**міністерство внутрішніх справ УКРАЇНИ**

**ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**

**ВНУТРІШНІХ СПРАВ**

## ***Кафедра економічної та інформаційної безпеки***

### **ЛЕКЦІЇ**

## **з дисципліни**

## **"Управління інформаційною безпекою"**

для здобувачів вищої освіти факультету СПОУ, що навчаються на бакалаврському рівні вищої освіти

Дніпро - 2020

 Лекцію підготував, доцент кафедри економічної та інформаційної безпеки, Гребенюк А.М., канд. техн. наук, доцент

Лекція обговорена та схвалена на засіданні кафедри економічної та інформаційної безпеки

“26” серпня 2020 р.,

протокол № 1

*Тема № 1.* *Основні поняття інформаційної безпеки*

**(2 години)**

ПЛАН ЛЕКЦІЇ

Вступ.

1. Види інформації, що захищається.

2. Міжнародні стандарти інформаційного обміну.

3. Інформаційна безпека в умовах функціонування глобальної мережі.

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдін // Підручник. — К. : НАУ, 2016. — 620 с.

2. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. — Житомир : ЖВІ НАУ, 2018. — 280 с.

3. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник — К. : Вид-во DIRECTLINE, 2019. — 714 с.

4. Семкин С. Н., Семкин А. Н. Основи інформаційної безпеки об'єктів обробки інформації: Науч.-практ. посібник. Орел: 2018г. –300 с.

5. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М: Логос; 2015г. –264с.

**МЕТА ЛЕКЦІЇ**

Актуальність вивчення різних аспектів інформаційної безпеки (ІБ) пов’язана із входженням України в глобалізаційні процеси, в яких постійно зростає значення інформації. По суті, йдеться про становлення інформаційного постіндустріального суспільства, однією з найголовніших ознак якого є перетворення інформації на найцінніший товар і продукт. В інформаційному суспільстві інформаційний вплив на державу, суспільство, громадянина є ефективнішим, ніж політичний, економічний, військовий. Значення інформації зростає в міру зникнення національних кордонів між державами, подолання наслідків інформаційної ізоляції пострадянського суспільства (хоча ці наслідки в багатьох сферах, зокрема науковій, не подолані дотепер). Водночас суспільство не може не турбувати інша проблема − інформаційне перенасичення, надмір недостовірної та шкідливої інформації, не зникає і загроза національній безпеці держави через інформаційне шпигунство, інформаційну агресію іноземних держав тощо.

**Вступ**

На сучасному етапі розвитку суспільства, пов'язаного з масовим використанням інформаційних технологій і створенням єдиного інформаційного простору, в рамкам якого відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми інформаційної безпеки набувають першорядного значення в усіх сферах суспільної і державної діяльності. Особлива гострота і актуальність цих проблем визначається такими факторами: • високими темпами зростання парку засобів обчислювальної техніки і зв'язку, розширенням областей використання комп'ютерів, різноманіттям і повсюдним поширенням інформаційно-керуючих систем, які підлягають захисту;

 • залученням до процесу інформаційної взаємодії все більшого числа людей і організацій, різким зростанням їх інформаційних потреб;

• підвищенням рівня попиту на автоматизовані системи управління і обробки інформації, використанням їх в критичних ситуаціях;

• ставленням до інформації, як до товару, переходом до ринкових відносін з властивою їм конкуренцією і промисловим шпигунством у сфері створення і надання інформаційних послуг;

• концентрацією великих обсягів інформації різного призначення на електронних носіях, вдосконалення доступу до інформаційних ресурсів;

• наявністю інтенсивного обміну інформацією між учасниками процесу;

 • загостренням протиріч між об'єктивно існуючими потребами суспільства в розширенні вільного обміну інформацією і надмірними або навпаки недостатніми обмеженнями на її поширення і використання;

• рівнями втрат (збитків) від знищення, фальсифікації, розголошення або незаконного тиражування інформації;

• різноманіттям видів загроз і можливих каналів несанкціонованого доступу (НСД) до інформації;

• зростанням числа кваліфікованих користувачів обчислювальної техніки і можливостей по створенню ними програмно-математичних впливів на систему;

• відсутністю достатньої кількості кваліфікованих спеціалістів у сфері захисту інформації. Зрозуміло, що в такій ситуації виникає потреба в захисті компʼютерних систем захисту інформації від несанкціонованого доступу, крадіжки, знищення та інших злочинних і небажаних дій, число яких безперервно зростає.

**І. ПИТАННЯ**

В даний час інформаційні системи та інформаційно-телекомунікаційні мережі підтримують сервіси та переносять дані в таких кількостях, які важко було собі уявити ще кілька років тому. Їх готовність необхідна для роботи дуже багатьох інфраструктур, наприклад, комунальні або електричні мережі, органи державного, муніципального та регіонального управління (ДМРУ), організації, населення і т. д. Тому безпека цих систем стає необхідною умовою їх подальшого розвитку. Для кожного випадку визначення безпеки означає специфікацію політики безпеки, тобто безлічі бажаних цілей. Наприклад, електронна система голосування повинна бути встановлена таким чином, щоб голосувати могли тільки зареєстровані виборці, доступ до вебсервера повинен здійснюватися аутентифікованими користувачами, тільки авторизовані користувачі повинні підключатися до банківської системи і т.д. Безпека об'єкта проявляється через безпеку його найбільш важливих властивостей або властивостей структурних складових. Якщо об'єктом безпеки є людина, то його безпека полягає в захищеності від загроз йому, як живому організму, і загроз йому, як носію певних психічних і духовних якостей, тобто особистості. Якщо об'єктом безпеки є суспільство (спільність людей на певній території, яка характеризується економічною і духовною єдністю), то його безпека буде полягати в захищеності від загроз його членів, а також історично склавшимися відносинами між людьми. Відповідно, в змісті національної безпеки розрізняють державну, економічну, суспільну, оборонну, інформаційну, екологічну та іншу безпеку. Державна безпека має своїм об'єктом стан органів ДМРУ, економічна безпека – економіку суспільства, громадська безпека – соціальні інститути, екологічна безпека – навколишнє середовище і людину і т.д. Безпека проявляється як протидія на заданому рівні спробами нанести шкоду функціонуванню або усього обʼєкта захисту, або його структурним складовим. Однією з важливих структурних складовихх багатьох обʼєктів безпеки є інформація (або діяльність, предметом котрої є інформація). 9 1.2. Основні поняття і визначення дисципліни Широко поширене в даний час поняття інформаційна безпека підкреслює важливість інформації в сучасному суспільстві і характеризує той факт, що інформаційний ресурс є сьогодні таким же багатством, як корисні копалини, виробничі і людські ресурси, і також як вони підлягає захисту від різного роду посягань, зловживань і злочинів. Під інформаційною безпекою будемо розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або преднавмисних впливів природного або штучного характеру, чреватих нанесенням шкоди власникам або користувачам інформації і підтримувальної інфраструктури. Підхід до проблем інформаційної безпеки необхідно починати з виявлення суб'єктів, зацікавлених у забезпеченні: • своєчасного доступу (за прийнятний час) до необхідної інформації; • конфіденційності певної частини інформації; • достовірності (повноти, точності, адекватності, цілісності) інформації; • захисту від нав'язування їм неправдивої (недостовірної, перекрученої) інформації (тобто від дезінформації); • захисту частини інформації від незаконного її тиражування (захисту авторських прав, прав власника інформації тощо); • розмежування відповідальності за порушення законних прав (інтересів) інших суб'єктів інформаційних відносин і встановлених правил поводження з інформацією; • можливості здійснення безперервного контролю і управління процесами обробки і передачі інформації. Очевидно, що забезпечення цих вимог суттєво і для держави в цілому, і для окремих громадських (комерційних) організаций, і для підприємств (юридичних осіб), і для окремих громадян (фізичних осіб), які і є суб'єктами інформаційних відносин. Тому введемо наступні визначення. Субʼєкт – це активний компонент інформаційної системи, який може стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи. Обʼєкт – пасивний компонент системи, який зберігає, приймає або передає інформацію. Доступ до об'єкту означає доступ до інформації, яка міститься в ньому. 10 У якості об'єктів, які підлягають захисту в інтересах забезпечення безпеки суб'єктів інформаційних відносин, необхідно розглядати: інформацію і інформаційні ресурси, носії інформації, процеси обробки інформації. Під інформацією розуміють відомості щодо обʼєктів та явищах навколишнього середовища, їх параметрах, властивостей і стану, які зменшують ступень невизначеності. Основними властивостями якості інформації з позиції користувача є: репрезентативность, змістовність, достатність, доступність, актуальність, своєчасність, точність, достовірність і сталість. Інформаційні ресурси – це окремі документи та масиви документів, представлені самостійно або в інформаційних системах (бібліотеках, архівах, фондах, базах даних та інших ІС). Інформаційні ресурси можна класифікувати: - за видом інформації – правові, науково-технічні, політичні, фінансовоекономічні, статистичні, метрологічні, соціальні, персональні, медичні, про надзвичайні ситуації та т.п.; - за режимом доступу – відкриті, обмеженого доступу, державна таємниця, конфіденційна інформація, комерційна таємниця, професійна таємниця, службова таємниця, особиста (персональна) таємниця; - за формою власності – державні, муніципальні, регіональні, приватні, колективні; - за видом носія – на папері (документи, листи, медичні карти, телефонні довідники організацій, чернетки і т.п.), на екрані, в пам'яті ЕОМ, в каналі зв'язку, на гнучких і жорстких магнітних дисках, на інших носіях. Носіями інформації можуть бути окремі люди, які володіють важливою інформацією (експерти), а також спеціально завербовані або випадкові інформатори. Поінформованість кінцевого користувача про заходи безпеки повинна проявлятися в умінні розрізняти 4 рівні захисту комп'ютерних та інформаційних ресурсів: - запобігання – доступ до інформації та технологій має тільки авторизований персонал; - виявлення – зловживання стають відомими ще на ранній стадії, навіть у разі обходу механізмів захисту; 11 - обмеження – зменшення розміру втрат, якщо злочин мав місце, незважаючи на вжиті заходи щодо його запобігання; - відновлення – забезпечення ефективного відновлення інформації при наявності документованих і перевірених планів проведення цієї операції. Далі надані основні поняття щодо інформаційної безпеки компʼютерних систем (КС). Під безпекою КС розуміють її захищеність від випадкового або навмисного втручання в нормальний процес її функціонування, а також від спроб розкрадання, зміни або руйнування її компонентів. Природа впливів на КС може бути найрізноманітнішою. Це і стихійні лиха (землетруси, урагани, пожежі), і вихід з ладу складових елементів КС, і помилки персоналу, і спроба проникнення зловмисника. Безпека КС досягається вживанням заходів щодо забезпечення конфіденціальності і цілісності оброблюваної нею інформації, а також доступності та цілісності компонентів і ресурсів системи. Під доступом до інформації розуміється ознайомлення з інформацією, її обробка, зокрема копіювання, модифікація або знищення інформації. Розрізняють санкціонований і несанкціонований доступ до інформації. Санкціонований доступ до інформації – це доступ до інформації, що не порушує встановлені правила розмежування доступу. Ці правила служать для регламентації права суб'єктів на доступ до об'єктів. Несанкціонований доступ (НСД) до інформації характеризується порушенням встановлених правил розмежування доступу. Це найбільш поширений вид комп'ютерних порушень. Конфіденційність даних – це статус, наданий даними і визначає необхідний ступінь їх захисту. За суттю конфіденційність інформації – це властивість інформації бути відомою тільки допущеним особам (авторизованим суб'єктам системи). Для інших суб'єктів системи ця інформація повинна бути невідомою. Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в семантичному відношенні від даних у вихідних документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування. 12 Цілісність компонента або ресурсу системи – це властивість компонента чи ресурсу бути незмінними в семантичному сенсі при функціонуванні системи в умовах випадкових або навмисних спотворень або руйнівних впливів. Доступність компонента або ресурсу системи – це властивість компонента чи ресурсу бути доступним для авторизованих законних субʼєктів системи. Метою захисту систем обробки інформації є протидія загрозам безпеки. Під загрозою безпеки КС розуміють можливі дії, які прямо або побічно можуть завдати шкоди її безпеки. Збиток безпеки має на увазі порушення стану захищеності інформації, що міститься і обробляється в КС. З поняттям загрози безпеки тісно пов'язане поняття уразливості КС. Комплекс засобів захисту являє собою сукупність програмних і технічних інструментів, що створюються і підтримуються для забезпечення інформаційної безпеки КС. Комплекс створюється і підтримується відповідно до прийнятої в даній організації політики безпеки. Політика безпеки – це сукупність норм, правил і практичних рекомендацій для надійної роботи засобів захисту КС від безлічі загроз. На практиці найважливішими є наступні аспекти информационої безпеки: доступність, цілісність і конфіденційність.

