Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

**А.М. Гребенюк, Л.В. Рибальченко**

# ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

***Навчальний посібник***

Дніпро
2020

УДК 33+004.056.5
Г 79

*Рекомендовано до друку*
*Науково-методичною радою*
*Дніпропетровського державного*
*університету внутрішніх справ*
*(протокол №10 від 18 червня 2020 р.)*

РЕЦЕНЗЕНТИ:
**Корнієнко Валерій Іванович** – доктор технічних наук, професор, завідувач кафедри безпеки інформації та телекомунікацій, Національний технічний університет "Дніпровська політехніка".
**Баранник Лілія Борисівна** – докторка економічних наук, професорка, професорка кафедри соціального забезпечення та податкової політики, Університет митної справи та фінансів.
**Рибальський Олег Володимирович** – доктор технічних наук, професор, головний науковий співробітник науково-дослідної лабораторії Національної академії внутрішніх справ. Лауреат державної премії.

Гребенюк А.М.
Г 79 **Основи управління інформаційною безпекою**: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.

**ISBN 978-617-627-148-2**

Навчальний посібник призначено для вивчення дисциплін "Управління інформаційною безпекою", "Сучасні інформаційні технології захисту даних". У ньому розглянуті основні загрози інформаційній безпеці, що виникають в сучасному суспільстві та на виробництвах, висвітлено питання протидії комп'ютерним вірусам та захист інформації у комп'ютерних мережах. Особливу увага приділено системі управління інформаційною безпекою, в тому числі її нормативно-правовим забезпеченням.
За кожною темою передбачено контрольні запитання та надається загальний перелік використаних джерел.
Розраховано на здобувачів вищої освіти.

**ISBN 978-617-627-148-2**

**З М І С Т**

# ВСТУП

Кожен технологічний бізнес-процес піддається загрозам безпеки і конфіденційності. Сучасні засоби захисту здатні боротися з атаками кіберзлочинців. Але цього недостатньо – тому фірма або підприємство повинні забезпечити такі умови внутрішньої політики і поведінки співробітників, щоби мінімізувати або значно зменшити ці ризики.

Оскільки цей процес складний і потребує висококваліфікованих фахівців, компанії впроваджують структурні підрозділи, що застосовують систему управління інформаційною безпекою. Система управління інформаційною безпекою (СУІБ) – основа політики і засобів управління, що систематично керують інформаційною безпекою та упередженням ризиків на підприємстві.

Ці заходи безпеки можуть відповідати загальним стандартам безпеки або бути більш сфокусованими на певній галузі. Наприклад, ISO 27001 представляє набір специфікацій з детальним описом створення, управління та реалізації політики і засобів управління СУІБ. ISO містить керівництво з розробки відповідних стратегій системи управління інформаційною безпекою.

Основа системи управління інформаційною безпекою орієнтована на оцінку ризиків і управління ними. Процес управління ризиками безпеки дозволяє організаціям досягти поєднання максимальної економічної ефективності з відомим та прийнятним рівнем ризику та надає керівникам різних рівнів зрозумілий метод організації та ресурсів з обмеженим доступом для реалізації управління ризиками. Реалізація управління ризиками інформаційної безпеки дозволяє організаціям з розподіленими корпоративними мережами використовувати економічно ефективний контроль, що знижує ризик до прийнятного рівня.

Управління інформаційною безпекою можливе за підтримки безпеки в інформаційно-комунікаційних системах та мережах певного діапазону засобів і заходів управління.

# ТЕМА 1. ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 1.1 Характеристика інформаційної безпеки

Під *інформаційною безпекою* розуміють захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, в тому числі власникам і користувачам інформації і підтримуючої інфраструктури.

***Захист інформації*** – комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Аналізуючи підходи до проблем інформаційної безпеки, необхідно починати з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). Загрози інформаційної безпеки пов'язані з використанням інформаційних технологій.

Інформаційна безпека залежить від усього комплексу заходів та сучасних технологій, керування якими відбувається із застосуванням різноманітних інформаційних систем.

**Інформаційна безпека** – багатогранна, багатовимірна діяльність, в якій успіх може принести тільки системний, комплексний підхід. Безпека використання інформаційних систем полягає у забезпеченні доступності, цілісності, конфіденційності та підтримці інформаційних ресурсів її інфраструктури.

До основних складових інформаційної безпеки належить конфіденційність, тобто захист від несанкціонованого доступу до інформації.

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, яка полягає в тому, що інформаційна безпека є складова частина інформаційних технологій – області, що розвивається безпрецедентно високими темпами. Тут важливі не

стільки окремі рішення (закони, навчальні курси, програмно-технічні вироби), що знаходяться на сучасному рівні, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу.

