP-150 фірми “Hewlett-Packard”, до останнього часу можна було придбати у відкритій торгівлі. Крім того є багато літератури, яка дозволяє практично будь-якому радіоаматору кустарно виготовити радіомікрофони та інші технічні засоби ведення розвідувальної та контррозвідувальної діяльності.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Бурхливий розвиток техніки, технології, інформатики в останні десятиліття викликав ще більш бурхливий розвиток технічних пристроїв і систем розвідки. Справді, занадто часто виявлялося вигідніше витратити N-у суму на добування, наприклад, технології, що вже існує, чим у кілька разів більшу на створення власної. А в політиці чи у військовій справі виграш іноді виявляється просто безцінним.

**2. Основні групи технічних засобів ведення розвідки.**

1. Радіопередавачі з мікрофоном (радіомікрофони):

— с автономним живленням;

— с живленням від телефонної лінії;

— с живленням від електромережі;

— керовані дистанційно;

— що використовують функцію вмикання по голосу;

— напівактивні;

* с накопиченням інформації і передачею в режимі швидкодії.

1. Електронні пристрої знімання акустичної інформації:

— мікрофони з проводами;

— електронні стетоскопи ( що прослухують через стіни);

— мікрофони з гострою діаграмою спрямованості;

— лазерні мікрофони;

— мікрофони з передачею через мережу 220 В.;

— прослуховування через мікрофон телефонної трубки;

* гідроакустичні мікрофони.

1. Пристрої перехоплення телефонних повідомлень:

— безпосереднього підключення до телефонної лінії;

— підключення з використанням індукційних датчиків (датчики Холу й ін.);

— с використанням датчиків, розташованих усередині телефонного апарату;

— телефонний радіотранслятор;

— перехоплення повідомлень сотового телефонного зв'язку;

— перехоплення пейджерних повідомлень;

— перехоплення факс-повідомлень;

* спеціальні багатоканальні пристрої перехоплення телефонних повідомлень.

1. Пристрої прийому, запису, управління:

— приймач для радіомікрофонів;

— пристрої запису;

— ретранслятори;

— пристрої запису і передачі в прискореному режимі;

* пристрої дистанційного управління.

1. Відеосистеми запису і спостереження.
2. Системи визначення місця розташування контрольованого об'єкта.
3. Системи контролю комп'ютерів і комп'ютерних мереж.

Радіомікрофон, як випливає з назви, це мікрофон, об'єднаний з радіо, тобто з радіоканалом передачі звукової інформації. В даний момент немає устояної назви цих пристроїв. Їх називають радіозакладками, радіобагами, радіокапсулами, іноді - "жуками", але все-таки самою точною назвою варто визнати назва "радіомікрофон".

Радіомікрофони є найпоширенішими технічними засобами отримання акустичної інформації. Їхня популярність пояснюється, насамперед, зручністю їхнього оперативного використання, простотою застосування (не потрібно тривалого навчання персоналу), дешевиною, дуже невеликими розмірами. У найпростішому випадку радіомікрофон складається з власне мікрофона, тобто пристрою для перетворення звукових коливань в електричні, а також радіопередавача - пристрою, що випромінює в простір електромагнітні коливання радіодіапазону (несучу частоту), промодульовані електричними сигналами з мікрофона. Мікрофон визначає зону акустичної чутливості (звичайно вона коливається від декількох до 20 -30 метрів), радіопередавач — дальність дії радіолінії. Визначальними параметрами з погляду дальності дії для передавача є потужність, стабільність несучої частоти, діапазон частот, вид модуляції. Істотний вплив на довжину радіоканалу надає, звичайно, і тип радіоприймального пристрою. На прийомних пристроях ми зупинимося, хоча і коротко, пізніше.

Пристрій управління не є обов'язковим елементом радіомікрофону. Він призначений для розширення його можливостей: дистанційного вмикання-вимикання передавача, мікрофона, пристрою, що записує. Можуть бути передбачені режими: включення по голосі, режим запису в реальному часі, режим прискореного відтворення і т.д.

Пристрій запису, як випливає зі сказаного вище, також не є обов'язковим елементом.

Розроблено і випускаються серійно сотні моделей радіомікрофонів, у тому числі не менш ста типів — у Росії і СНД (в основному на Україні й у Білорусії).

Технічні дані радіомікрофонів знаходяться в наступних межах:

вага .................................................. від 5 до 350 гр

габарити .......................................... від 1 см3 до 8 дм3

частотний діапазон ........................ від 27 до 900 Мгц

потужність ...................................... від 0,2 до 500 мвт

дальність без ретранслятора ......... від 10 до 1500 м

час безупинної роботи ..........від декількох годин до декількох років.

Дальність дії, габарити і час безупинної роботи знаходяться в дуже тісній залежності друг від друга. Справді, для збільшення дальності необхідно, насамперед, підняти потужність, одночасно зростає струм, споживаний від джерела живлення, що швидше витрачає свій ресурс, а виходить, скорочується час безупинної роботи. Щоб збільшити цей час, збільшують ємність батарей живлення, але це збільшує габарити радіомікрофону. Можна збільшити тривалість роботи передавача введенням у його склад пристрою дистанційного управління (умикання-вимикання), однак це також збільшує габарити. Крім того, потрібно мати на увазі, що збільшення потужності передавача полегшує можливість його виявлення.