**ІІ. ПИТАННЯ**

Електронний обмін даними — це міжкомп'ютерний обмін діловими, комерційними та фінансовими електронними документами, наприклад, замовленнями, платіжними інструкціями, контрактними пропозиціями, накладними, квитанціями.

Такий обмін даними забезпечує оперативну взаємодію торговельних партнерів (клієнтів, постачальників, торговельних посередників, експедиторів та ін.) на всіх етапах підготовки торговельної угоди, укладення контракту і реалізації постачання.

На етапі оплати контракту і переказу грошових коштів електронний обмін даними для комерційних цілей може взаємодіяти зі службою електронного обміну фінансовими документами. Така взаємодія створює для покупців (клієнтів) ефективне середовище під час виконання всіх торговельно-платіжних операцій, а саме:

* он-лайн-перегляд каталогів торговельних пропозицій, товарів і послуг на ринку;
* вибір в інтерактивному режимі потрібного товару/послуги, уточнення умов (вартості й термінів постачання, торговельних знижок, гарантійних і сервісних зобов'язань);
* он-лайн-замовлення товару/послуги або запит контрактної пропозиції, погодження й укладення контракту;
* оперативний контроль постачання товару;
* одержання за допомогою електронної пошти супровідних документів (накладних, фактур, комплектуючих відомостей та ін.);
* підтвердження завершення постачання товару/послуги, виставлення й оплата рахунків;
* виконання банківсько-кредитних і платіжних операцій.

Виконуючи ці операції, користувачі служби електронного обміну даними мають використовувати відповідне телекомунікаційне обладнання, програмне забезпечення та канали зв'язку.

Історія виникнення і розвитку електронного обміну даними починається у 60-х роках, коли несумісність окремих фірмових технологій обробки комерційних даних не давала змоги інтегрувати їх в єдину систему, яка б забезпечила комплексну автоматизацію міжнародних торговельних операцій.

Так, якщо дві компанії використовують національні стандарти для подання електронних документів, то під час обміну інформацією їм буде потрібне подвійне перетворення форматів повідомлень (рис. 1).

Стандарт 1 1

Стандарт 2 1

Рис. 1 Схема перетворення форматів для двох підприємств у різних країнах

У разі збільшення кількості партнерів, які беруть участь в інформаційній взаємодії, кількість перетворень зростає.

У 1983—1985 pp. міжнародні організації ООН (UN/ЕСЕ та ISO) почали розробку процедур, форматів даних і міжнародних кодових систем для електронного обміну даними. У 1988 р. оприлюднено першу версію міжнародного стандарту United National Electronic Data Interchange for Administration, Commerce and Transport — UN/EDIFACT (ООН / Електронний обмін даними для адміністрації, торгівлі і транспорту).

EDIFACT виокремлено чотири основні компоненти, які підлягають стандартизації під час підготовки документів для передачі каналами телекомунікацій:

* елементи даних (data elements);
* стандартні групи елементів даних (standard data segments);
* стандартні повідомлення (standard message);
* правила створення форматів документів (syntax rules).

Таким чином, розроблено набір синтаксичних правил і комерційних елементів, який отримав назву EDIFACT і був оформлений у вигляді двох стандартів ISO:

* ISO 7372 — Trade Data Elements Directory (Довідник комерційних елементів даних);
* ISO 9735 — Application Level Syntax Rules (Правила синтаксису на рівні користувача).

Стандарти EDIFACT розроблялись для глобальних комп'ютерних мереж з широким колом користувачів: державних установ, виробників товарів, виробів і послуг, дистриб'юторів, брокерів, транспортних експедиторів, банків, страхових компаній та ін. По суті вони є універсальною мовою електронного спілкування на міжнародному рівні, тобто лінгвістичним забезпеченням для інформаційних систем у міжнародному бізнесі.

Головними цілями створення і використання EDIFACT визнано:

* визначення стандартних щодо синтаксису і семантики повідомлень, які відповідають міжнародним стандартам;
* заміну звичайних паперових форм і документів електронними документами та відповідними методами їх обробки;
* прискорення документообігу і відповідно оперативності обробки комерційних і фінансових трансакцій;
* створення для малих, середніх і великих фірм більш сприятливих і рівних умов ринкової конкуренції;
* покращання умов для підготовки і здійснення торговельних угод;
* більш широке та масове використання клієнтами сучасних комп'ютерних мереж і послуг.

На базі стандарту EDIFACT інтенсивно розвивається інфраструктура електронного обміну даними. Інформаційні й телекомунікаційні системи забезпечують для своїх користувачів комплекс послуг з обробки і видачі довідкових даних, комерційних звітів, замовлень і торговельних пропозицій, розрахунків і платіжних квитанцій.

Усі ці послуги надаються як прикладні служби, які створюються технологіями електронного обміну даними. На сучасному етапі розрізняють такі основні види прикладних служб.

1. Онлайнові бази даних — бази даних, які доступні в оперативному режимі з терміналів користувачів. Онлайнові бази даних цілодобово відкриті для діалогового пошуку інформації і видачі довідок та різних статистичних звітів. Користувачами онлайнових баз даних можуть бути спеціалісти комерційних і фінансових організацій, економісти, дилери, постачальники, агенти фінансових і торговельних організацій.

2. Електронна пошта — система обміну й обробки повідомлень (сукупність електронних поштових скриньок, програмних засобів обробки, збереження і передачі повідомлень, термінальних станцій для підготовки і виведення повідомлень). Користувачі електронної пошти можуть проводити міжперсональний обмін повідомленнями, розсилання повідомлення за списками адрес, зажадати свої повідомлення з поштових скриньок, організувати проблемні телеконференції і виконувати інші функції обробки повідомлень (електронних документів).

3. Електронна передача грошових коштів (EFT - Electronic Funds Transfer) - система передачі фінансових (кредитних, платіжних) документів між клієнтами і банками, між банками між банками та іншими фінансовими і комерційними організаціями. Міжнародна мережа обміну фінансовою інформацією SWIFT забезпечує багато функцій EFT.

4. Електронний обмін даними (EDI -- Electronic Data Interchange) — багатоцільова система обміну документами, які мають розвинуту структуру даних. Як правило, реалізується на базі стандартних програмних і технічних засобів електронної пошти.

Керівні мережні служби (Managed Network Services) виконують різні виробничі, адміністративні та службові функції управління об'єктами, технологічними лініями, транспортними системами і службовцями підприємств. Реалізуються на базі внутрішньофірмових мереж ЕОМ, розподілених між підрозділами фірми.

Телеметричні служби — система оперативного спостереження, дистанційного виміру і контролю за нерухомими та рухомими об'єктами.

Бізнесмени, торговельні агенти, транспортні службовці, банківські спеціалісти, адміністратори, економісти і бухгалтери переважно використовують перші чотири служби електронного обміну даними.

На сучасному етапі електронний обмін даними діє або впроваджується практично в усіх країнах. Міжнародний статус стандарту EDIFACT спонукає до того, що його використання є обов'язковою умовою адекватного обміну даними із закордонними партнерами для всіх без винятку підприємств і організацій України, які здійснюють зовнішньоекономічну діяльність.

*Міжнародний стандарт електронного обміну даними EANCOM*

Стандарт EANCOM є практичним підстандартом стандарту UN/EDIFACT і нині вже прийнятий як національний і міжнародний майже в 50 країнах світу.

Характерна особливість EANCOM у тому, що він є однією зі складових всеохопного пакета міжнародних стандартів для ідентифікації товарів, послуг і розташування, автоматизованої ідентифікації на основі штрихових кодів та електронного обміну даними EAN (Electronic Data Interchange), у комбінації з якими забезпечує засоби для побудови ефективної системи створення, передачі й обробки інформації на основі автоматизованої ідентифікації.

Стандарт EANCOM доступний для організацій будь-яких розмірів, необхідно лише мати комп'ютер, телефонну лінію, модем і конвертор (спеціальне програмне забезпечення).

Електронний обмін даними в найближчому майбутньому, очевидно, стане єдиною можливою формою господарської діяльності, оскільки участь і конкурентоспроможність на ринку буде неможливою без автоматизованого подання інформації і негайної відповіді на потреби клієнтів.

**ІІІ. ПИТАННЯ**

Інформаційна безпека складається з багатьох компонентів. Вона залежить і від рівня забезпечення свободи слова в державі, і від захищеності громадян від впливу на їх світосприйняття, психічне та фізичне здоров’я таких негативних чинників, як пропаганда жорстокості, насильства, і від наявності у органів влади достатньої інформації для прийняття відповідних рішень.

В цьому процесі надзвичайно велика питома вага саме інформаційного впливу як на людину, так і на все те, що відбувається в колективі людей, в суспільстві, у державі. У сучасному комп’ютерному суспільстві атаки на інформацію стали буденною практикою. Повідомлення про атаки “хакерів” і комп’ютерні злами заповнили всі засоби масової інформації. З масовим впровадженням комп’ютерів у всі сфери діяльності людини об’єм інформації, що зберігається в електронному вигляді, виріс в тисячі разів. І тепер скопіювати за півхвилини і винести носій з файлом, що містить план випуску продукції, набагато простіше, ніж копіювати або переписувати безліч паперів. А з появою комп’ютерних мереж навіть відсутність фізичного доступу до комп’ютера перестала бути гарантією збереження інформації. Прикладів підміни, “зламу”, втручання у конфіденційну інформацію можна навести безліч.