Складність механізмів прийняття сучасних управлінських рішень щодо захисту інформації в новому інформаційному середовищі пов'язана із застосуванням стрімко розвиваючих інформаційних систем, призначених для великого обсягу обробки, обміну та використання їх в сучасному житті кожної особистості, підприємства, держави, світі, а також швидкими темпами розвитку технічних засобів.

**Загрозу** можна розглядати як атаку та можливість порушення інформаційної безпеки і посягання на заволодіння інформацією, а той, хто посягає на інформацію є зловмисником. Загроза проявляються через низький захист або знаходження вразливих місць у системі захисту інформаційних систем.

*Основними завданнями системи інформаційної безпеки є*:

- виявлення та усунення загроз безпеки нанесенню економічного, фінансового, матеріального та морального збитку;

- створення механізмів реагування на загрози розвитку і функціонуванню підприємства та національній безпеці;

- прийняття заходів щодо забезпечення безпеки персоналу підприємства та інше.

Поняття інформаційної безпеки включає:

- ✓ надійність роботи комп'ютера;
- ✓ збереження цілісності даних;
- ✓ захист інформації від несанкціонованого доступу;
- ✓ таємниця електронного листування.

*Інформаційні загрози можуть бути обумовлені*:

- ✓ природними факторами;
- ✓ людськими факторами.

***До природніх факторів*** відносяться такі джерел загроз, які об'єднують, обставини, що становлять непереборну силу, тобто такі обставини, що носять об'єктивний і абсолютний характер, поширюється на всіх. До непереборної сили в законодавстві і договірній практиці відносять стихійні лиха або інші обставини, що неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти при сучасному рівні людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до тих, що захищаються і під ними розуміються насамперед природні катаклізми (пожежі, землетруси, повені, урагани, різні непередбачені обставини, незрозумілі явища та інші форс-мажорні обставини)

***До людських факторів відносяться:***

- ✓ загрози випадкового характеру (помилки обробки, передачі, обміну інформації);
- ✓ загрози навмисного характеру (несанкціонований доступ до інформації).

Навмисні загрози призводять до шкідливих наслідків користувачам автоматизованих інформаційних систем і можуть бути *активні і пасивні.*

*Пасивні загрози* спрямовані на несанкціоноване використання інформаційних ресурсів і не впливають на функціонування системи (прослуховування).

*Активні загрози* спрямовані на порушення нормального процесу функціонування системи через вплив на апаратні, програмні та інформаційні ресурси. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і т.п.

## 1.2 Класифікація загроз

Загрози інформаційної безпеки класифіковані за різними ознаками.

**1. За аспектом інформаційної безпеки, на який спрямовані загрози.**

✓ *Загрози конфіденційності* (неправомірний доступ до інформації).

✓ *Загроза порушення конфіденційності* полягає в тому, що інформація стає відомою тому, хто не має повноважень доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в обчислювальній системі чи переданої від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози виникають внаслідок «людського фактору» (наприклад, випадкове делегування тому чи іншому користувачеві привілеїв іншого користувача), збоїв в роботі програмних і апаратних засобів.

✓ *До інформації обмеженого доступу належить державна таємниця* [2] *і конфіденційна інформація* [3] (комерційна таємниця; персональні дані; професійні види таємниць: лікарська, адвокатська, банківська, службова, нотаріальна, таємниця страхування, слідства і судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця зв'язку); відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації (ноу-хау) і ін.).

- *Загрози цілісності* (неправомірна зміна даних). Загрози порушення цілісності – загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними факторами – від навмисних дій персоналу до виходу з ладу обладнання.

- *Загрози доступності* (здійснення дій, що унеможливлюють чи утруднюють доступ до ресурсів інформаційної системи). Порушення

доступності є створення таких умов, при яких доступ до послуги або інформації буде або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

**2. За розташуванням джерела загроз:**

- ✓ *внутрішні* (джерела загроз розташовуються всередині системи);
- ✓ *зовнішні* (джерела загроз знаходяться поза системою).

**Внутрішні загрози**:

- ✓ виток інформації;
- ✓ неавторизований доступ.

**Зовнішні загрози**:

- ✓ шкідливі програми (віруси, трояни, черв'яки і т.п.);
- ✓ атаки хакерів;
- ✓ Ddos-атаки;
- ✓ таргінг атаки;
- ✓ спам;
- ✓ фішинг;
- ✓ промислові загрози (stuxnet, flame, duqu);
- ✓ шпигунське програмне забезпечення (spyware, adware);
- ✓ botnets (ботнети або зомбі-мережі).

**3. За розмірами завдання шкоди:**

- ✓ *загальні* (нанесення збитку об'єкту безпеки в цілому, заподіяння значної шкоди);
- ✓ *локальні* (заподіяння шкоди окремим частинам об'єкта безпеки);
- ✓ *приватні* (заподіяння шкоди окремим властивостям елементів об'єкта безпеки).