Одним з перспективних напрямків збільшення скритності і часу ефективного використання є застосування дистанційного включення. Прикладами є вироби TRM-1530 і TRM-1532. Це радіомікрофони з живленням від батарей, габаритами 87х54х70 мм, вагою близько 100 гр, із ЧМ передавачем діапазону 380-400 Мгц чи 100-150 Мгц і дальністю до 300 м. Дистанційне вмикання-вимикання дозволяє довести час ефективної роботи виробу до 1 року при часі безупинної роботи 280-300 годин. Подібна апаратура, але більш великих габаритів, починає надходити в продаж і від вітчизняних виробників.

Дуже перспективним є застосування радіомікрофонів з активацією від звуку — музики, мови і т.д. Така модель STG-4001. Включення пристрою походить від звуку, вимикання — автоматично через 5 секунд після зникнення звуку. Застосування функції включення по голосі дозволило довести час ефективної роботи до 300 годин. Прилад має дуже прийнятні розміри — 20х38х12 мм, вага з батареями — 18 м, забезпечує дальність до 500 м, частоти — 130-150 Мгц. Варто підкреслити, що такого роду радіомікрофони досить важко знайти.

У складних випадках можлива побудова системи передавачів. Наприклад, при русі об'єкта по шляху проходження заздалегідь розміщаються радіомікрофони, що працюють на різних частотах. Спостереження ведеться за допомогою багатоканального приймача. Можлива побудова схеми з використанням передавача-ретранслятора. Потужність радіомікрофону робиться дуже невеликою (для збільшення часу роботи і підвищення скритності), а на невеликій відстані, наприклад, у сусіднім приміщенні, установлюється передавач-ретранслятор, габарити і потужність якого піддаються набагато меншим обмеженням.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Як уже говорилося вище, дальність дії радіопередавачів визначається в істотному ступені якостями радіоприймальних пристроїв, насамперед, чутливістю. Як приймачі часто використовують побутові радіоприймальні пристрої. У цьому випадку кращим є застосування магнітол, тому що з'являється можливість одночасного ведення запису. До недоліків таких пристроїв відносяться низька чутливість і можливість настроювання сторонніх облич на частоту передавача. Частково ці недоліки можна усунути перебудовою частотного діапазону, у тому числі за допомогою конверторів, а також переналагодженням підсилювачів для підвищення чутливості. Достоїнством таких систем є низька вартість, а також те, що вони не викликають підозр. Але все-таки кращим варто вважати застосування спеціальних прийомних пристроїв.

**ВИСНОВКИ З ТЕМИ**

Безпека інформаційного середовища підприємства безпосередньо залежить від співвідношення між технічним рівнем устаткування, яке застосовується для несанкціонованого доступу і технічним рівнем устаткування, яке застосовується для захисту від несанкціонованого доступу.

При цьому необхідно враховувати, що придбання обладнання для захисту інформації зазвичай обходиться дорожче, ніж отримання обладнання такого ж рівня для несанкціонованого доступу. Це пов'язано з тим, що зловмисники використовують якийсь один спосіб несанкціонованого доступу, а забезпечувати захист треба від усіх можливих способів.

Тому при організації захисту завжди визначається розумний компроміс між цінністю інформації та витратами на забезпечення її безпеки.

**ТЕМА 5. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**

**ПЛАН ЛЕКЦІЇ:**

1. Криптографічні методи захисту

2. Основи криптоаналізу

3. Стеганографія

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1.Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с.

2.Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації -Харків: ХНУРЕ, 2004 -368 с.

3.Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. –Львів : Видавництво Львівської політехніки, 2013. –96 с

4. Інформатика в юридичній діяльності / Кудінов В.А., Хахановський В.Г., Пакриш О.Є. та ін. за заг. редакцією В.А. Кудінова. – К.: Нац. акад. внутр. справ, 2016. – 256 с.

5. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

6. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2014.

**МЕТА ЛЕКЦІЇ:**

Познайомити студентів з основними поняттями криптології, сформувати в студентів представлення про сучасні методи криптології.

**ВСТУП**

Проблемою захисту інформації шляхом її перетворення займається криптологія (kryptos – таємний, logos – повідомлення). Вона має два напрямки: криптографію і криптоаналіз. Цілі цих двох напрямків прямо протилежні.

Криптографія займається пошуком, дослідженням і розробкою математичних методів перетворення інформації, основою яких є шифрування, а криптоаналіз – дослідженням можливості розшифровки інформації.

Основні напрямки використання криптографічних методів – це передача конфіденційної інформації через канали зв’язку (наприклад, електронна пошта), встановлення дійсності переданих повідомлень, збереження інформації (документів, баз даних) на носіях у зашифрованому вигляді.

**1. Криптографічні методи захисту.**

Сучасна криптографія вивчає і розвиває такі напрямки:

* симетричні криптосистеми (зі секретним ключем);
* несиметричні криптосистеми (з відкритим ключем);
* системи електронного підпису;
* системи управління ключами.