По повідомленню IBM, кіберзлочинці, атакуючи веб-браузери, які призначені для користувача комп’ютерів, здійснюють розкрадання конфіденційної персональної інформації, що ідентифікує особу користувачів, в небачених раніше масштабах. Результати дослідження IBM свідчать, що витончені атаки з боку кримінального співтовариства все частіше направлені на отримання незаконних прибутків від “експлуатації” вразливостей Веб ресурсів. Посібники кіберзлочинців надають їм інструментарій для маскування атак на веб-браузери, що допомагає уникнути виявлення таких атак системами інформаційної безпеки. Завдяки техніці атак кіберзлочинці можуть проникнути в систему користувача і отримати доступ до особистої інформації, такої як: номери страховок і ідентифікаційних документів, дані кредитних карт і таке інше. Атакуючи корпоративний комп’ютер, зловмисники можуть отримати доступ до важливої комерційної інформації і використовувати заражений комп’ютер, щоб обійти захист брандмауера. В законі також визначено гарантію прав споживачів, особливо що стосується безпеки інформаційних послуг: постачальник інформаційної послуги повинен вживати відповідних технічних та організаційних заходів для гарантування безпеки своїх послуг, захисту інформації, запобігання несанкціонованого доступу до телекомунікацій відповідно до вимог законодавства про захист інформації в автоматизованих системах. Постачальник несе відповідальність за надання інформаційної послуги, яка містить заборонену до поширення інформацію, відповідно до законодавства. Тому вже сьогодні необхідним є відповідна координація зусиль щодо забезпечення протидії цьому виду правопорушень. Не менш важливою проблемою забезпечення інформаційної безпеки користувачів є небажання людей вірити в те, що з ними щось може трапитися – до тих пір поки це не трапиться. Насправді неприємності трапляються значно частіше ніж думають більшість користувачів. Незалежно від того яким способом і з якої причини була здійснена атака на комп’ютерну систему, відновлення займе багато часу і сил. Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні і організаційно-економічні методи. Правові методи – передбачають розробку комплексу нормативно-правових актів і положень, які регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки. Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно вимогам інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах. Програмно-технічні методи – це сукупність засобів для: запобігання витоку інформації; виключення можливості несанкціонованого доступу до інформації; запобігання впливам, які призводять до знищення, руйнування, спотворення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації; виявлення прикладних пристроїв; виключення перехоплення інформації технічними засобами; використання криптографічних засобів захисту інформації при передачі по каналах зв’язку. При вивченні проблеми інформаційної безпеки, нами було розроблено ряд корисних порад користувачам мережі Інтернет, які варто знати. Отож для захисту себе від несанкціонованого втручання потрібно знати та використовувати необхідні програми захисту такі як: брандмауери (фаєрволи), та антивірусні програми. При використанні електронної пошти потрібно: Уважніше відкривати підозрілі листи електронної пошти, або ж не відкривати їх взагалі; Використовувати фільтр спаму програми електронної пошти; При запитах в Інтернеті користуватися додатковою електронною поштою; Не пересилати “ланцюгові” повідомлення електронної пошти. Видаляти їх одразу після надходження. В мережі Інтернет потрібно бути дуже обачним та закривати сумнівні спливаючі вікна та не допускати того, щоб вас ошукали;

Серія “Культура і соціальні комунікації” завжди оновлювати операційну систему; робити резервні копії важливих файлів; дотримуватися правил та законів навіть в Інтернеті. Хоча більшість законів було створено до того, як Інтернет набув широкого розповсюдження, дія законів розповсюджується і на Інтернет. Все, що є незаконним у повсякденному житті, є незаконним і в он-лайні; Варто також пам’ятати, що при розміщенні інформації в Інтернеті, втрачається контроль над нею; не рекомендується зберігати особисту інформацію у веб-браузері та інших програмах, з’єднаних із Інтернетом. Це найголовніші правила, яких так чи інакше варто дотримуватись задля забезпечення захисту конфіденційної інформації, що стосується як користувача особисто, так і інформації для роботи. Підсумувавши все вище зазначене слід сказати, що на даному етапі розвитку інформаційних технологій, існує загроза забезпечення інформаційної безпеки користувачів мережі Інтернет. Для реалізації цього комплексного завдання державі необхідно відшукати динамічний баланс між свободою слова, забезпеченням права на інформацію, ефективним використанням її як засобу контролю громадянського суспільства за діями влади, обмеженням поширення таємної інформації та підтриманням моральної і духовної стабільності у суспільстві. Знаходження цього балансу дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної і якісної інформації. Це завдання передбачає здійснення гнучкої і активної державної політики у питаннях циркуляції інформації, доступу до неї, діяльності засобів масової інформації, розвитку видавничої справи, освіти і масової культури. Найкраще забезпечити інформаційну безпеку українська держава зможе, якщо створить умови для всебічного розвитку інститутів громадянського суспільства, закладів освіти і культури, засобів масової інформації. Державна політика має передбачати системну превентивну діяльність органів влади з надання гарантій інформаційної безпеки особі, суспільним групам та суспільству в цілому. Взагалі, доцільно законодавчо визначити інформаційну безпеку України як комплекс системних превентивних заходів із наданням гарантій захисту життєво важливих інтересів особистості, суспільству й державі від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз. Та не менш важливим є поінформованість користувачів, із загрозами які чекають їх на кожному кроці. Ступінь обізнаності користувачів у сучасній ситуації представлених загроз – запорука якісній роботі, та необхідному захисту, в таких важливих, на сьогоднішній день реаліях.

Не можна відкидати і переваги, що створюються завдяки більш вільному та швидкому переміщенню інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції. Одна з таких переваг полягає в тому, що гарна поінформованість розвиває громадянські якості, що сприяє інтенсифікації розвитку громадянського суспільства в різних країнах і регіонах світу. «Громадяни «цифрового світу» не відчужені ні від інших людей, ні від громадських інститутів. Для них не характерне неуцтво стосовно того, як функціонує наша система, чи байдужість до соціальних і політичних питань, із якими зіштовхується суспільство. Навпаки, онлайновий світ охоплює багатьох із найбільш інформованих і політично активних громадян, яких ми мали будь-коли чи хотіли б мати». В Україні також необхідно повноцінно використати «громадянський» ресурс глобальної інформаційної цивілізації. Такий ресурс може бути дуже корисний при реалізації різноманітних громадянсько-просвітницьких та освітніх проектів. Окрім того, саме розвиток громадянських якостей людей, однією з яких є вміння фільтрувати складні інформаційні потоки, може стати в пригоді при протидії ризикам інформаційних впливів і агресивних дій. У той же час, на фоні активізації громадянської активності, що відбувається завдяки простішому переміщенню інформації, створюється передумови і для значних негативних ефектів, одним з яких є загроза втрати національно-культурної ідентифікації. Користуючись новітніми інформаційними технологіями, людина отримує безліч можливостей занурюватися в глобальне середовище цінностей і смислів, що повністю втратили національно-культурне коріння. «Фахівці, вивчаючи проблеми сучасних відносин, дійшли висновку, що користувачі Інтернету становлять модернізовану групу, яка за своїми соціокультурними характеристиками значно ближча до представників інших культур у глобальному інформаційному просторі, ніж до українського населення, не охопленого Інтернетом» [10, 38]. Таким чином, важливо в будь-якому аспекті дослідження проблематики інформаційної безпеки звертати увагу на такий подвійний вплив інформаційної революції, коли люди, отримуючи нові корисні можливості, втрачають важливий зв’язок з традиціями, що визначають їх національну, суспільно-групову, особистіснодуховну ідентичність. Таким чином, в аспекті переваг та ризиків переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції, проблематика інформаційної безпеки має розглядатися в якості концептуального ядра, навколо Філософія 93 якого вибудовується вся система сучасних соціальних, економічних, політичних, національно-безпекових відносин. «Інформаційна безпека вже набуває того структуроутворюючого компонента, на якому будується вся система національної безпеки держави. Адже в інформаційному суспільстві канали, мережі і системи інформації та комунікації стають, так би мовити, і нервовою, і серцево-судинною системою суспільства водночас. Розробка та поширення інформаційних засобів впливу та мирні моменти співіснування відбуваються одночасно у межах інформаційної протидії. Збереження стану рівноваги у стосунках, скоріше за все, і буде визначником інформаційної безпеки». Таким чином, в умовах глобального характеру сучасних безпекових механізмів неможливо виносити інформаційну безпеку людини, соціуму, держави за межі глобальних тенденцій. Тим більше, що ті суб’єкти, які готують інформаційні загрози, операції, війни, повноцінно використовують глобальний характер сучасного інформаційного середовища, застосовуючи всі можливі інформаційно-технологічні та психологічні можливості впливу.

Таким чином, важливо розуміти, що всі переваги та ризики переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції, безпосередньо пов’язані між собою. Щоб скористатися перевагами, яких дійсно багато, необхідно вибудовувати таку систему інформаційної безпеки, яка б дозволила максимально нівелювати всі можливі ризики, реальні загрози та суперечності.

**ВИСНОВКИ**

Всучасних умовах спостерігається поступовий вихід на міжнародний рівень підходів і заходів щодо забезпечення інформаційної безпеки у цивільних і військових сферах. МСІБ, що формується, включає наступні елементи: міжнародні доктринальні документи універсального характеру, присвячені інформатизації, інформаційному суспільству та інформаційній безпеці; міжнародні стандарти інформаційної безпеки; міжнародні професійні установи, які займаються питаннями інформаційної безпеки; міжнародно-регіональні інститути та структури, які створюються інтеграційними об’єднаннями; інститути, які створюються військо-політичними організаціями; національні доктрини, концепції та стратегії. У перспективних дослідженнях планується дослідити політику національних і міжнародних компаній у сфері інформаційної безпеки.

***Тема № 2. Загрози інформаційної безпеки в інформаційних системах.***

(2 години)

ПЛАН ЛЕКЦІЇ

Вступ.

1. Основні нормативно-правові акти у галузі інформаційної безпеки. Правові особливості забезпечення безпеки конфіденційної інформації та державної таємниці.

2. Призначення і завдання в сфері забезпечення інформаційної безпеки на рівні держав.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Конституція України від 28.06.1996 за №254к/96-ВР.
2. Закон України «Про інформацію» від 02.10.1992 за № 2657-XII.
3. Закон України «Про доступ до публічної інформації» від 13.01.2011 за № 2939-VI.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 за № 2594-IV.
5. Закон України «Про захист персональних даних» від 01.06.2010 за № 2297-VI.
6. Закон України «Про захист інформації в автоматизованих системах» від 5.07.1994 за № 80/94-ВР.
7. Інформаційне забезпечення професійної діяльності : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти факультету економіко-правової безпеки, що навчаються на бакалаврському рівні вищої освіти, основ функціонування та основних вимог системи інформаційного забезпечення України.

Формування у студентів знань основних видів інформаційних загроз та вміння впроваджувати новітні методи і заходи та побудову ефективної технології захисту інформації. Використовувати основні теоретичні положення і методи, формування умінь і прищеплення навичок застосування теоретичних знань для вирішення прикладних завдань, а також розвиток нових підходів до забезпечення інформаційної безпеки в сфері економіки. Використовувати комплексу нормативно-правових актів, що регулюють діяльність людей.

Основними завданнями вивчення навчальної дисципліни «Сучасні інформаційні технології захисту даних» є:

- вивчення теоретичних основ створення і використання сучасних інформаційних технологій;

- знань про сучасні тенденції загроз інформаційній безпеці, про нормативні правові документи щодо захисту інформації, а так само про сучасні методи захисту даних.

- засобах забезпечення інформаційної безпеки в контексті економічних інформаційних систем;

**ВСТУП**

Перехід до ринкових відносин в економіці і науково-технічний прогрес надзвичайно прискорили темпи впровадження в усі сфери соціально-економічного життя українського суспільства останніх досягнень в області інформатизації. Термін «інформатизація» уперше з'явився при створенні локальних багатотермінальних інформаційно-обчислювальних систем і мереж масового обслуговування. Сучасні інформаційні технологій знаходяться у всіх аспектах людської діяльності, що дозволяє підвищити ефективності суспільної праці.

Протягом останніх років в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій – закон України “Про інформацію” від 02.10.92р. Відомості Верховної Ради УРСР. – 1992. – № 48. ст. 650. Розвиток і широке застосування електронної обчислювальної техніки в промисловості, управлінні, зв'язку, наукових дослідженнях, освіті, сфері послуг, комерційної, фінансовій і інших сферах людської діяльності є в даний час пріоритетним напрямком науково-технічного прогресу. Ефект, який досягається за рахунок застосування обчислювальної техніки, зростає при збільшенні масштабів обробки інформації, тобто концентрації по можливості великих обсягів даних і процесів їх обробки в рамках однієї технічної системи, включаючи територіально розосереджені обчислювальні мережі і автономну систему управління. Масштаби і сфери застосування цієї техніки стали такими, що поряд з проблемами надійності та стійкості її функціонування виникає проблема забезпечення безпеки циркулюючої в ній інформації. Безпека інформації - це здатність системи її обробки забезпечити в заданий проміжок часу можливість виконання заданих вимог по величині ймовірності настання подій, виникаючих в результаті виток інформації, модифікації або втрати даних, що представляють ту чи іншу цінність для їх власника. При цьому вважається, що причиною цих подій можуть бути випадкові впливи або впливи в зв'язку з навмисним несанкціонованим доступом людини-порушника.