**4. За ступенем впливу на інформаційну систему**:

- ✓ *пасивні* (структура і зміст системи не змінюються);

✓ *активні* (структура і зміст системи піддається змінам).

**5. За природою виникнення**:

✓ *природні* (об'єктивні) – викликані впливом на інформаційне середовище об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини;

✓ *штучні* (суб'єктивні) – викликані впливом на інформаційну сферу людини. Серед штучних загроз в свою чергу виділяють:

– ненавмисні (випадкові) загрози – помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної і комунікаційної техніки;

– навмисні (умисні) загрози – неправомірний доступ до інформації, розробка спеціального програмного забезпечення, що використовується для здійснення незаконного втручання, розробка та поширення вірусних програм і т.і. Навмисні загрози обумовлені діями людей.

Основні проблеми інформаційної безпеки пов'язані, перш за все, з навмисними загрозами, так як вони є головною причиною злочинів і правопорушень.

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд і структуру як в процесі зберігання, так і після неодноразової передачі. Вносити зміни, видаляти або доповнювати інформацію вправі тільки власник або користувач з легальним доступом до даних.

*Конфіденційність* – характеристика, що вказує на необхідність обмеження доступу до інформаційних ресурсів для певного кола осіб. У процесі дій і операцій інформація стає доступною тільки користувачам, які включені в інформаційні системи і успішно пройшли ідентифікацію.

Доступність інформаційних ресурсів означає, що інформація, яка знаходиться у вільному доступі, надається повноправним користувачам ресурсів своєчасно і безперешкодно.

Достовірність вказує на приналежність інформації довіреній особі або власнику, який одночасно виступає в ролі джерела інформації.

Забезпечення і підтримка інформаційної безпеки включають комплекс різнопланових заходів, що запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи інформаційної безпеки спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово, щоби всі завдання вирішувалися одночасно – тільки тоді забезпечується повноцінний, надійний захист.

### *Класифікація вразливостей систем безпеки*

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об’єкті-носії.

Основні вразливості виникають внаслідок дії наступних факторів:

- ✓ недосконалість програмного забезпечення, апаратної платформи;
- ✓ різні характеристики будови автоматизованих систем в інформаційному потоці;
- ✓ частина процесів функціонування систем є неповноцінною;
- ✓ неточність протоколів обміну інформацією та інтерфейсу;
- ✓ складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливі і випадкові загрози через недостатні міри захисту і дії масового загрозливого фактору.

Існує поділ вразливостей за класами:

- об’єктивні;
- випадкові;
- суб’єктивні.

Якщо усунути або, як мінімум, послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему зберігання інформації.

Таким чином, класифікація погроз ІБ розподіляється за характером загрози, видом впливу, джерелом та об'єктом загрози.

Дослідники виділяють три основних види погроз безпеки:

- ✓ *загрози розкриття;*
- ✓ *загрози цілісності;*
- ✓ *загрози відмови в обслуговуванні.*

**Загроза розкриття** полягає в тому, що інформація стає відомою тому, кому не варто було б її знати. У термінах комп'ютерної безпеки загроза розкриття має місце щоразу, коли отриманий доступ до певної конфіденційної інформації, що зберігається в ІС, або передається від однієї системи до іншої.

**Загроза цілісності** включає будь-яку навмисну зміну (модифікацію або навіть видалення) даних, що зберігаються в ІС, або передаються з однієї системи до іншої. Зазвичай вважається, що загрозі розкриття піддаються більшою мірою державні структури, а загрозі цілісності – ділові або комерційні структури.

**Загроза відмови в обслуговуванні** виникає щоразу, коли в результаті деяких дій блокується доступ до певного ресурсу ІС. Реальне блокування може бути постійним, так щоб запитуваний ресурс ніколи не був отриманий, або блокування може викликати тільки затримку запитуваного ресурсу, досить тривалу для того, щоб він став непридатним. У таких випадках кажуть, що ресурс вичерпаний.

Крім того, пропонується наступна класифікація погроз ІБ [25]. Хоча єдиної й загальноприйнятої класифікації погроз ІБ не існує й, швидше за усе, не буде взагалі, тому що згодом з'являються нові загрози, які все складніше ідентифікувати.

Найпоширеніші dos атаки (відмова в обслуговуванні).

**1. Ping-of-Death**.

Посилає ICMP-пакет, розміром більше 64 Кб, що може призвести до переповнення буфера операційної системи і виведення системи, що атакується, з ладу.