Сучасні криптографічні системи забезпечують високу стійкість зашифрованих даних за рахунок підтримки режиму таємності криптографічного ключа. Однак на практиці будь-який шифр, який використовується в тій або іншій криптосистемі, піддається розкриттю з визначеною трудомісткістю. Через це, виникає необхідність оцінки криптостійкості шифрів, які застосовуються, в алгоритмах криптоперетворення.

Допомагаючи зберегти зміст повідомлення в таємниці, криптографію можна використовувати для забезпечення:

– аутентифікації;

– цілісності;

– незаперечності.

Під час аутентифікації одержувачу повідомлення потрібно переконатися, що воно виходить від конкретного відправника. Зловмисник не може надіслати фальшиве повідомлення від будь-якого імені.

Під час визначення цілісності одержувач повідомлення в змозі перевірити, чи були внесені які-небудь зміни в отримане повідомлення під час його передачі. Зловмисникові не дозволено замінювати дійсне повідомлення на фальшиве.

Незаперечність необхідна для того, щоб відправник повідомлення не зміг згодом заперечувати, що він не є автором цього повідомлення.

В цей час аутентифікація, що здійснюється користувачем, забезпечується за допомогою:

– смарт-карт;

– засобів біометрії;

* клавіатури комп’ютера;

– криптографії з унікальними ключами для кожного користувача.

Основною сферою застосування смарт-карт є ідентифікація користувачів мобільними телефонами.

Біометрія заснована на анатомічній унікальності кожної людини. Біометричні системи ідентифікації наведені на рис. 5.1.

Біометричні системи ідентифікації

Фізичні

Особливості поведінки

Відбитки пальців

Підпис

Геометрія руки

Геометрія обличчя

Структура ДНК

Форма вушної раковини

Рисунок райдужної оболонки ока

Форма вушної раковини

Форма вушної раковини

Форма вушної раковини

Рис. 5.1. Біометричні системи ідентифікації

Цілісність інформації забезпечується за допомогою криптографічних контрольних сум і механізмів управління доступом і привілеями. Як криптографічна контрольна сума для виявлення навмисної або випадкової модифікації даних використовується код аутентифікації повідомлення – MAC (Message Autentification Code).

Для виявлення несанкціонованих змін у переданих повідомленнях можна застосувати:

* електронно-цифровий підпис (ЕЦП), заснований на криптографії з відкритим і закритим ключами;
* програми виявлення вірусів;
* призначення відповідних прав користувачам для управління доступом;
* точне виконання прийнятого механізму привілеїв.

Незаперечність повідомлення підтверджується електронно-цифровим підписом.

*Характеристика алгоритмів шифрування.* У цей час спостерігається різке зростання об’ємів інформації (у тому числі і конфіденційної), яка передається по відкритих каналах зв’язку. Тому все більш актуальною стає проблема захисту переданої інформації. Незважаючи на те, що конкретні реалізації систем захисту інформації можуть істотно відрізнятися одна від іншої через розбіжність методів і алгоритмів передачі даних, усі вони повинні забезпечувати вирішення триєдиного завдання:

* конфіденційність інформації (доступність її тільки для того, кому вона призначена);
* цілісність інформації (її достовірність і точність, а також захищеність від навмисних і ненавмисних перекручувань);
* готовність інформації (використання в будь-який момент, коли в ній виникає потреба).

Успішне вирішення перерахованих завдань можливе як за рахунок використання організаційно-технічних заходів, так і за допомогою криптографічного захисту інформації.

Організаційно-технічні заходи містять у собі фізичну охорону об’єктів конфіденційної інформації, застосування спеціального адміністративного персоналу і цілу низку інших дорогих технічних заходів для захисту важливих даних.

Криптографічний захист здебільшого є більш ефективним і дешевим. Конфіденційність інформації у цьому разі забезпечується шифруванням переданих документів або всього трафіка.

Процес криптографічного захисту даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги, а саме: висока продуктивність, простота, захищеність і так далі. Програмна реалізація більш практична, допускає значну гнучкість у використанні. До сучасних криптографічних систем захисту інформації висувають такі вимоги:

* зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;
* кількість операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинна бути не менше, ніж загальна кількість можливих ключів;
* кількість операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинна мати чітку нижню оцінку і виходити за межі можливостей сучасних комп’ютерів (з урахуванням можливості використання мережевих обчислень);
* знання алгоритму шифрування не повинне впливати на надійність захисту;
* незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення навіть під час використання того ж ключа;
* структурні елементи алгоритму шифрування повинні бути незмінними;
* додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;
* довжина шифрованого тексту повинна дорівнювати довжині вихідного тексту;
* не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;
* будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;
* алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

Криптографічний алгоритм, названий алгоритмом шифрування, являє собою деяку математичну функцію, яка використовується для шифрування і розшифрування. Точніше таких функцій дві: одна застосовується для шифрування, а інша – для розшифрування.

Розрізняють шифрування двох типів:

* симетричне (із секретним ключем);
* несиметричне (з відкритим ключем).