Заходи безпеки спрямовані на запобігання несанкціонованого отримання інформації, фізичного знищення або модифікації інформації, що захищається.

Зарубіжні публікації останніх років показують, що зловживання інформацією, яка передається по каналах зв'язку, удосконалювалися не менше інтенсивною, ніж засоби їх попередження. В цьому випадку для захисту інформації потрібно не просто розробка приватних механізмів захисту, а організація цілого комплексу заходів, тобто використання спеціальних засобів, методів і заходів з метою запобігання втрати інформації. Сьогодні народжується нова сучасна технологія - технологія захисту інформації в комп'ютерних інформаційних системах і в мережах передачі даних.

**І. ПИТАННЯ**

**В законі України “Про інформацію” від 02.10.92р.** Відомості Верховної Ради УРСР. – 1992. – № 48. ст. 650. Визначаються основні терміни та положення про інформацію, регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації

Терміни:

**документ** - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

**захист інформації** - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

**інформація** - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

суб'єкт владних повноважень - орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Основними принципами інформаційних відносин є:

* гарантованість права на інформацію;
* відкритість, доступність інформації, свобода обміну інформацією;
* достовірність і повнота інформації;
* свобода вираження поглядів і переконань;
* правомірність одержання, використання, поширення, зберігання та захисту інформації;
* захищеність особи від втручання в її особисте та сімейне життя.

**Основними напрямами державної інформаційної політики є:**

* забезпечення доступу кожного до інформації;
* забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
* створення умов для формування в Україні інформаційного суспільства;
* забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
* створення інформаційних систем і мереж інформації, розвиток електронного урядування;
* постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
* забезпечення інформаційної безпеки України;
* сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

За змістом інформація поділяється на такі види:

**Інформація про фізичну особу** (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

**Інформація довідково-енциклопедичного характеру** - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

**Інформація про стан довкілля** (екологічна інформація) - відомості та/або дані про:

стан складових довкілля та його компоненти, фактори, що впливають або можуть впливати на складові довкілля, стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути,

**Інформація про товар** (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару про вплив товару (роботи, послуги) на життя та здоров'я людини. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України

**Науково-технічна інформація** - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Правовий режим науково-технічної інформації визначається [Законом України](https://zakon.rada.gov.ua/laws/show/3322-12) "Про науково-технічну інформацію", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

**Податкова інформація** - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому [Податковим кодексом України](https://zakon.rada.gov.ua/laws/show/2755-17).

**Правова інформація** - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо. Джерелами правової інформації є [Конституція України](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80), інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

**Статистична інформація** - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства. Правовий режим державної статистичної інформації визначається [Законом України](https://zakon.rada.gov.ua/laws/show/2614-12) "Про державну статистику", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

**Соціологічна інформація** - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

**Доступ до інформації** – поділяється на відкриту інформацію та інформацію з обмеженим доступом.

1. ***Інформацією з обмеженим доступом*** є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

**ВИСНОВКИ З першого ПИТАННЯ:**

В першому питанні лекції ми розглянули основні нормативно-правові аспекти які регулюють інформаційний обмін в мережах. Джерелами правової інформації є [Конституція України](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80), інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

**ІІ. ПИТАННЯ**

Згідно з визначенням інформаційної безпеки, вона залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електро-, водо- - і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою запропонованих їй функцій.

**Закон України Про захист інформації в інформаційно-телекомунікаційних системах (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286)**

У цьому Законі наведені нижче терміни вживаються в такому значенні:

* **блокування інформації в системі** - дії, внаслідок яких унеможливлюється доступ до інформації в системі;
* **виток інформації** - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;
* **володілець інформації** - фізична або юридична особа, якій належать права на інформацію;
* **власник системи** - фізична або юридична особа, якій належить право власності на систему;
* **доступ до інформації в системі** - отримання користувачем можливості обробляти інформацію в системі;
* **захист інформації в системі** - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;
* **знищення інформації в системі** - дії, внаслідок яких інформація в системі зникає;
* **інформаційна** (автоматизована) **система** - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;
* **інформаційно-телекомунікаційна система** - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;
* **комплексна система захисту інформації** - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;
* **користувач інформації в системі** (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;
* **криптографічний захист інформації** - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;
* **несанкціоновані дії щодо інформації в системі** - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;
* **обробка інформації в системі** - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;
* **порушення цілісності інформації в системі** - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;
* **порядок доступу до інформації в системі** - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;
* **телекомунікаційна система** - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;
* **– технічний захист інформації** - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

**Відповідальність за забезпечення захисту інформації в системі** покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

[**Вимоги**](https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF)до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

* розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;
* визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
* організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;
* здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
* здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

За законом особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

**ВИСНОВКИ З ДРУГОГО ПИТАННЯ:**

В першому питанні лекції ми розглянули стратегію розвитку системи інформаційного забезпечення в Україні, основні закони які регламентують інформаційну діяльність в країні.

***ТЕМА 3.******Стандарти управління інформаційною безпекою***

**(2 години)**

**ПЛАН ЛЕКЦІЇ:**

1. Основні стандарти в галузі забезпечення інформаційної безпеки. Політика безпеки.
2. Загальна характеристика систем захисту в інформаційних мережах.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Інформаційне забезпечення професійної діяльності : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.
2. Информационные технологии и защита информации в информационнокоммуникационных системах: монография / под ред. В.С. Пономаренко. – Х. : вид. тов “Щедра садиба плюс”, 2015. – 486 с., русск. яз. ISBN 978-617-7225-03-3
3. Н.Е. Березюк., А.Г.Андрущенко и др. Кодирование информации. Харьков, Висшая школа, 2016.
4. Гундарь К.Ю. , Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерних системах - К:"Корнійчук" 2017.
5. В.В.Домарев. Защита информации и безопасность комьютерних систем - К. издательство Диасофт, 2019.

**МЕТА ЛЕКЦІЇ**

Несанкціоноване використання інформаційних ресурсів, з одного боку, є засобом розкриття або компрометації інформації, а з іншого має самостійне значення, оскільки, навіть не торкаючись користувацької або системної інформації, може завдати певної шкоди абонентам і адміністрації. Цей збиток може варіюватися в досить широких межах від скорочення надходження фінансових коштів до повного виходу автоматизованих інформаційних ресурсів з ладу.

Помилкове використання інформаційних ресурсів будучи санкціонованим тим не менш може привести до руйнування, розкриття або компрометації вказаних ресурсів. Дана загроза найчастіше є наслідком помилок, наявних в програмному забезпеченні автоматизованих інформаційних ресурсів.

Несанкціонований обмін інформацією між абонентами може призвести до отримання одним з них відомостей, доступ до яких йому заборонений, що за своїми наслідками рівносильно розкриттю змісту банківської інформації.

**І. ПИТАННЯ**

Витік інформації полягає в розкритті будь-якої таємниці: державної, військової, службової, комерційної або особистої.

Захисту повинна підлягати не тільки секретна інформація. Модифікація несекретних даних може привести до витоку секретних або до не виявлення одержувачем прийому помилкових даних. Руйнування або зникнення накопичених з великими труднощами даних може призвести до непоправної їх втрати. Фахівцями розглядаються і інші ситуації порушення безпеки інформації, але всі вони за своєю суттю можуть бути зведені до перерахованих вище подій. Залежно від сфери і масштабів застосування тієї чи іншої системи обробки даних втрата або витік інформації може призвести до різної тяжкості наслідків: від невинних жартів до виключно великих втрат економічного і політичного характеру.

У пресі і технічній літературі наводиться маса подібних прикладів. Особливо широкий розмах отримали злочини в автоматизованих системах, обслуговуючих банківські і торгові структури. За зарубіжними даними, втрати в банках в результаті комп'ютерних злочинів щорічно складають від 170 млн. до 41 млрд. доларів.

Попри всі дорогі методи захисту, функціонування комп'ютерних інформаційних систем виявило слабкі місця в захисті інформації. Як наслідок постійно збільшуються витрати і зусилля на захист інформації. Однак для того, щоб вжиті заходи виявилися ефективними, необхідно визначити, що таке загроза безпеці інформації, виявити можливі канали витоку інформації та шляхи несанкціонованого доступу до захищених даних.

Таким чином, в даний час благополуччя і навіть життя багатьох людей залежать від забезпечення інформаційної безпеки безлічі комп'ютерних систем обробки інформації, а також контролю і управління різними об'єктами.

До таких об'єктів (їх називають критичними) можна віднести системи телекомунікацій, банківські системи, атомні станції, системи управління електропостачанням, системи управління повітряним і наземним транспортом, а також системи обробки і зберігання секретної та конфіденційної інформації. Для нормального і безпечного функціонування цих систем необхідно підтримувати їх безпеку і цілісність.

Під **загрозою безпеки інформації** розуміється дія або подія, яка може привести до руйнування, спотворення чи несанкціонованого використання інформаційних ресурсів, включаючи збережену, передану і оброблювану інформацію, а також програмні і апаратні засоби.

Загрози прийнято ділити на випадкові, чи ненавмисні, і навмисні. Джерелом перших можуть бути помилки в програмному забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації і т.п. Умисні загрози, на відміну від випадкових, мають на меті нанесення шкоди користувачам автоматизованих інформаційних технологій і, в свою чергу, поділяються на активні і пасивні.

***Пасивні*** загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів, не надаючи при цьому впливу на її функціонування. Пасивної загрозою є, наприклад, спроба отримання інформації, що циркулює в каналах, за допомогою їх прослуховування.

***Активні*** загрози мають на меті порушення нормального процесу функціонування за допомогою цілеспрямованого впливу на апаратні, програмні та інформаційні ресурси. До активних загроз відносяться, наприклад, руйнування або радіоелектронне придушення ліній зв'язку, виведення з ладу комп'ютер або її операційної системи, спотворення відомостей в базах даних або в системній інформації в комп'ютерних технологіях і т.д. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і т.п.

До основних загроз безпеки інформації відносять:

• розкриття конфіденційної інформації;

• компрометація інформації;

• несанкціоноване використання інформаційних ресурсів;

• помилкове використання інформаційних ресурсів;

• несанкціонований обмін інформацією;

• відмова від інформації;

• відмова в обслуговуванні.

Засобами реалізації загрози розкриття конфіденційної інформації можуть бути несанкціонований доступ до баз даних, прослуховування каналів і т.п. У будь-якому випадку отримання інформації, що є надбанням певної особи (групи осіб) іншими особами, завдає її власникам істотної шкоди.

Компрометація інформації, як правило, реалізується за допомогою внесення несанкціонованих змін до бази даних, в результаті чого її споживач змушений або відмовитися від неї, або вжити додаткових зусиль для виявлення змін і відновлення істинних відомостей. У разі використання скомпрометованої інформації споживач наражається на небезпеку прийняття неправильних рішень з усіма наслідками, що випливають звідси.

Несанкціоноване використання інформаційних ресурсів, з одного боку, є засобом розкриття або компрометації інформації, а з іншого має самостійне значення, оскільки, навіть не торкаючись користувацької або системної інформації, може завдати певної шкоди абонентам і адміністрації. Цей збиток може варіюватися в досить широких межах від скорочення надходження фінансових коштів до повного виходу автоматизованих інформаційних ресурсів з ладу.

Помилкове використання інформаційних ресурсів будучи санкціонованим тим не менш може привести до руйнування, розкриття або компрометації вказаних ресурсів. Дана загроза найчастіше є наслідком помилок, наявних в програмному забезпеченні автоматизованих інформаційних ресурсів.

Несанкціонований обмін інформацією між абонентами може призвести до отримання одним з них відомостей, доступ до яких йому заборонений, що за своїми наслідками рівносильно розкриттю змісту банківської інформації.