**2. SYN Flood** .

Дуже швидко посилає велику кількість TCP SYN-пакетів (які ініціюють з'єднання), залишаючи жертву чекати величезну кількість з'єднань і викликаючи таким чином посилене завантаження ресурсів і відмову від санкціонованих з'єднань.

**3. Land/Latierra**.

Посилає підроблений SYN-пакет з ідентичними вихідною адресою та кінцевим портом так, що система рухається по нескінченній петлі, намагаючись виконати TCP-з'єднання.

**4. WinNuke**.

Посилає OOB/URG-дані для TCP-з'єднання із портом 139 (NetBIOS Session/SMB), що призводить до зависання ОС Windows. Найбільшому впливу піддається ОС Windows 95, пізніші версії ОС Windows мають проти цієї атаки відповідний захист.

**Найпоширеніші процеси сканування**

**1. Ping sweeps**.

Протягом цього простого процесу сканування діапазон IP-адрес аналізується утилітою **ping** (так зване пінгування) з метою визначення активних комп'ютерів. Слід зауважити, що більшість складних сканерів буде використовувати інші протоколи (такі, як SNMP sweep), щоб виконувати ту ж саму дію.

**2. TCP-сканування**.

Зондування відкритих TCP-портів у пошуках сервісів, які може використовувати порушник. Сеанси сканування можуть використовувати звичайні TCP-з'єднання або приховані (stealth) сеанси сканування, що

використовують наполовину відкриті з'єднання (для того, щоби захистити їх від реєстрації в журналах) або FIN-сеанси сканування (ніколи не відкривають порт, але тестують, якщо щось прослуховується). Сеанси сканування можуть бути послідовними або випадковими, або зконфігуровані за переліком портів.

**3. UDP-сканування**.

Ці сеанси сканування є складнішими, тому що (User Datagram Protocol) UDP- працює без встановлення віртуального з'єднання. Метод полягає в тому, щоби послати «сміттєвий» UDP-пакет до наміченого порту. Більшість машин будуть реагувати за допомогою ICMP-повідомлення «destination port unreachable», яке вказує, що на даному порту немає сервісу, який прослуховується. Однак багато комп'ютерів «поглинають» ICMP-повідомлення, тому ви не зможете здійснювати швидке UDP-сканування.

**4. Ідентифікація ОС**.

Шляхом посилання неприпустимих (або дивних) ICMP або TCP-пакетів порушник може ідентифікувати ОС. Стандарти зазвичай встановлюють, яким чином комп'ютери повинні реагувати на легальні пакети, тому машини мають тенденцію бути однаковими у своїй реакції на припустимі вхідні дані. Однак стандарти упускають (як правило навмисно) реакцію на неприпустимі вхідні дані. Таким чином, унікальні реакції кожної ОС на неприпустимі вхідні дані формують сигнатуру, яку хакери можуть використовувати для того, щоби зрозуміти, під чиїм управлінням функціонує обраний комп'ютер. Цей тип діяльності має місце на нижньому рівні (начебто прихованих сеансів TCP-сканування), на якому аналізовані системи не реєструють події.

## 1.3. Сучасні загрози

Носіями загроз інформаційній безпеці є джерела загроз, якими виступають як суб'єктивні (особистості), так і об'єктивні обставини (конкуренти, злочинці, корупціонери, адміністративно-управлінські органи, інше). Джерела загроз переслідують при цьому наступні цілі: ознайомлення з

відомостями які охороняють, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Всі джерела загроз інформаційній безпеці можна розділити на три основні групи.

**Обумовлені діями суб'єкта** (антропогенні джерела) – суб'єкти, дії яких призводять до порушення безпеки інформації, кваліфікуються як умисні або випадкові злочини.

Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми так і внутрішніми. Дані джерела можна зпрогнозувати, і вжити адекватних заходів.

**Обумовлені технічними засобами** (техногенні джерела) – ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Дані джерела загроз інформаційній безпеці, також можуть бути як внутрішніми, так і зовнішніми.

**Стихійні джерела** – дана група об'єднує обставини, що становлять непереборну силу (стихійні лиха або інші обставини, що неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти). Ці обставини, що носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню і, тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до інформаційних джерел що захищаються і під ними, як правило, розуміються природні катаклізми.

**Загроза безпеці комп'ютерної системи** – це потенційно можлива подія, незалежно від того, навмисна чи ні, що може здійснити небажаний вплив на саму систему, а також на інформацію, що зберігається в ній.

**Вразливість комп'ютерної системи** – це якась її невдала характеристика, що уможливлює виникнення загрози. Інакше кажучи, саме через наявність вразливостей у системі відбуваються небажані події.