У разі симетричного шифрування (рис. 5.2) створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв’язку. Адресат, запустивши ту ж шифрувальну програму з отриманим ключем, зможе прочитати повідомлення. Симетричне шифрування не таке надійне, як несиметричне, оскільки ключ може бути перехоплений, але через високу швидкість обміну інформацією воно широко використовується, наприклад, в операціях електронної торгівлі.

010101100010001

Шифрування

Привіт

Розшифровка

Привіт

Ключ

Канал зв'язку

Шифроване повідомлення

Повідомлення

Повідомлення

Рис. 5.2. Симетричне шифрування

Несиметричне шифрування складніше, але і надійніше. Для його реалізації (рис. 5.3) потрібні два взаємозалежних ключі: відкритий і закритий. Одержувач повідомляє всім, хто бажає, свій відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифроване повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній розшифровує його за допомогою свого закритого ключа. Підвищена надійність несиметричного шифрування потребує складнішого обчислення, тому процедура розшифровки займає більше часу.

Коли надійність криптографічного алгоритму забезпечується за рахунок збереження в таємниці суті самого алгоритму, такий алгоритм шифрування називається обмеженим. Обмежені алгоритми становлять значний інтерес з погляду історії криптографії, однак зовсім непридатні у сучасних вимогах, які висуваються до шифрування. Адже, в цьому разі, кожна група користувачів, які бажають обмінюватися секретними повідомленнями, повинна мати свої оригінальні алгоритми шифрування.

01100010001

Привіт

Привіт

Шифрування

Розшифровка

Відкритий ключ

Канал зв'язку

Шифроване повідомлення

Повідомлення

Повідомлення

11110101

Закритий ключ

Рис. 5.3. Несиметричне шифрування

У сучасній криптографії зазначені вище проблеми вирішуються за допомогою використання ключа, який потрібно вибирати серед значень, що належать безлічі (ключовий простір). Функції шифрування і розшифрування залежать від цього ключа. Деякі алгоритми шифрування використовують різні ключі для шифрування і розшифровування. Це означає, що ключ шифрування відрізняється від ключа розшифровування.

Надійність алгоритму шифрування з використанням ключів досягається за рахунок їх належного вибору і наступного збереження в секреті. Це означає, що такий алгоритм не потрібно тримати в таємниці. Можна організувати масове виробництво криптографічних засобів, в основу функціонування яких покладений цей алгоритм. Навіть знаючи криптографічний алгоритм, зловмисник не зможе прочитати зашифровані повідомлення, оскільки він не знає секретний ключ, використаний для його зашифровування.

Симетричні алгоритми шифрування поділяють на:

* потокові;
* блокові.

Алгоритми, у яких відкритий текст обробляється побітно, називаються потоковими алгоритмами або потоковими шифрами. В інших алгоритмах відкритий текст розбивається на блоки, що складаються з декількох біт. Такі алгоритми називаються блоковими або блоковими шифрами. У сучасних комп’ютерних алгоритмах блокового шифрування довжина блока звичайно складає 64 біти. Симетричні алгоритми у разі виявлення в них будь-яких слабкостей можуть бути дороблені шляхом внесення невеликих змін, а для несиметричних – така можливість відсутня.

Симетричні алгоритми працюють значно швидше, ніж алгоритми з відкритим ключем. На практиці несиметричні алгоритми шифрування часто застосовуються в сукупності з симетричними алгоритмами: відкритий текст зашифровується симетричним алгоритмом, а секретний ключ цього симетричного алгоритму зашифровується на відкритому ключі несиметричного алгоритму. Такий механізм називають цифровим конвертом (digital envelope). Найчастіше в цей час застосовують такі алгоритми шифрування:

* DES (Data Encryption Standard);
* Blowfish;
* IDEA (International Decryption-Encryption Algorithm);
* ГОСТ 28147-89;
* RSA (автори: Rivest, Shamir і Alderman);
* PGP.

У симетричних криптоалгоритмах (DES, ДСТ, Blowfish, RC5, IDEA) для шифрування і розшифрування інформації використовується той же секретний ключ. Перевагами таких алгоритмів є:

* простота програмної та апаратної реалізації;
* висока швидкість роботи в прямому і зворотному напрямках;
* забезпечення необхідного рівня захисту інформації під час використання коротких ключів.

До основних недоліків цих криптоалгоритмів варто віднести збільшення витрат щодо забезпечення додаткових заходів таємності під час поширення ключів, а також те, що алгоритм із секретним ключем виконує своє завдання тільки в умовах повної довіри кореспондентів один одному.

У несиметричних криптоалгоритмах (RSA, PGP, ECC) пряме і зворотне перетворення виконуються з використанням відкритого і секретного ключів, що не мають взаємозв’язку, що дозволяє по одному ключу обчислити інший. За допомогою відкритого ключа практично будь-який користувач може зашифрувати своє повідомлення або перевірити електронно-цифровий підпис. Розшифрувати таке повідомлення або поставити підпис може тільки власник секретного ключа.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

Такі алгоритми дозволяють реалізувати протоколи типу цифрового підпису, забезпечують відкрите поширення ключів і надійну аутентифікацію в мережі, стійкій навіть до повного перехоплення трафіка.