Відмова від інформації полягає в невизнанні одержувачем або відправником цієї інформації фактів її отримання або відправки. В умовах банківської діяльності це, зокрема, дозволяє одній зі сторін розривати укладені фінансові угоди «технічним» шляхом, формально не відмовляючись від них і завдаючи тим самим другій стороні значної шкоди.

Відмова в обслуговуванні є дуже істотна і поширена загроза, джерелом якої є сама автоматизована інформаційна система. Подібна відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів абоненту може привести до тяжких для нього наслідків. Так, відсутність у користувача даних, необхідних для прийняття рішення, протягом періоду часу, коли це рішення ще можливо ефективно реалізувати, може стати причиною його нераціональних або навіть антимонопольних дій.

Найбільш поширеними шляхами несанкціонованого доступу до інформації, сформульованими на основі аналізу зарубіжній пресі, є:

• перехоплення електронних випромінювань

• примусове електромагнітне опромінення (підсвічування) ліній зв'язку з метою отримання паразитної модуляції несучої;

• застосування підслуховуючих пристроїв (закладок);

• дистанційне фотографування;

• перехоплення акустичних випромінювань і відновлення тексту принтера; • розкрадання носіїв інформації і документальних відходів;

• читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

• копіювання носіїв інформації з подоланням заходів захисту;

• маскування під зареєструвати користувача;

• містифікація (маскування під запити системи);

• використання програмних пасток;

• використання недоліків мов програмування і операційних систем;

• включення в бібліотеки програм спеціальних блоків типу «Троянський кінь»;

• незаконне підключення до апаратури та ліній зв'язку;

• зловмисний виведення із ладу механізмів захисту;

• впровадження та використання комп'ютерних вірусів.

Особливу небезпеку в даний час представляє проблема комп'ютерних вірусів, так як з огляду на велику кількість різновидів вірусів надійного захисту проти них розробити не вдається. Всі інші шляхи несанкціонованого доступу піддаються надійної блокування при правильно розробленої і реалізованої на практиці системі забезпечення безпеки.

Цілісність розуміється як здатність засобів обчислювальної техніки або автоматизованої системи забезпечувати незмінність виду і якості інформації в умовах випадкового спотворення або загрози руйнування.

Загрози безпеці і цілісності складаються в потенційно можливих впливах на обчислювальну систему, які прямо або побічно можуть завдати шкоди безпеці і цілісності інформації, що обробляється системою.

Збиток цілісності інформації складається в її зміні, що приводить до порушення її виду або якості.

**ВИСНОВКИ**

В лекції розглянуті основні загрози які діляться на ненавмисні і навмисні. Джерелом перших можуть бути помилки в програмному забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації і т.п. Умисні загрози, на відміну від випадкових, мають на меті нанесення шкоди користувачам автоматизованих інформаційних технологій і, в свою чергу, поділяються на активні і пасивні.

**ІІ. ПИТАННЯ**

Реалізація загрози називається атакою. Людина, яка прагне реалізувати загрозу, називається порушником, або зловмисником.

Існує безліч класифікацій видів загроз за принципами і характером їх впливу на систему, по використовуваних засобів, цілям атаки і т

**Класифікація засобів захисту інформації**

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

**Морально-етичні засоби**. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут.

**Правові засоби захисту** — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання IT.

Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства.

Загальною тенденцією, що її можна простежити, є підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців. Так, уже сьогодні у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу 1C або Web-сайту, є 10 років позбавлення волі. Для порівняння, у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

**Адміністративні (організаційні) засоби захисту інформації** регламентують процеси функціонування 1C, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою усклад-нити або не допустити порушень безпеки. Вони охоплюють:

• заходи, які передбачаються під час проектування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);

• заходи, що здійснюються під час проектування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо);

• заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань і т. ін.);

• розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо).

Адміністративні засоби є неодмінною частиною захисту інформації, їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації (див. приклад), а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).

**ВИСНОВКИ З ДРУГОГО ПИТАННЯ:**

Під час розгляду другого питання лекції ми ознайомились зі складовими залежності від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

***ТЕМА 4. Методика оцінки ризиків інформаційної безпеки компанії***

**(2 години)**

**ПЛАН ЛЕКЦІЇ:**

1. Інженерний захист об'єктів.
2. Захист інформації від витоку технічними каналами та методи захисту інформації
3. Криптографічне перетворення інформації, контроль і облік доступу, законодавчі заходи, забезпечення інформаційної безпеки в Internet.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Информационные технологии и защита информации в информационнокоммуникационных системах: монография / под ред. В.С. Пономаренко. – Х. : вид. тов “Щедра садиба плюс”, 2015. – 486 с., русск. яз. ISBN 978-617-7225-03-3
2. Н.Е. Березюк., А.Г.Андрущенко и др. Кодирование информации. Харьков, Висшая школа, 2016.
3. Гундарь К.Ю. , Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерних системах - К:"Корнійчук" 2017.
4. В.В.Домарев. Защита информации и безопасность комьютерних систем - К. издательство Диасофт, 2019.
5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2016. – 476 с. (Укр. мов.)
6. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2016.
7. Защита информации. Сб.научних трудов - К, 2019.
8. К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений.– М., 2015.
9. Луцкер А. Авторское право в цифровых технологиях и СМИ. – М., 2005.
10. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях: Учебное пособие. - М. : ДМК Пресс, 2018. - 592 с.
11. Семкин С. Н., Семкин А. Н. Основи інформаційної безпеки об'єктів обробки інформації: Науч.-практ. посібник. Орел: 2016г. –300 с.
12. Герасименко В. А., Малюк А. А. Основи захисту інформації. М.: Инкомбук, 2017. –540 с.
13. Герасименко В. А. Захист інформації в автоматизованих системах обробки даних: У 2 кн. М.: Энергоатомиздат, 2016. –214с
14. Медведовский И.Д., Семьянов П.В., Платонов В.В. “АТАКА ЧЕРЕЗ INTERNET” :НПО "Мир и семья-95", 2017 г..
15. Барбара Гутман, Роберт Бэгвилл, Политика безопасности при работе в Интернете - техническое руководство. - М: Логос; 2017г. –178с.

**МЕТА ЛЕКЦІЇ**

Розглянути основні інженерні системи захисту інформації. Під несанкціонованим доступом розуміється порушення встановлених правил розмежування доступу, що в результаті випадкових або навмисних дій користувачів або інших суб'єктів системи розмежування, що є складовою частиною системи захисту інформації.

 Суб'єкти, які вчинили несанкціонований доступ до інформації, називаються порушниками. З точки зору захисту інформації несанкціонований доступ може мати такі наслідки: витік оброблюваної конфіденційної інформації, а також її спотворення або руйнування в результаті навмисного порушення працездатності автоматизованої системи.

Захист конфіденційної і цінної інформації від несанкціонованого доступу і модифікації покликана забезпечити вирішення однієї з найбільш важливих завдань: захисту майнових прав власників і користувачів комп'ютерів - захист власності, втілену в оброблюваної інформації, від всіляких вторгнень і розкрадань, які можуть завдати істотної економічний і інший матеріальний і нематеріальний збиток.

**І. ПИТАННЯ**

**Засоби фізичного (технічного) захисту інформації** — це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів 1C, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять:

* засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи (СКС), в якій використовуються однакові кабелі для організації передавання даних в 1C, сигналів від датчиків пожежної безпеки, відео-інформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів;
* засоби захисту системи електроживлення. Американські дослідники з компанії Best Power1 після п'яти років досліджень проблем електроживлення зробили висновок, що в кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності 1C можливе використання ава-рійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій;
* засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);
* засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо.

До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи і предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього.

Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

У практичній діяльності комерційних банків застосування заходів і засобів захисту інформації включає наступні самостійні напрямки:

• захист інформації від несанкціонованого доступу;

• захист інформації в системах зв'язку;

• захист юридичної значимості електронних, документів;

• захист конфіденційної інформації від витоку каналами побічних електромагнітних випромінювань і наводок;

• захист інформації від комп'ютерних вірусів і інших небезпечних впливів по каналах поширення програм;

• захист від несанкціонованого копіювання та розповсюдження програм і цінної когось пьютерной інформації. Для кожного напряму визначаються основні цілі та завдання.

Під несанкціонованим доступом розуміється порушення встановлених правил розмежування доступу, що послідувало в результаті випадкових або навмисних дій користувачів або інших суб'єктів системи розмежування, що є складовою частиною системи захисту інформації.

Суб'єкти, які вчинили несанкціонований доступ до інформації, називаються порушниками. З точки зору захисту інформації несанкціонований доступ може мати такі наслідки: витік оброблюваної конфіденційної інформації, а також її спотворення або руйнування в результаті навмисного порушення працездатності автоматизованої системи.

Порушником може бути будь-яка людина з наступних категорій:

• штатні користувачі автоматизованої системи;

• співробітники-програмісти, які супроводжують системне, загальне і прикладне програмне забезпечення системи;

• обслуговуючий персонал (інженери);

• інші співробітники, що мають санкціонований доступ до автоматизованої системи.

Доступ до автоматизованої системи інших, сторонніх осіб (які не належать до зазначених категорій) виключається організаційно-режимними заходами.

Під каналом несанкціонованого доступу до інформації розуміється послідовність дій осіб і виконуваних ними технологічних процедур, які або виконуються не-санкціоновано, або обробляються неправильно в результаті помилок персоналу або збою обладнання, що призводять в остаточному підсумку до факту несанкціонованого доступу. Виявлення всієї множини каналів несанкціонованого доступу проводиться в ході проектування шляхом аналізу технології зберігання, передачі і обробки інформації, певного порядку проведення робіт, розробленої системи захисту інформації та обраної моделі порушника.

Захист конфіденційної і цінної інформації від несанкціонованого доступу і модифікації покликана забезпечити вирішення однієї з найбільш важливих завдань: захисту майнових прав власників і користувачів комп'ютерів - захист власності, втілену в оброблюваної інформації, від всіляких вторгнень і розкрадань, які можуть завдати істотної економічний і інший матеріальний і нематеріальний збиток.

Програмно-технічний рівень протидії загрозам інформаційної безпеки такі механізми безпеки: ідентифікація і аутентифікація користувачів; управління доступом; протоколювання і аудит; криптографія; екранування каналів зв’язку; забезпечення високої доступності тощо. Важливо керувати інформаційними системами у цілому і механізмами безпеки особливо. Згадані заходи безпеки повинні спиратися на загальноприйняті стандарти, бути стійким до мережевих загроз, враховувати специфіку окремих сервісів.

Доступ до інформаційних систем слід надавати тільки зареєстрованим користувачам. Комп’ютерні системи, що обслуговують багатьох користувачів, мають задовольняти такі вимоги: ідентифікувати і перевіряти відповідність особистості користувачів, а також за потребою – термінал або місцеперебування зареєстрованого користувача; фіксувати випадки успішного і безуспішного доступу до інформаційних систем;

* надати систему управління паролями, що забезпечує вибір надійних паролів;
* обмежити час підключення користувачів до інформаційних систем.

Доступ до інформаційних систем необхідно здійснювати за допомогою надійної процедури входу в систему. Процедура входу в комп’ютерну систему повинна зводити ризик несанкціонованого доступу до мінімуму. Процедура входу в систему повинна виконувати такі функції:

* не виводити на екран ідентифікатори системи або додатки доти, поки не завершиться процес входу в систему;
* виводити на екран загальне попередження про те, що тільки зареєстровані користувачі мають право доступу до комп’ютера;
* не надавати довідкову інформацію під час виконання процедури входу в систему;
* перевіряти точність реєстраційної інформації тільки після завершення введення всіх даних;
* при виникненні ситуації збою система не повинна вказувати, яка частина введених даних правильна чи неправильна;
* повинно бути обмеження кількості невдалих спроб входу в систему (рекомендується три спроби), перш ніж розірвати канал зв’язку з користувачем.