**Атака на комп'ютерну систему** – це дія, що вчиняється зловмисником і полягає в пошуку й використанні загрози або іншої вразливості. Таким чином, атака – це реалізація загрози. Слід зауважити, що таке тлумачення атаки (за участю людини, яка має злий намір), виключає присутній у визначенні загрози елемент випадковості. Але, як показує досвід, часто буває неможливо розрізнити навмисні й випадкові дії, і надійна система захисту повинна адекватно реагувати на кожне з них.

Більш детально розглянемо особливості зовнішніх загроз.

**1. Хакерські атаки.**

Отримавши доступ до системи, вони направлені на крадіжку конфіденційних даних або встановлюють шкідливі програми та використовують "взламані" комп'ютери для розсилки спаму. В програми закрадаються помилки, що робить їх уразливими для атаки. Хакерам ці лазівки дозволяють проникнути в систему, а ті, хто пише віруси, використовують помилки в коді додатків, щоб забезпечити автоматичний запуск на комп'ютері шкідливих програм.

***Хакери*** – це електронні "взламники", які проникають в комп'ютерну систему, використовуючи особливі уразливі лазівки у програмному забезпеченні. Захиститися від них можна за допомогою особливого додатку – мережевого екрану з пакетною фільтрацією, що входить до складу антивірусних програм і робить комп'ютер невидимим для хакерів.

Для захисту від шкідливого коду і хакерських атак:

- ✓ встановлюється антивірусна програма;
- ✓ встановлюється оновлення ОС Windows (Update), що відповідає за безпеку;
- ✓ увага при роботі зі спамом в електронній пошті і системах миттєвих повідомлень;
- ✓ збереження резервної копії (BackUp) даних.

## 2. Технологія інфраструктури відкритих ключів.

Технологія інфраструктури відкритих ключів дозволяє перевіряти і засвідчувати справжність користувача. Інфраструктура відкритих ключів або PKI забезпечує єдину ідентифікацію, аутентифікацію і авторизацію користувачів системи, додатків і процесів і разом з цим гарантує доступність, цілісність і конфіденційність інформації. Інфраструктура PKI являє собою систему цифрових сертифікатів, носіями яких є USB-ключі або смарт-карти.

При використанні індивідуального секретного пароля і засобів криптографічного захисту, цифрові сертифікати отримують роль електронних паспортів. Використання в корпоративній мережі технології інфраструктури відкритих ключів значно підвищує безпеку всієї мережі в цілому, так як дозволяє відмовитися від використання парольної аутентифікації користувачів всередині, а також забезпечує безпечний доступ віддалених користувачів в систему. Основними носіями інформації є USB-ключі та смарт-карти. Користувачам не треба запам’ятовувати складні паролі і періодично їх міняти – досить підключити електронний ключ або смарт-карту і ввести PIN-код.

## 3. Системи одноразових паролів.

Системи багатофакторної аутентифікації засновані на технології одноразових паролів (one time password) OTP призначені для аутентифікації мобільних користувачів, які відрізняється простотою у використанні, установці і адмініструванні.

Дана технологія заснована на тому, що пароль користувача не постійний і змінюється з плином часу спеціальним пристроєм (апаратним або програмним) – токеном. Дане рішення широко використовується в системах віддаленого доступу, в тому числі системах клієнт-банк, для аутентифікації користувачів при доступі з недовірених середовища (Інтернет-кафе, бізнес-центри, і т.д.).

OTP-токен – мобільний персональний пристрій, що належить певному користувачеві і генерує одноразові паролі, які використовуються для

аутентифікації даного користувача. OTP-токени мають невеликий розмір і випускаються у вигляді: кишенькового калькулятора; брелока; смарт-карти; пристрою, комбінованого з USB-ключем; спеціального програмного забезпечення для кишенькових комп'ютерів. Як приклад рішень OTP, можна привести лінійку RSA SecurID, ActivCard Token, комбінований USB-ключ Aladdin eToken NG-OTP.

**Структура системи:**

- ✓ сервер аутентифікації (баз даних акаунтів, прив'язаних до пристроїв, синхронізація за часом);
- ✓ канал передачі;
- ✓ форма для введення аутентифікаційних даних (зазвичай три поля (Login, OTP, PIN));
- ✓ клієнтська частина (OTP брелок і ін.).

**4. Біометричні системи.**

***Біометричні системи*** – це вимірні фізіологічні або поведінкові дані людини. Біометричні дані унікальні для кожної людини і їх можна використовувати для встановлення особи або перевірки декларованих особистих даних:

- ✓ для ідентифікації користувача (замість введення імені користувача);
- ✓ для однофакторної аутентифікації користувача;
- ✓ спільно з паролем або аутентифікаційї токеном (таким, як смарт-карта) для забезпечення двофакторної аутентифікації.

Біометричні дані діляться на групи:

1. *Фізіологічні біометричні* характеристики – засновані на даних, отриманих шляхом вимірювання анатомічних характеристик людини, таких, як відбиток пальця, форма обличчя або кисті, сітківка ока.