**5.2. Основи криптоаналізу**

Криптоаналіз (від давньогрец. κρυπτός – прихований і аналіз) – наука про методи розшифровування зашифрованої інформації без призначеного для такої розшифровки ключа.

Термін був введений американським криптографом Уїльямом Ф. Фрідманом 1920 року. Неформально криптоаналіз називають також зломом шифру.

Здебільшого під криптоаналізом розуміють з’ясування ключа; криптоаналіз включає також методи виявлення уразливості криптографічних алгоритмів або протоколів.

Спочатку методи криптоаналізу ґрунтувалися на лінгвістичних закономірностях природного тексту і реалізовувалися з використанням тільки олівця й паперу. В криптоаналізі застосовують математичні методи, для реалізації яких використовують спеціалізовані криптоаналітичні комп’ютери.

Спробу розкриття конкретного шифру із застосуванням методів криптоаналізу називають криптографічного атакою на цей шифр. Криптографічну атаку, в ході якої розкрити шифр вдалося, називають зломом або розкриттям.

Брюс Шнайер виділяє 4 основних і 3 додаткових методи криптоаналізу, припускаючи знання криптоаналітика алгоритму шифру :

Атаки на основі шифротексту. Припустимо, криптоаналітик має деяку кількість шифротекстів, отриманих в результаті використання одного і того ж алгоритму шифрування. У цьому разі криптоаналітик може зробити тільки атаку на основі шифротексту. Метою криптографічної атаки в цьому разі є знаходження якомога більшої кількості відкритих текстів, відповідних наявним шифротекстам, або, що ще краще, знаходження використовуваного під час шифрування ключа.

Вхідні дані для подібних атак криптоаналітик може отримати в результаті простого перехоплення зашифрованих повідомлень. Якщо передача здійснюється по відкритому каналу, то реалізація завдання щодо збору даних порівняно легка і тривіальна. Атаки на основі шифротексту є найслабшими і найнезручнішими.

Атака на основі відкритих текстів і відповідних шифротекстів. Нехай у розпорядженні криптоаналітика є не тільки шифротексти, але і відповідні їм відкриті тексти. Тоді існує два варіанти постановки завдання: 1) знайти ключ, використаний для перетворення відкритого тексту в шифротекст; 2) створити алгоритм, здатний дешифрувати будь-яке повідомлення, закодоване за допомогою цього ключа.

Отримання відкритих текстів відіграє вирішальну роль у здійсненні цієї атаки. Відкриті тексти витягують з різних джерел. Так, наприклад, можна здогадатися про вміст файлу по його розширенню.

У разі злому листування можна зробити припущення, що лист має у вигляді:

«Привітання»

«Основний текст»

«Заключна форма ввічливості»

«Підпис».

Отже, атака може бути організована шляхом підбору різних видів «Привітання» (наприклад, «Привіт!», «Добрий день» і т. д.) і/або «Заключною формою ввічливості» (таких як «З повагою», «Щиро Ваш» тощо). Легко помітити, що ця атака сильніша, ніж атака на основі одного лише шифротексту.

Атака на основі підібраного відкритого тексту. Для здійснення такого типу атаки криптоаналітику необхідно мати не тільки якусь кількість відкритих текстів та отриманих на їх основі шифротекстів, до того ж у цьому разі криптоаналітик повинен мати можливість підібрати кілька відкритих текстів і отримати результат їх шифрування.

Завдання криптоаналітика повторюють завдання для атаки на основі відкритого тексту, тобто отримати ключ шифрування, або створити алгоритм дешифрування для даного ключа.

Отримати вхідні дані для такого виду атаки можна, наприклад, так: створити і відправити підроблене НЕ зашифроване повідомлення нібито від одного з користувачів, які зазвичай користуються шифруванням.

У деяких випадках можна отримати відповідь, в якій буде зашифрований текст, що цитує зміст підробленого повідомлення.

Під час здійснення атаки подібного типу криптоаналітик має можливість підбирати блоки відкритого тексту, що за певних умов може дозволити отримати більше інформації про ключі шифрування.

*Атаки на основі адаптаційно підібраного відкритого тексту.* Атака такого типу є більш зручним окремим випадком атаки на основі підібраного відкритого тексту. Зручність атаки на основі адаптаційно підібраного відкритого тексту полягає в тому, що крім можливості вибирати шифрований текст, криптоаналітик може прийняти рішення про шифрування того чи іншого відкритого тексту на основі вже отриманих результатів операцій шифрування. Інакше кажучи, під час атаки на основі підібраного відкритого тексту криптоаналітик вибирає всього один великий блок відкритого тексту для подальшого шифрування, а потім на основі цих даних починає зламувати систему. У разі організації адаптаційної атаки криптоаналітик може отримувати результати шифрування будь-яких блоків відкритого тексту, щоб зібрати цікаві для нього дані, які будуть враховані при виборі наступних відправлених на шифрування блоків відкритого тексту і так далі.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

Через наявність зворотного зв’язку атака на основі адаптаційно підібраного шифротексту має перевагу перед усіма перерахованими вище типами атак.