Спостереження за доступом до інформаційних систем та використанням ІР адресу. Для забезпечення відповідності ПБ (управління доступом і стандартами) необхідно стежити за роботою ІС та використанням ІР. Це необхідно для того, щоб визначити ефективність вжитих заходів і забезпечити відповідність моделі ПБ. Усі надзвичайні ситуації і події, що пов’язані з порушенням режиму безпеки необхідно реєструвати в контрольному журналі. Записи в такому журналі варто зберігати протягом заданого проміжку часу для надання допомоги в майбутніх розслідуваннях і здійсненні контролю за доступом до ІС. Крім відкинутих спроб входу в систему, доцільно також реєструвати випадки успішного доступу до неї. Контрольний журнал повинний включати наступні дані: ідентифікатори користувачів; дата і час входу і виходу із системи; ідентифікаційний код робочої станції та за ким вона закріплена.

Необхідно також встановити процедури спостереження за використанням систем. Такі процедури вимагаються для забезпечення виконання користувачами тільки явно дозволених процесів. Рівень контролю, необхідний для окремих систем, варто визначити за допомогою незалежної оцінки ризиків. Усі дії, пов’язані зі спостереженням за системами, повинні бути формально дозволені керівництвом. Для забезпечення точності ведення контрольних журналів, що можуть знадобитися для розслідувань або як свідчення під час судових розглядів і при накладенні дисциплінарних стягнень, важливо правильно встановити системний годинник комп’ютерів. Неточні записи у контрольних журналах можуть перешкодити таким розслідуванням і підірвати довіру до такого свідчення.

*Аудит інформаційних систем*

Для зведення ризику виникнення збоїв у ІР до мінімуму вимоги щодо аудиту і роботи, які пов’язані з перевіркою робочих станцій варто планувати і погодити. З цією метою пропонуються наступні рекомендації:

вимоги до аудиту ІС повинні бути погоджені з відповідним керівництвом;

масштаб перевірок необхідно погодити і контролювати;

перевірки повинні бути обмежені доступом до даних і програм тільки на читання;

інші типи доступу (відмінні від доступу тільки на читання) повинні бути дозволені для окремих копій системних даних, які необхідно стерти по завершенні процесу аудиту;

необхідно явно ідентифікувати ІР для проведення перевірок і зробити їх доступними;

необхідно визначити вимоги щодо спеціальної чи додаткової обробки даних і погодити їх з постачальниками послуг;

усі випадки доступу необхідно відслідковувати і фіксувати в контрольному журналі для перевірок.

*Ідентифікація і аутентифікація користувачів.*

Одним з найбільш поширених засобів ідентифікації та аутентифікації користувачів у системах електронного урядування є електронний цифровий підпис (ЕЦП). ЕЦП – це вид електронного підпису, що отриманий за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого (закритого, секретного) ключа та перевіряється за допомогою відкритого ключа. ЕЦП призначений для використання фізичними або юридичними особами та використовується для: - ідентифікації особи (підписувача); - підтвердження цілісності даних в електронному документі (формі). Вагомість ЕЦП полягає у наданні юридичної сили електронному документу. ЕЦП вважається інструментом забезпечення інформаційної безпеки держави. ЕЦП є ефективним засобом контролю походження та цілісності інформації на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави. Механізм формування ЕЦП полягає у тому, що відбувається накладання особистого ключа та перевірка результату дії за допомогою відкритого ключа. За правовим статусом така дія прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа. За умови правильного зберігання власником особистого (закритого, секретного) ключа його підробка вважається неможливою. Електронний документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документу, будуть під час перевірки миттєво виявлені. Особистий ключ ЕЦП формується на підставі генератора випадкових чисел. Друга частина ЕЦП – відкритий ключ обчислюється з особистого ключа таким чином, щоб одержати закритий ключ з відкритого було неможливо. Документ підписується ЕЦП тільки за допомогою особистого ключа, який існує у його власника. Таким чином, особистий ключ ЕЦП є унікальною послідовністю символів довжиною 264 біта, що отримана випадковим чином та генерація якої з відкритого ключа є неможливою. Працює особистий ключ тільки в парі з відкритим ключем. Особистий ключ необхідно зберігати в таємниці, тому що будь-хто зможе підробити ЕЦП. Також, є поняття Сертифіката (в якому міститься відкритий ключ), що підтверджує приналежність відкритого ключа певній особі. Крім самого відкритого ключа, Сертифікат містить в собі персональну інформацію про його власника (ім’я, реквізити), унікальний реєстраційний номер та термін дії Сертифіката.

З метою забезпечення цілісності представлених у Сертифікаті даних він ще підписується особистим ключем Центру сертифікації ключів (ЦСК). Сертифікат відкритого ключа може публікуватися на сайті відповідного центру (ЦСК) відповідно до Договору про надання послуг ЕЦП. В Україні існує Національна система електронного цифрового підпису, яка складається з:

- центрального засвідчувального органу;

- акредитованих центрів сертифікації ключів;

- центрів сертифікації ключів; - контролюючого органу.

Послуги з надання ЕЦП в Україні впроваджуються акредитованими центрами сертифікації ключів.

**ІІ. ПИТАННЯ**

Основною в проблемі захисту інформації від несанкціонованого доступу є завдання розмежування функціональних повноважень і доступу до інформації, спрямована на запобігання не тільки можливості потенційного порушника «читати» зберігається в ПЕОМ інформацію, але і можливості порушника модифікувати її штатними і позаштатними засобами.

Вимоги щодо захисту інформації від несанкціонованого Доступу спрямовані на досягнення трьох основних властивостей інформації, що захищається:

• конфіденційність (засекречена інформація повинна бути доступна тільки тому, кому вона призначена);

• цілісність (інформація, на основі якої приймаються важливі рішення, повинна бути достовірною і точною і повинна бути захищена від можливих ненавмисних і зловмисних спотворень);

• готовність (інформація і відповідні інформаційні служби повинні бути доступні, готові до обслуговування завжди, коли в них виникає необхідність). В основі контролю доступу до даних лежить система розмежування доступу між користувачами автоматичної системи та інформації, що обробляється системою. Для успішного функціонування будь-якої системи розмежування доступу необхідне рішення двох завдань.

1. Зробити неможливим обхід системи розмежування доступу діями, що знаходяться в рамках обраної моделі.

2. Гарантувати ідентифікацію користувача, що здійснює доступ до даних (аутентифікація користувача).

Одним з ефективних методів збільшення безпеки автоматизованої системи є реєстрація. Система реєстрації і обліку, відповідальна за ведення реєстраційного журналу, дозволяє простежити за тим, що відбувалося в минулому, і відповідно перекрити канали витоку інформації. У реєстраційному журналі фіксуються всі здійснені або нездійснені спроби доступу до даних або програм. Зміст реєстраційного журналу може аналізуватися як періодично, так і безперервно.

У реєстраційному журналі ведеться список всіх контрольованих запитів, що здійснюються користувачами системи.

Система реєстрації і обліку здійснює:

• реєстрацію входу (виходу) суб'єктів доступу в систему (з системи) або реєстрацію завантаження і ініціалізації операційної системи і її програмного зупину.

При наявності простих засобів зберігання і передачі інформації існували і не втратили значення до теперішнього часу такі методи її захисту від навмисного доступу:

- обмеження доступу:

- розмежування доступу;

- поділ доступу (привілеїв);

- криптографічне перетворення інформації;

- контроль і облік доступу;

- законодавчі заходи.

Зазначені методи здійснювалися суто організаційно чи з допомогою технічних засобів.

З появою автоматизованої обробки інформації змінився і доповнився новими видами фізичний носій інформації та ускладнилися технічні засоби її обробки.

З ускладненням обробки, збільшенням кількості технічних засобів, що беруть участь в ній, збільшуються кількість і види випадкових впливів, а також можливі канали несанк-ціонірованного доступу. Зі збільшенням обсягів, зосередженням інформації, збільшенням кількості користувачів іншими зазначеними вище причинами збільшується ймовірність навмисного несанкціонованого доступу до інформації. У зв'язку з цим розвиваються старі і виникають нові додаткові методи захисту інформації в обчислювальних сі-стем:

- методи функціонального контролю, що забезпечують виявлення і діагностику відмов, збоїв апаратури і помилок людини, а також програмні помилки;

- методи підвищення достовірності інформації;

- методи захисту інформації від аварійних ситуацій;

- методи контролю доступу до внутрішнього монтажу апаратури, лініях зв'язку і технологічними-ським органам управління;

- методи розмежування і контролю доступу до інформації;

- методи ідентифікації і аутентифікації користувачів, технічних засобів, носіїв інформації і документів; - методи захисту від побічного випромінювання і наведень інформації.

При розробці АІТ виникає проблема щодо вирішення питання безпеки інформації, зі складової комерційну таємницю, а також безпеки самих комп'ютерних інформаційних систем.

Сучасні АІТ володіють наступними основними ознаками:

• наявністю інформації різного ступеня конфіденційності;

• необхідністю криптографічного захисту інформації різного ступеня конфіденцністю при передачі даних;

• иерархичностью повноважень суб'єктів доступу і програм до АРМ, файл-серверам, каналам зв'язку і інформації системи, необхідністю оперативного зміни цих повноважень;

• організацією обробки інформації в діалоговому режимі, в режимі поділу часу між користувачами і в режимі реального часу;

• обов'язковим управлінням потоками інформації, як в локальних мережах, так і при передачі по каналах зв'язку на далекі відстані;

• необхідністю реєстрації та обліку спроб несанкціонованого доступу, подій в системі і документів, що виводяться на друк;

• обов'язковим забезпеченням цілісності програмного забезпечення та інформації в АІТ;

• наявністю коштів відновлення системи захисту інформації;

• обов'язковим урахуванням магнітних носіїв;

• наявністю фізичної охорони засобів обчислювальної техніки і магнітних носіїв.

Організаційні заходи і процедури, які використовуються для вирішення проблеми безпечно-сті інформації, вирішуються на всіх етапах проектування і в процесі експлуатації АІТ.

Суттєве значення при проектуванні надається передпроектному обстеження об'єктивним та. На цій стадії:

• встановлюється наявність секретної (конфіденційної) інформації в розробляється АІТ, оцінюється рівень конфіденційності і обсяги;

• визначаються режими обробки інформації (діалоговий, телеобробки і режим реально-го часу), склад комплексу технічних засобів, загальносистемні програмні засоби і т.д .;

• аналізується можливість використання наявних на ринку сертифікованих засобів захисту-інформації;

• визначається ступінь участі персоналу, функціональних служб, фахівців і допоміжні-них працівників об'єкта автоматизації в обробці інформації, характер взаємодії між собою і зі службою безпеки;

• визначаються заходи щодо забезпечення режиму секретності на стадії розробки.

Серед організаційних заходів щодо забезпечення безпеки інформації важливе ме-сто займає охорона об'єкту, на якому розташована захищається АІТ (територія будівлі, по-ня, сховища інформаційних носіїв). При цьому встановлюються відповідні пости охорони, технічні засоби, що запобігають або істотно ускладнюють хіще-ня засобів обчислювальної техніки, інформаційних носіїв, а також вилучати не-санкціонований доступ до АІТ і лініях зв'язку.

Функціонування системи захисту інформації від несанкціонованого доступу, як комплексу програмно-технічних засобів і організаційних (процедурних) рішень, перед-сматрівает:

• облік, зберігання і видачу користувачам інформаційних носіїв, паролів, ключів;

• ведення службової інформації (генерація паролів, ключів, супровід правил розгром-ніченний доступу);

• оперативний контроль за функціонуванням систем захисту секретної інформації;

• контроль відповідності загальносистемного програмного середовища еталону;

• приймання включаються в АІТ нових програмних

**ВИСНОВКИ**

Проблеми захисту інформації в комп'ютерних системах показують, що заходи, що запобігають можливі економічні втрати від незахищеності інформації, вимагають вкладення значних коштів.