2. *Поведінкові біометричні* характеристики (динамічні) – засновані на даних, отриманих шляхом вимірювання дій людини. Характерною рисою для

поведінкових характеристик є їх протяжність в часі – вимірюється дією, що має початок, середину і кінець. Наприклад, голос, підпис.

**5. Криптографічний захист даних.**

**Криптографія** – область знань, що вивчає тайнопис (криптографія) і методи його розкриття (криптоаналіз). Криптографія вважається розділом математики.

*Мета криптографічної системи* полягає в тому, щоби зашифрувати вихідний текст (шифртекст, криптограма).

Одержувач, якому він призначений, повинен бути здатний розшифрувати («дешифрувати») цей шифртекст, відновивши, таким чином, відповідний йому відкритий текст. При цьому зловмисник повинен бути нездатний розкрити вихідний текст.

Існує відмінність між розшифрування (дешифрованием) і розкриттям шифртексту. Широко відомим історичним прикладом криптосистеми є так званий шифр Цезаря, що представляє з себе просту заміну кожної букви відкритого тексту третьої наступної за нею буквою алфавіту (з циклічним перенесенням, коли це необхідно). Наприклад, «A» замінювалося на «D», «B» на «E», «Z» на «C».

*Всі методи шифрування поділяються на дві групи*:

- ✓ шифри з секретним ключем (симетрична схема);
- ✓ шифри з відкритим ключем (асиметрична схема).

Перший тип шифрів має на увазі наявність інформації (ключа), володіння якою дозволяє як зашифрувати, так і розшифрувати повідомлення. Шифри з відкритим ключем – відкритого і закритого типу; один використовується для шифрування, інший для розшифровки повідомлень.

*Основні напрямки шифрування*:

✓ шифрування даних на локальних дискових системах (клієнтське шифрування);

✓ криптографічний алгоритм (шифр) – математичний спосіб обробки інформації для приховування її змісту.

*Основні тенденції застосування шифрування*:

✓ шифрування окремих файлів;

✓ шифрування окремих розділів на жорсткому диску, віртуальних дисків;

✓ шифрування жорстких дисків цілком.

**6. Електронний підпис (ЕП).**

**Електронний підпис** – послідовність символів, отримана в результаті криптографічного перетворення вихідної інформації з використанням закритого ключа ЕЦП, яка дозволяє підтверджувати цілісність і незмінність цієї інформації, а також її авторство за умови використання відкритого ключа ЕП і його сертифіката.

**Цифровий підпис забезпечує:**

✓ вихідні джерела документа. Залежно від деталей визначення «документа» можуть бути підписані такі поля як автор, внесені зміни, мітка часу т.і.;

✓ захист від змін документа. При будь-якому випадковому або навмисному зміні документа (або підпису) зміниться хеш (хеш-функція або геш-функція – функція, що перетворює вхідні дані будь-якого розміру в дані фіксованого розміру), отже підпис стане недійсним;

✓ неможливість відмови від авторства. Так як створити коректний підпис можна лише знаючи закритий ключ, а він відомий тільки власнику, то власник не може відмовитися від свого підпису під документом.

Для підпису документа з початку обчислюється значення хеш-функції для документа, а потім це значення за спеціальним криптоалгоритмом підписується секретним ключем автора документа.

Для перевірки справжності документа необхідно за допомогою відкритого ключа перевірити підпис, потім обчислити його хеш-значення і

порівняти з підписаним контрольним підписом. Якщо обидва значення збігаються, то підпис вірний, інакше документ недійсний.

## 1.4. Інформаційні ризики

Сучасні системи спеціального призначення характеризуються наявністю в своєму складі інформаційних систем (ІС). Реалії часу диктують необхідність в умовах обмеженої можливості фінансування розробки ІС отримати оцінку розумної достатності захищеності таких ІС від ризиків. Класичне визначення ризику визначає його як комбінацію ймовірності події та її наслідків [ISO Guide 73: 2002]. Серед різновидів ризиків українські та зарубіжні автори виділяють операційний ризик відповідно до Базель III (Базель III - документ Базельського комітету з банківського нагляду, що містить методичні рекомендації в області банківського регулювання), що визначається ризиком прямих або непрямих втрат, джерелами яких можуть бути невідповідні або неправильно організовані внутрішні процеси, людські ресурси і системи або зовнішні події. Наслідком виникнення таких подій є зниження вірогідності, повноти та актуальності створюваної і інформації, що обробляється.

Отже, інформаційний ризик може бути визначений як різновид операційного ризику, що відбувається в результаті неадекватних і помилкових внутрішніх процесів, дій працівників або зовнішніх подій. Стандарт ISO27000: 2018 вказує: інформаційний ризик – це потенційна можливість того, що загроза буде використовувати уразливість активу або групи активів, завдаючи шкоди організації.