**5.3. Стеганографія**

Стеганографія — (з грец. *στεγανός* — прихований + *γράφω* — пишу) — тайнопис, при якому повідомлення, закодоване так, що не виглядає як повідомлення — на відміну від криптографії. Отже, непосвячена людина принципово не може розшифрувати повідомлення — бо не знає про факт його існування.

Якщо криптографія приховує зміст повідомлення, то стеганографія приховує сам факт існування повідомлення.

*Історія.* Перший запис про використання стеганографії зустрічається в трактаті Геродота «Історія», що належить до 440 року до н. е. У трактаті були описані два методи приховування інформації. Демарат відправив попередження про майбутній напад на Грецію, записавши його на дерев’яну підкладку воскової таблички до нанесення воску. Другий спосіб полягав у такому: на поголену голову раба записувалося необхідне повідомлення, а коли його волосся відростало, він вирушав до адресата, який знову голив його голову і зчитував доставлене повідомлення.

У Китаї листи писали на смужках шовку. Для приховування повідомлень смужки з текстом листа згортали в кульки, покривали воском і потім посильні їх ковтали.

У XV ст. чернець Трітеміус (1462–1516), який займався криптографією і стеганографією, описав багато різних методів прихованої передачі повідомлень. Пізніше, в 1499 році, ці записи були об’єднані в книгу «Steganographia».

Метод приховування інформації за допомогою мікроточки з’явився відразу ж після винаходу Даґером фотографічного процесу, і вперше у військовій справі був використаний під час Франко-прусської війни (1870 р.), але широкого застосування до Другої світової війни цей метод не мав.

У березні 2000 р. 17-річна американська школярка Вівіана Риска (Viviana Risca) створила алгоритм, який може «ховати» повідомлення в генну послідовність ДНК. На конкурсі молодих вчених компанії Intel Science Talent Search вона продемонструвала технологію впровадження комп’ютерних повідомлень в генну послідовність молекули.

*Методи.* Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі дізнатися про його існування. Одна з перших згадок про застосування тайнопису датується V ст. до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносилась шифрована інформація про умови складання контракту.

Комп’ютерна стеганографія ґрунтується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію. Сімейна цифрова фотографія може містити комерційну інформацію, а файл із записом сонати Гайдна — приватний лист.

Але найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканність документа, ідентифікувати автора або власника, перевірити права дистриб’ютора або користувача, навіть якщо файл був оброблений або спотворений.

Щодо впровадження засобів програмно-технічного захисту в ІС, розрізняють два основні його способи:

* додатковий захист — засоби захисту є доповненням до основних програмних і апаратних засобів комп’ютерної системи;
* вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потреби, але під час його реалізації можуть виникнути проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таке доповнення характеристик способів захисту зумовлено тим, що в реальній системі їх комбінують.

*Класифікація стеганографії.* Наприкінці 90-х років виділилося кілька напрямків стеганографії:

* класична стеганографія;
* комп’ютерна стеганографія;
* цифрова стеганографія;
* мережева стеганографія.

*Класична.* Одним з найпоширеніших методів класичної стеганографії є використання симпатичних чорнил (невидимих). Зазвичай процес запису здійснюється так: перший шар — наноситься важливий запис невидимими чорнилами, другий шар — запис видимими чорнилами, який нічого не означає.

Текст, записаний такими чорнилами, проявляється лише за певних умов (нагрівання, освітлення, хімічний проявник і т. д.).

Ці чорнила винайдені були ще в I ст. н. е. Філоном Александрійським. Їх використовували як в середньовіччі, так і в новітній час, наприклад, у листах революціонерів з російських в’язниць. Написаний звичайним молоком текст на папері між рядків видимого тексту проявляється під час нагрівання над полум’ям (зазвичай свічки).

Існує також чорнило з хімічно нестабільним пігментом. Написане цими чорнилами виглядає як написане звичайною ручкою, але через певний час нестабільний пігмент розкладається, і від тексту не залишається і сліду. Хоча у разі використання звичайної кулькової ручки текст можливо відновити по деформації паперу, цей недолік можна усунути за допомогою м’якого пишучого вузла, на зразок фломастера.

Симпатичними чорнилами можуть слугувати найрізноманітніші речовини: лимонна кислота, віск, яблучний сік, молоко, сік цибулі, слина, пральний порошок, аспірин, крохмаль з різними хімічними чи фізичними «декодерами»: температура, сода, йод, сіль, залізо, ультрафіолетове світло, для воску навіть крейда чи зубний порошок.