Автоматизація (без якої неможливо сучасний розвиток) призводить до зростання загроз несанкціонованого доступу до інформації та, як наслідок, до необхідності постійної підтримки і розвитку системи захисту. Захист інформації є не разовим заходом і навіть не сукупністю заходів, а безперервним процесом, який повинен протікати в часі на всіх етапах життєвого циклу комп'ютерної системи.

Створення ефективних засобів захисту може бути здійснено висококваліфікованими фахівцями. Аналізу та оцінки, проектування системи захисту інформації, сертифікацію захищеності необхідно проводити незалежні організації, що мають державну ліцензію на проведення зазначених робіт.

***ТЕМА 5. Управління інформаційною безпекою на державному рівні.***

**(2 години)**

**ПЛАН ЛЕКЦІЇ:**

1. Аналіз різних способів порушень інформаційної безпеки.
2. Основні види мережевих і комп'ютерних загроз.
3. Засоби і методи захисту від мережевих комп'ютерних загроз.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Информационные технологии и защита информации в информационнокоммуникационных системах: монография / под ред. В.С. Пономаренко. – Х. : вид. тов “Щедра садиба плюс”, 2015. – 486 с., русск. яз. ISBN 978-617-7225-03-3
2. Н.Е. Березюк., А.Г.Андрущенко и др. Кодирование информации. Харьков, Висшая школа, 2016.
3. Гундарь К.Ю. , Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерних системах - К:"Корнійчук" 2017.
4. В.В.Домарев. Защита информации и безопасность комьютерних систем - К. издательство Диасофт, 2019.
5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2016. – 476 с. (Укр. мов.)
6. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутрішніх справ, 2015. – 104 с.

**МЕТА ЛЕКЦІЇ**

Розглянути основні види інформаційних загроз необхідність впроваджувати новітні методи і заходи та побудову ефективної технології захисту інформації. Використовувати основні теоретичні положення і методи, формування умінь і прищеплення навичок застосування теоретичних знань для вирішення прикладних завдань, а також розвиток нових підходів до забезпечення інформаційної безпеки в сфері економіки.

**І. ПИТАННЯ**

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи описи і класифікації. Для здійснення ефективного захисту системи управління НБ слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження при чинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють:

1) фізичний;

2) програмно-технічний;

3) управлінський;

4) технологічний;

5) рівень користувача;

6) мережевий;

7) процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Виділяють декілька типів методів забезпечення інформаційної безпеки:

• однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

• багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

• комплексні методи — багаторівневі технології, які об'єднані у єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

• інтегровані високоінтелектуальні методи — багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать: прийняття рішення по визначенню області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління НБ; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також переслідуваних цілей. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю по забезпеченню інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже, система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Втім не слід плекати надію на створення абсолютної системи інформаційної безпеки, оскільки, як зазначалося нами вище, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже, їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою, і водночас слугують імпульсом до вдосконалення, тобто до розвитку. Отже, важливим метод забезпечення інформаційної безпеки е метод розвитку.

Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загрози, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз тощо. Мета якісної оцінки ризиків — ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. При чому аналіз подій в світі надає усі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн.

Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно проводяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак в ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення відіграє метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як у напряму надання певного впливу на джерело загрози, так і в напряму укріплення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша — сукупністю заходів по забезпеченню інформаційної безпеки об'єкта.

Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберітеються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного і програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Методи впливу на інформаційну інфраструктуру можуть бути поділені на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації, і таким чином, на попередження нанесення шкоди предметам суспільних відносин, що захищаються.

У цілому ж слід зазначити, що вибір цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

**Висновки з першого питання**

Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загрози, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків.

**ІІ. ПИТАННЯ**

У зв'язку зі стрімким розвитком інформаційних технологій і їх проникненням у всі сфери людської діяльності зросла кількість злочинів, спрямованих проти інформаційної безпеки. Велику зацікавленість з боку кібер-злочинців викликає діяльність і державних структур, і комерційних підприємств. Їхньою метою є розкрадання, розголошення конфіденційної інформації, підрив ділової репутації, порушення працездатності і, як наслідок, доступності інформаційних ресурсів організації. Такі дії завдають величезних моральних і матеріальних збитків.

Насправді ризик чатує не лише на крупні компанії, але й на окремих користувачів. За допомогою різних засобів злочинці дістають доступ до персональних даних – номерів банківських рахунків, кредитних карт, паролей, виводять обчислювальну систему з ладу або дістають повний доступ до комп'ютера. Надалі такий комп'ютер може використовуватися як частина зомбі-мережі – мережі заражених комп'ютерів, які використовують зловмисники для проведення атак на сервери, розсилки спаму, збору конфіденційної інформації, розповсюдження нових вірусів і троянських програм.

Сьогодні всі визнають, що інформація є цінним надбанням і підлягає захисту. В той самий час інформація має бути доступною для певного круга користувачів (наприклад, співробітникам, клієнтам і партнерам підприємства). Таким чином, постає питання про створення комплексної системи інформаційної безпеки. Така система має враховувати всі можливі джерела загроз (людський, технічний і стихійний чинники) і використовувати весь комплекс захисних заходів: фізичних, адміністративних і програмно-технічних засобів захисту.

**Джерела загроз**

1. **Людський чинник.** Ця група загроз пов'язана з діями людини, що має санкціонований або несанкціонований доступ до інформації. Загрози цієї групи можна розділити на:
	* *зовнішні* — дії кібер-злочинців, хакерів, інтернет-шахраїв, недобросовісних партнерів, кримінальних структур;
	* *внутрішні* — дії персоналу компаній і також користувачів домашніх комп'ютерів. Дії даних людей можуть бути як умисними, так і випадковими.
2. **Технічний чинник.** Ця група загроз пов'язана з технічними проблемами – фізичне і моральне старіння устаткування, неякісні програмні і апаратні засоби опрацювання інформації. Все це приводить до відмови устаткування втрати інформації.
3. **Стихійний чинник.** Ця група загроз включає природні катаклізми, стихійні лиха і інші форс-мажорні обставини, незалежні від діяльності людей.

Всі ці джерела загроз необхідно обов'язково враховувати при розробці системи захисту інформаційної безпеки. Ми зупинимося лише на одному з них — зовнішніх загрозах, пов'язаних з діяльністю людини.

**Шляхи поширення загроз (людський чинник)**

**Глобальна мережа Інтернет** унікальна тим, що не є чиєюсь власністю і не має територіальних меж. Це багато в чому сприяє розвитку численних веб-ресурсів і обміну інформацією. Зараз будь-яка людина може дістати доступ даним, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, утрудняючи їх виявлення і покарання. Зловмисники розміщують віруси і інші шкідливі програми на веб-ресурсах, «маскують» їх під корисне і безкоштовне програмне забезпечення.

Cкрипти, що автоматично запускаються при відкритті веб-сторінки, можуть виконувати шкідливі дії на вашому комп'ютері, включаючи зміну системного реєстру, крадіжку особистих даних і установку шкідливого програмного забезпечення. Використовуючи мережеві технології, зловмисники реалізують атаки на видалені приватні комп'ютери і сервери компаній. Результатом таких атак може бути виведення ресурсу з ладу, діставання повного доступу до ресурсу, а, отже, до інформації, що зберігається на ньому, використання ресурсу як частини зомбі- мережі. У зв'язку з появою кредитних карт, електронних грошей і можливістю їх використання через Інтернет інтернет-шахрайство стало одним з найбільш поширених злочинів.

**Інтранет** – це внутрішня мережа, спеціально розроблена для управління інформацією усередині компанії або приватної домашньої мережі. Інтранет є єдиним простором для зберігання, обміну і доступу до інформації для всіх комп'ютерів мережі. Тому, якщо якій-небудь з комп'ютерів мережі заражений, решту комп'ютерів піддано величезному ризику зараження. Щоб уникнути виникнення таких ситуацій необхідно захищати не лише периметр мережі, але й кожний окремий комп'ютер.

**Електронна пошта**. Наявність поштових застосунків практично на кожному комп'ютері і використання шкідливими програмами вмісту електронних адресних книг для виявлення нових жертв забезпечують сприятливі умови для розповсюдження шкідливих програм. Користувач зараженого комп'ютера, сам того не підозрюючи, розсилає заражені листи адресатам, які у свою чергу відправляють нові заражені листи і т.д. Нерідкісні випадки, коли заражений файл-документ унаслідок недогляду потрапляє в списки розсилки комерційної інформації якої-небудь крупної компанії. В цьому випадку страждають сотні або навіть тисячі абонентів таких розсилок, які потім розішлють заражені файли десяткам тисячам своїх абонентів.

Крім загрози проникнення шкідливих програм існують проблема зовнішньої небажаної пошти рекламного характеру (спаму). Не будучи джерелом прямої загрози, небажана кореспонденція збільшує навантаження на поштові сервери, створює додатковий трафік, засмічує поштову скриньку користувача, веде до втрати робочого часу і тим самим наносить значні фінансові втрати. Зловмисники стали використовувати так звані спамерські технології масового розповсюдження, щоб примусити користувача відкрити лист, перейти по посиланню з листа на якийсь інтернет-ресурс. Отже, можливості фільтрації спаму важливі не лише самі по собі, але і для протидії інтернет-шахрайству і розповсюдженню шкідливих програм.

**Знімні носії інформації** — дискети, CD-диски, флеш-карти — широко використовують для зберігання і поширення інформації. При активуванні файлу знімного носія, що містить шкідливий код, є загроза пошкодити дані на вашому комп'ютері і розповсюдити вірус на інші носії інформації або комп'ютери мережі.

**Розглянемо види загроз.**

**Черви (Worms)** використовують для розповсюдження «діри» (недоліки) операційної системи. Назву отримали виходячи із здатності черв'яків «переповзати» (з комп'ютера на комп'ютер), використовуючи мережі, електронну пошту й інші інформаційні канали. Завдяки цьому багато черви мають високу швидкістю розповсюдження. Вони проникають у комп'ютер, обчислюють мережеві адреси інших комп'ютерів і розсилають за цими адресами свої копії. Крім мережевих адрес використовуються дані адресної книги поштових клієнтів. Представники цього класу шкідливих програм іноді створюють робочі файли на дисках системи, але можуть і взагалі не звертатися до ресурсів комп'ютера (за винятком оперативної пам'яті).

**Віруси (Viruses)** заражають інші програми, додаючи в них свій код з метою отримати управління при запуску зараженого файлу.

**Троянські програми (Trojans)** виконують в уражених комп'ютерах несанкціоновані користувачем дії: знищують інформацію на дисках, приводять систему до «зависання», крадуть конфіденційну інформацію тощо. Такі програми не є вірусом в традиційному розумінні цього терміну, бо не заражають інші програми або дані). Вони не здатні *самостійно* проникати у комп'ютери і розповсюджуються зловмисниками під виглядом «корисного» програмного забезпечення. Нанесена ними шкода може багатократно перевищувати втрати від традиційної вірусної атаки.

Останнім часом найпоширенішими типами шкідливих програм, що псують комп'ютерні дані, стали черви. Далі по поширеності слідують віруси і троянські програми. Деякі шкідливі програми суміщають у собі ознаки двох або навіть трьох з перералічених вище класів.

**Програми-реклами (Adware)** — програмний код, без відома користувача включений у програмне забезпечення з метою демонстрації рекламних оголошень. Зазвичай програми-реклами вбудовано у програмне забезпечення, яке розповсюджують безкоштовно. Рекламу розташовують у робочому інтерфейсі. Часто такі програми збирають і переправляють своєму розробникові персональну інформацію про користувача, змінюють різні параметри браузера (стартові і пошукові сторінки, рівні безпеки тощо) і створюють неконтрольований користувачем трафік. Все це може привести як до порушення політики безпеки, так і до прямих фінансових втрат.