Ризик викликає інцидент інформаційної безпеки – одне або серія небажаних або несподіваних подій інформаційної безпеки, що мають значну ймовірність порушення бізнес-операцій або становлять загрозу для інформаційної безпеки [SO / IEC TR 15446: 2017]. Таким чином, приступаючи до аналізу інформаційних ризиків, необхідно визначити перелік об’єктів і їх

вразливостей, на які спрямовані атаки, реалізуючи загрози. Інформаційні ризики спрямовані на наступні види активів: інформація, мережеве, системне і прикладне програмне забезпечення, персональні комп'ютери, накопичувальні і друкувальні пристрої, мережеві сервера, шлюзи, інтерфейси, сервіси.

## 1.5. Витік інформації

Сьогодні більшість підприємств використовують багаторівневі системи обробки інформації – комп'ютери, хмарні сховища, корпоративні мережі і т. п. Всі ці системи не тільки передають дані, але і є середовищем їх можливого витоку. Витік секретної інформації – процес неконтрольованого розголошення ключових даних.

**Комерційна таємниця** – інформація про організацію діяльності підприємства, технології розробки продукції, дані про грошові потоки, інтелектуальна власність та інші відомості, володіючи якими отримуються фінансові вигоди.

**Причина 1 – Персонал**

Кожен співробітник підприємства є потенційною загрозою для безпеки інформації. Часто люди забирають роботу додому – переміщують робочі файли на свої флеш-носії, передають їх по незахищеним каналам з'єднання, обговорюють інформацію зі співробітниками конкуруючих компаній.

Дії персоналу бувають навмисними і ненавмисними. Ненавмисні дії – це наслідок незнання регламенту роботи з комерційною інформацією.

Ризик витоку інформації від персоналу є завжди, і його не можна виключити повністю. Служба безпеки може вжити заходів, щодо обмежень взаємодії працівників з конфіденційною інформацією та впровадити правила розмежування доступу.

Правила – перелік чітких прав і обмежень, що повинні дотримуватися кожним співробітником. Їх основний принцип – кожен працівник взаємодіє

тільки з тими даними, які потрібні для його роботи. Таким чином, простий менеджер не зможе дізнатися технологію розробки продукції та інші важливі дані, що бажає знати зловмисник.

Питаннями контролю роботи персоналу з секретними матеріалами повинен займатися уповноважений співробітник або відділ безпеки. Їхнє завдання це стежити за діяльністю працівників протягом усього робочого дня і оперативно виявляти всі випадки витоку інформації.

На практиці виявити людину, що зливає комерційну таємницю, можна за такими ознаками:

– *Співробітник без попередження затримується після роботи на своєму робочому місці.*

В такому випадку є ймовірність того, що він намагається отримати доступ до секретної інформації в момент, коли поруч нікого немає.

На такого працівника потрібно звернути увагу і простежити, чи не є його метою дізнатися таємні відомості. Контролювати час перебування персоналу на робочому місці допомагають спеціальні системи обліку доступу. Починати розслідування потрібно лише в тому випадку, якщо стали відомі конкретні факти витоку інформації, що захищається.

– *Співробітник зберігає на свій персональний комп'ютер або смартфон занадто багато електронних документів компанії.*

Такий варіант витоку можна відстежити в компаніях, що використовують системи захисту файлової системи. Суть їх роботи полягає в створенні загального сервера, що діє в рамках однієї корпоративної або Wi-Fi-мережі. Під час кожного відкриття, копіювання та переміщення даних на службовому комп'ютері вся інформація про процеси надходить на сервер. Таким чином, адміністратор безпеки може виявити, з якого комп'ютера і в якій кількості була переміщена секретна інформація.

– *Співробітник без необхідності копіює паперовий документообіг електронним (сканує документи або фотографує).*

Згідно з нормами документування, все фізичні папки і файли з комерційною таємницею повинні зберігатися в захищеній частині архіву. Доступ до документів можливий тільки для уповноважених працівників. Всі дані про отримання документа з таємницею для користування повинні документуватися (із зазначенням імені працівника і точного часу видачі документа).

Якщо ж секретний документ потрапив в руки недобросовісного співробітника, відстежити його несанкціоноване копіювання можна на сканері або ксероксі, що зберігає звіт щодо діяльності за останній час. Також існують факсимільні апарати, доступ до яких можливий тільки після правильного введення пари «ідентифікатор користувача-пароль».