*Комп’ютерна стеганографія.* Напрям класичної стеганографії, заснований на особливостях комп’ютерної платформи. Наприклад, це стеганографічна файлова система StegFS для Linux, приховування даних в невикористовуваних форматів файлів, підміна символів у назвах файлів, текстова стеганографія і так далі. Наведемо деякі приклади:

* Використання зарезервованих полів комп’ютерних форматів файлів. Суть методу полягає в тому, що частина поля розширень, не заповнена інформацією про розширення, за замовчуванням заповнюється нулями. Відповідно ми можемо використовувати цю «нульову» частину для запису своїх даних. Недоліком цього методу є низький ступінь скритності і малий обсяг переданої інформації.
* Метод приховування інформації в невикористовуваних місцях гнучких дисків. Під час використання цього методу інформація записується в невживані частини диска, наприклад, на нульову доріжку. Недоліки: маленька продуктивність, передача невеликих за обсягом повідомлень.
* Метод використання особливих властивостей полів форматів, які не відображаються на екрані. Цей метод ґрунтується на спеціальних «невидимих» полях для отримання виносок, покажчиків. Наприклад, написання чорним шрифтом на чорному тлі. Недоліки: маленька продуктивність, невеликий обсяг переданої інформації.
* Використання особливостей файлових систем — при зберіганні на жорсткому диску файл завжди (не враховуючи деяких ФС, наприклад, ReiserFS) займає кластерів (мінімальних адресуються обсягів інформації). Наприклад, у раніше широко використовуваної файлової системи FAT32 (використовувалася в Windows98/Me/2000) стандартний розмір кластера — 4 Кб. Відповідно для зберігання 1 Кб інформації на диску виділяється 4 Кб інформації, з яких 1Кб потрібен для зберігання файлу, а інші 3 Кб ні на що не використовуються — відповідно їх можна використовувати для зберігання інформації. Недолік цього методу: легкість виявлення.

*Цифрова стеганографія.* Розвиток засобів цифрової обчислювальної техніки дав поштовх для розвитку комп’ютерної стеганографії, яка ґрунтується на вбудовуванні секретного повідомлення в цифрові дані, що, як правило, мають аналогову природу (аудіозаписи, зображення, відео). Можливе також вбудовування інформації в текстові та скомпресовані файли.

Цифрова стеганографія — напрямок класичної стеганографії, заснований на захованні або впровадженні додаткової інформації в цифрові об’єкти, викликаючи при цьому деякі спотворення цих об’єктів. Але, як правило, ці об’єкти є мультимедійними об’єктами (зображення, відео, аудіо, текстури 3D-об’єктів), і внесення спотворень, які знаходяться нижче межі чутливості середньостатистичної людини, не призводить до помітних змін цих об’єктів.

Крім того, в оцифрованих об’єктах, тобто таких, що спочатку мають аналогову природу, завжди наявний шум квантування; також при відтворенні цих об’єктів з’являється додатковий аналоговий шум і нелінійні спотворення апаратури – все це сприяє більшій непомітності прихованої інформації.

*Мережева стеганографія.* Останнім часом популярні методи, коли прихована інформація передається через комп’ютерні мережі з використанням особливостей роботи протоколів передачі даних. Такі методи одержали назву «мережева стеганографія». Цей термін вперше ввів Кжиштоф Шиперський (Krzysztof Szczypiorski) у 2003 р. Типові методи мережевої стеганографії включають зміну властивостей одного з мережевих протоколів. Крім того, може використовуватися взаємозв’язок між двома або більше різними протоколами для більш надійного приховування передачі секретного повідомлення. Мережева стеганографія охоплює широкий спектр методів, зокрема:

* WLAN стеганографія ґрунтується на методах, які використовуються для передачі стеганограм у бездротових локальних мережах (Wireless Local Area Networks). Практичний приклад WLAN стеганографії — система HICCUPS (Hidden Communication System for Corrupted Networks).
* LACK стеганографія — приховування повідомлень під час розмов з використанням IP-телефонії. Наприклад: використання пакетів, що затримуються, або навмисно пошкоджуються та ігноруються приймачем (цей метод називають LACK — Lost Audio Packets Steganography), або приховування інформації в полях заголовка, які не використовуються.
* VoIP (англ. voice over IP) — технологія передачі медіа даних в реальному часі за допомогою сімейства протоколів TCP/IP. IP-телефонія — система зв’язку, при якій аналоговий звуковий сигнал від одного абонента дискретизується (кодується в цифровий вигляд), компресується і пересилається по цифрових каналах зв’язку до іншого абонента, де проводиться зворотна операція — декомпресія, декодування і відтворення. Розмова відбувається у формі аудіопотоків за допомогою протоколів RTP (Real-Time Transport Protocol).
* LACK — це метод стеганографії для IP-телефонії, який модифікує пакети з голосовим потоком. Він використовує те, що в типових мультимедійних комунікаційних протоколах, таких як RTP, надмірно затримані пакети вважаються приймачем марними і відкидаються.

Принцип функціонування LACK полягає у такому: передавач (Аліса) вибирає один з пакетів з голосового потоку і його корисне навантаження замінює бітами таємного повідомлення — стеганограмою, яка вбудовується в пакет. Потім обраний пакет навмисно затримується. Кожного разу, коли надмірно затриманий пакет досягає отримувача, незнайомого з стеганографічною процедурою, він відкидається. Однак якщо отримувач (Боб) знає про прихований зв’язок, то замість видалення отриманих RTP пакетів, він вилучає приховану інформацію.