**Програми-шпигуни (Spyware)** збирають відомості про окремо взятого користувача або організацію без їх відома. Про наявність програм-шпигунів на своєму комп'ютері ви можете і не здогадуватися. Як правило, метою програм-шпигунів є:

* відстежування дій користувача на комп'ютері;
* збір інформації про зміст жорсткого диска (найчастіше йдеться про сканування деяких тек і системного реєстру з метою складання списку програмного забезпечення, встановленого на комп'ютері);
* збір інформації про якість зв'язку, спосіб підключення, швидкість модему тощо.

**Потенційно небезпечні додатки (Riskware)** не мають якої-небудь *власної* шкідливої функції, але ними можуть скористатися зловмисники як допоміжними складовими шкідливої програми, що містять проломи й помилки. Наявність таких програм на комп'ютері піддає ваші дані ризику. До таких програм відносять деякі утиліти видаленого адміністрування, програми автоматичного перемикання розкладки клавіатури, IRC-клієнти, FTP-сервери, всілякі утиліти для зупинки процесів або утаєння їх роботи.

Ще одним видом шкідливих програм на межі Adware, Spyware і Riskware є програми, що вбудовуються у встановлений на комп'ютері браузер і перенаправляють трафік. Можливо, ви зустрічалися з такими програмами, якщо при запиті одного сайту відкривався зовсім інший.

**Програми-жарти (Jokes)** не заподіють комп'ютеру якої-небудь прямої шкоди, але виводять повідомлення про те, що таку шкоду вже заподіяно або буде заподіяно за яких-небудь умов. Такі програми часто виводять повідомлення про форматування диска (хоча ніякого форматування насправді не відбувається), виявляють віруси в незаражених файлах тощо.

**Програми-маскувальники (Rootkit)** — утиліти, використовувані для приховання шкідливої активності. Вони маскують шкідливі програми, щоб уникнути їх виявлення антивірусними програмами. Програми-маскувальники модифікують операційну систему на комп'ютері і замінюють основні її функції, щоб приховати свою власну присутність і дії, які робить зловмисник на зараженому комп'ютері.

**Інші небезпечні програми**

Програми, створені для організації DОS-атак на віддалені сервери, злому інших комп'ютерів, а також середовища розробки шкідливого програмного забезпечення. До таких програм відносяться утиліти (Hack Tools) хакерів, конструктори вірусів, сканери вразливості, програми для злому паролів, інші види програм для злому мережевих ресурсів або проникнення в систему, яку атакують.

**Класифікація комп'ютерний вірусів**

**За об'єктами зараження:**

* *файлові* — уражають програми (основні й допоміжні, тобто ті, що завантажуються лише під час виконання основних);
* *завантажувальні* — уражають завантажувальні сектори дисків;
* *віруси структури файлової системи* — здатні вносити зміни в службові структури файлової системи таким чином, що вірус включається у файли, призначені для виконання, явно не вкорінюючи в них свій код. Усі записи в теках щодо цих програм ммодифікуються таким чином, що першим кластером програми стає кластер, який містить код вірусу. Під час запуску будь-якої такої програми замість неї працює вірус. Першим вірусом, що використовував подібну технологію, був DIR-вірус;

Кажуть також: *файлово-бутові, пакетні, мережеві, WinWord-віруси, Windows-віруси, OS/2-віруси, Novell NеtWare-віруси, BIOS-віруси, CD-ROM-віруси* тощо.

**За способом зараження** середовища мешкання вірусів:*резидентні й нерезидентні.*

**За зовнішнім виглядом:**

* *звичайні* — код вірусу видно на диску;
* *невидимі (Stealth-віруси)* — використовують особливі методи маскування, при перегляді код вірусу не видно. Stealth-віруси мають резидентний модуль, який постійно знаходиться в оперативній пам’яті комп’ютера. Маскування Stealth-вірусів спрацьовує лише тоді, коли в ОЗУ знаходиться резидентний модуль вірусу. Якщо ОС завантажувати з дискети, вірус не отримує керування ПК і Stealth-механізм не спрацьовує;
* *поліморфні* — код вірусу змінний.

**За результатами діяльності:**

* *безпечні* — лише поширюють себе та інколи призводять до виведення повідомлень, перезавантаження та інших несподіваних, незручних ефектів, але без втрати наявної інформації чи шкоди апаратному забезпеченню;
* *небезпечні* — призводять до втрати інформації, руйнування обчислювальної системи як програмного, так і (можливо) апаратного забезпечення.

**За кількістю засобів знешкодження:** *знешкоджені однією антивірусною програмою (АVО-віруси) чи знешкоджені кількома антивірусними програмами (комплектом N антивірусів — АVN-віруси).*

**За способом створення вірусів:** *створені ручними засобами розробки (Н-віруси) і створені автоматизованими засобами розробки (А-віруси).*

**ВИСНОВКИ З ДРУГОГО ПИТАННЯ**

Сьогодні всі визнають, що інформація є цінним надбанням і підлягає захисту. В той самий час інформація має бути доступною для певного круга користувачів (наприклад, співробітникам, клієнтам і партнерам підприємства). Таким чином, постає питання про створення комплексної системи інформаційної безпеки. Така система має враховувати всі можливі джерела загроз (людський, технічний і стихійний чинники) і використовувати весь комплекс захисних заходів: фізичних, адміністративних і програмно-технічних засобів захисту.

**ІІІ. ПИТАННЯ**

**Програмні засоби захисту** забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в 1C, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям 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* базується 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 ко-льору або звуку обмежені. 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 недоторканість 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 1C, розрізняють два основні його способи:

• додатковий захист — засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;

• вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів 1C або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом 1C. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

**Захист від комп'ютерних вірусів**

Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивіруси плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання антивірусних програм — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

**Антивірусні програми** поділяють на кілька видів.

**Програми-детектори** здійснюють пошук сигнатур вірусів. Недоліком детекторів є те, що вони можуть знаходити тільки ті віруси, які відомі їхнім розробникам, а отже, вони швидко застарівають. Деякі програми-детектори можна настроювати на нові типи вірусів, проте неможливо розробити програму, яка могла б виявити будь-який заздалегідь невідомий вірус. Отже, негативний результат перевірки програмою-детектором не гарантує відсутності вірусів. Багато детекторів мають режими лікування або знищення заражених файлів — функції докторів.

**Програми-доктори («фаги»)** не тільки знаходять заражені вірусами файли, а й «лікують» їх (видаляють з файла тіло програ-ми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед фагів виок-ремлюють поліфаги — програми-доктори, призначені для пошуку і знищення великої кількості вірусів. Як і детектори, програми-доктори потребують постійного оновлення.

**Програми-ревізори** запам'ятовують початковий стан програм, каталогів і системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, порівнюють поточний стан системи з початковим. Як правило, перевірка здійснюється відразу після завантаження операційної системи — контролюються довжина файла, його контрольна сума, дата і час модифікації та інші параметри. Деякі програми-ревізори можуть при цьому виявляти і стелс-віруси. Гібриди програм-ревізорів і докторів можуть не тільки виявляти зміни, а й повертати файли і сис-темні області до початкового стану. Вони є більш універсальними, оскільки можуть захистити і від вірусу, не відомого на час їх створення, якщо він використовує стандартний механізм зараження.

**Програми-фільтри** («сторожа», «монітори») — резиденти} програми, призначені для виявлення підозрілих дій при роботі комп'ютера. Після одержання відповідного повідомлення користувач може дозволити або відмінити виконання операції. Деякі програми-фільтри перевіряють програми, які викликаються до виконання, та файли, що копіюються. Недоліком подібних програм є їх «набридливість», можливі конфлікти з іншим програмним забезпеченням, а перевагами — виявлення вірусів на ранній стадії, що мінімізує втрати.

**Програми-вакцини** («іммунізатори») модифікують програми і диски таким чином, що це не відбивається на роботі програм, але вірус, від якого проводиться вакцинація, вважає їх інфікованими. Це вкрай неефективний спосіб захисту. Вакцини мають обмежене використання — їх можна застосувати тільки проти відомих вірусів.

Жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержувати загальних правил (див. вставки) і користуватись останніми розробками антивірусних лабораторій.

**Класифікація антивірусних програм:**

* *детектори* (*сканери,* наприклад, антивірус Касперського, Doctor Web, MS AntiVirus, Eset Smart Security (NOD32) — перевіряють, чи є у файлах специфічна для відомого вірусу комбінація байтів. Вимагають постійного оновленя своїх баз даних;
* *лікарі (фаги)* — відривають від інфікованих програм тіло вірусу і відтворюють початковий стан програм;
* *ревізори* (наприклад, програма Adinf) — контролюють уразливі для вірусної атаки компоненти комп’ютера: запам’ятовують дані про стан файлів і системних ділянок дисків, а при наступних запусках порівнюють їхній стан із вихідним;
* *вакцини (імунізатори,* наприклад, Anti Trojan Elite, Trojan Remover або Dr.Web CureIt!) — модифікують програми і диски таким чином, що вірус вважає їх уже інфікованими. Така модифікація не позначається на роботі програмного забезпечення. Зараз малопоширені;
* *фільтри (охоронці)* — повідомляють користувача про всі дії на його комп'ютері. Якщо троянська програма або вірус захочуть проникнути у ПК або викрасти пароль і відправити його зловмисникові, фільтр миттєво спрацює і запитає: «Дозволити чи заборонити виконання операції?». Робота з таким типом захисту вимагає певних навичок: не кожен користувач знає, що означає того чи іншого процесу. Може це Windows надумала оновитися? До речі, антивірус-фільтр є практично на кожному ПК і називають його брандмауер. Якщо такий стандартний охоронець не влаштовує користувача, він може придбати що-небудь інше, наприклад [Outpost Security Suite](http://www.agnitum.com/products/security-suite/index.php). Багато сучасних антивірусів мають вбудований брандмауер, що дозволяє контролювати мережевий трафік і стежити за змінами в системі.

Поширені такі антивірусні програми:

* для *Linux:* [avast!](http://www.avast.com/linux-home-edition), [Bitdefender](http://bitdefender.com/), [ClamAV](http://www.clamav.net/lang/en/download/packages/packages-linux/), [F-Prot Antivirus](http://www.f-prot.com/download/home_user/);
* для *Windows*: [avast!](http://www.avast.com/), [ADinf](http://adinf.com/), [AVG](http://free.avg.com/), [Bitdefender](http://bitdefender.com/), [ClamAV](http://www.clamav.net/lang/en/about/win32/), [F-Prot Antivirus](http://www.f-prot.com/download), [Dr.Web](http://download.drweb.com/), [ESET NOD32](http://www.esetnod32.ru/), [KASPERSKY](http://kaspersky.ru/), [Norton](http://us.norton.com/downloads/).

**ВИСНОВКИ ДО ТРЕТЬОГО ПИТАННЯ**

Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивіруси плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання антивірусних програм — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

**ВИСНОВКИ З ТЕМИ**

При розгляді проблеми інформаційної безпеки важливим кроком є виділення загроз інформаційній безпеці, а також аналіз захисту від цих загроз. Загроза інформаційній безпеці – явище, дії негативних чинників або процес, через які: соціальні об’єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері; а також, порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об’єктів інформаційної безпеки.

***ТЕМА 6. Організаційні заходи забезпечення безпеки комп'ютерних інформаційних систем***

**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

**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.

**І. ПИТАННЯ**

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

Р

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.

01100010001

Привіт

Привіт

Шифрування

Розшифровка

Відкритий ключ

Канал зв'язку

Шифроване повідомлення

Повідомлення

Повідомлення

11110101

Закритий ключ

Р

Рис. 5.3. Несиметричне шифрування

Адже, в цьому разі, кожна група користувачів, які бажають обмінюватися секретними повідомленнями, повинна мати свої оригінальні алгоритми 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.

**ІІ. ПИТАННЯ**

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.

**ІІІ ПИТАННЯ**

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.