*Алгоритми.* Існуючі алгоритми вбудовування таємної інформації можна поділити на декілька підгруп:

* працюючі з самим цифровим сигналом. Наприклад, метод LSB (Least Significant Bit);
* «впаювання» прихованої інформації. У цьому разі відбувається накладення приховуваного зображення (звуку, іноді тексту) поверх оригіналу. Часто використовується для вбудовування ЦВЗ (цифровий водяний знак);
* використання особливостей форматів файлів. Сюди можна віднести запис інформації в метадані або в різні інші не використовувані зарезервовані поля файлу.

За способом вбудовування інформації стегоалгоритми можна поділити на лінійні (адитивні: А17, А18, Ь18Б, А21, А25), нелінійні та інші.

*LSB (Least Significant Bit, найменший значущий біт)* — суть цього методу полягає в заміні останніх значущих бітів у контейнері (зображення, аудіо або відеозапису) на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини.

Принцип цього методу полягає в такому: припустимо, є 8-бітне зображення в градаціях сірого. 00h (00000000b) позначає чорний колір, FFh (11111111b) — білий. Усього є 256 градацій. Також припустимо, що повідомлення складається з 1 байта — наприклад, 01101011b. Під час використання 2 бітів в описах пікселів нам буде потрібно 4 пікселі. Припустимо, вони чорного кольору. Тоді пікселі, що містять приховане повідомлення, виглядатимуть так: 00000001 00000010 00000010 00000011. Тоді колір пікселів зміниться: першого — на 1/255, другого і третього — на 2/255 і четвертого — на 3/255. Такі градації не тільки непомітні для людини, а й можуть взагалі не відобразитися при використанні низькоякісних пристроїв виведення. У ролі базового контейнера пропонується використовувати файли BMP-зображень високої роздільності з глибиною кольору 24 та 32 біти, таємне зображення може мати розширення .BMP, .GIF, .PNG, .JPEG.

Недоліком методу LSB є чутливість до розміру зображення, тобто чим менший розмір зображення, тим більше будуть відрізнятися два сусідні пікселі, тому пропонується використовувати зображення з великою роздільністю. Також метод «видає себе» при побітовому перегляді зображення, де чітко видно області зображення, в які «вбудовано» таємну інформацію. Попри це, метод запису Least Sagnificant Bit є досить популярним, стійким та простим під час реалізації.

*Підвиди LSB-алгоритмів для растрових зображень без палітри. BlindHide* (приховування наосліп). Найпростіший алгоритм: дані записують, починаючи з верхнього лівого кута зображення до правого нижнього — піксель за пікселем. Приховані дані програма записує у бітах кольорів пікселя. Приховані дані розподіляються у контейнері нерівномірно. Якщо приховані дані не заповнять повністю контейнер, то лише верхня частина зображення буде засміченою.

*HideSeek* (заховати-знайти). Цей алгоритм у псевдовипадковий спосіб розподіляє приховане повідомлення у контейнері. Для генерації випадкової послідовності використовує пароль. Дещо «розумніший» алгоритм, але все ж не враховує особливостей зображення-контейнера.

*FilterFirst* (попередня фільтрація). Виконує фільтрацію зображення-контейнера — пошук пікселів, у які записуватиметься прихована інформація (для яких зміна розрядів буде найменш помітною для ока людини).

*BattleSteg* (стеганографія морської битви). Найскладніший і найдосконаліший алгоритм. Спочатку виконує фільтрацію зображення-контейнера, після чого прихована інформація записується у «найкращі місця» контейнера у псевдовипадковий спосіб (подібно, як у HideSeek).

Інші методи приховування інформації в графічних файлах орієнтовані на формати файлів з втратою, наприклад, JPEG. На відміну від LSB вони більш стійкі до геометричних перетворень. Це виходить за рахунок варіювання в широкому діапазоні якості зображення, що призводить до неможливості визначення джерела зображення.

*Цифрові водяні знаки (ЦВЗ).* Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканність документа, ідентифікувати автора або власника, перевірити права дистриб’ютора або користувача, навіть якщо файл був оброблений або спотворений.

Цифровий водяний знак (ЦВЗ) — технологія, створена для захисту авторських прав мультимедійних файлів та інтелектуальної власності контейнера (Intellectual Property). Зазвичай цифрові водяні знаки невидимі. Однак ЦВЗ можуть бути видимими на зображенні або відео. Зазвичай ця інформація являє собою текст або логотип, який ідентифікує автора.

Стеганографія застосовує ЦВЗ, коли сторони обмінюються секретними повідомленнями, впровадженими в цифровий сигнал. Використовується як засіб захисту документів з фотографіями — паспортів, водійських посвідчень, кредитних карток з фотографіями. ЦВЗ можна також використовувати для виявлення потенційних піратів: під час продажу в зображення вбудовують інформацію про час продажу та інформацію про покупця.

**ВИСНОВКИ ДО ТРЕТЬОГО ПИТАННЯ**

Ключовою відмінністю ЦВЗ від звичайного приховання інформації є наявність активного противника. Наприклад, використовуючи ЦВЗ для захисту авторського права, активний противник намагатиметься видалити чи змінити вбудовані ЦВЗ. Тому основною вимогою є стійкість вбудованих даних до атак. Таємність не є настільки важливою, як у прихованій комунікації.

**ВИСНОВКИ З ТЕМИ**

Криптографічний захист секретної інформації-вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових Даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.