– *Працівник регулярно порушує загальні вимоги безпеки при роботі з комерційною таємницею.*

Якщо персонал регулярно намагається обійти систему заборони, переглядаючи заборонені ресурси, або використовує особисту техніку для обробки секретних даних, необхідно впровадити додаткові системи контролю користувачів. Наприклад, DLP-системи. Їх завдання полягає в моніторингу всіх листувань користувачів з комерційної пошти та інших електронних скриньок, які зареєстровані в системі. Також модуль захисту забороняє установку стороннього ПЗ, а всі дії співробітника за комп’ютером видно адміністратору безпеки.

– *Співробітник був викритий в контактах із службовцями конкуруючих компаній.*

У великих компаніях працівники часто спілкуються поза робочим часом. Таким чином, вони отримують більше інформації один про одного і можуть дізнатися про зв’язки колеги і працівника конкуруючої організації. Ймовірність звичайних дружніх відносин між людьми теж можлива, але краще оповістити керівництво компанії про це, щоб уникнути непотрібних підозр.

**Причина 2 – Проблеми підбору кадрів**

Часта зміна персоналу, масштабні зміни в організації роботи компанії, зниження заробітних плат, скорочення співробітників – все це є частиною «плинності» кадрів. Таке явище часто стає причиною витоку секретної інформації.

Криза, нестача коштів для видачі зарплат змушують керівництво погіршувати умови роботи персоналу. В результаті підвищується невдоволення працівників, які можуть звільнитися або ж просто почати поширювати секретні дані конкурентам. Проблема зміни персоналу особливо важлива для керівних посад, адже всі керуючі повинні мати доступ до секретної документації.

Загрозу поширення таємниці можуть нести не тільки ті співробітники, які звільнилися, але і поточні працівники, рівень мотивації яких знижений.

Для запобігання проблеми слід створити для працівників максимально комфортні умови роботи. У разі серйозної кризи рекомендується зібрати персонал для обговорення можливих шляхів виходу зі складної ситуації. Важливо повідомляти співробітників про всі зміни в нарахуванні заробітних плат заздалегідь, а не за фактом виплати окладу.

Часом несприятливу атмосферу в колективі створює один співробітник. Встановлення систем автоматизованого профайлингу які аналізують листування працівників в електронній пошті і месенджерах та створюють їх психологічні портрети. Система визначає позитивні і негативні сторони характеру людини, що дозволяє приймати вірні управлінські рішення.

***Для усунення «плинності» працівників важливо виконувати наступні рекомендації:***

– *Налагодити систему найму кадрів.*

Всі передові організації мають спеціальний відділ, що займається питаннями найму, звільнення і підтримки співробітників. Не слід шукати працівника на вакансію, що звільнилася або з'явилась якомога швидше. Хороший HR (фахівець з підбору кадрів Human resources) зобов’язаний

прослухати кілька претендентів на посаду, поширити інформацію про вільну вакансію на популярних Інтернет-майданчиках, провести підсумковий конкурс, результати якого визначать кандидатуру, яка найбільше підходить.

– *Впровадження системи винагород.*

За успіхи в роботі, перевиконання планів і укладення вигідних контрактів співробітників потрібно заохочувати. Прикладами заохочення можуть бути підвищення заробітної плати, покращення умов роботи, просування по кар'єрним сходах.

– *Надання всім співробітникам можливості професійного зростання, підвищення кваліфікації.*

Хороші компанії завжди відправляють своїх співробітників на курси підвищення кваліфікація або ж закуповують онлайн-тренінги для більш зручного проходження навчання. Також рекомендується організовувати тренінги від провідних професіоналів галузі.

**Причина 3 – Відрядження**

Робочий процес фірми включає ділові зустрічі, поїздки в інші філії компанії, країни. Співробітники, які часто виїжджають у відрядження, можуть ненавмисно стати основною причиною витоку секретної інформації підприємства.

У поїздці такий працівник завжди має при собі особистий або корпоративний ноутбук/смартфон, що обробляє захищені документи. Техніка може бути залишена в громадському місці, зламана або викрадена. Якщо за співробітником ведеться стеження або ж він зустрічається з керівниками конкуруючої компанії, загублений ноутбук може стати головним джерелом розголошення службової інформації.

Для запобігання подібних випадків важливо використовувати системи шифрування жорсткого диска тих ПК, що видаються співробітникам на час ділових зустрічей. Навіть в результаті крадіжки і несанкціонованого доступу

інформація буде надійно захищена, і зламати її, без знання ключа, буде неможливо.

**Причина 4 – Співпраця з іншими компаніями**

Більшість автоматизованих систем захисту здатні обмежити доступ до службової інформації тільки в рамках однієї будівлі або одного підприємства (якщо кілька філій використовують загальний сервер зберігання даних).

У процесі спільного виконання проєкту декількома фірмами, служби безпеки не можуть в повній мірі простежити за тим, як реалізується доступ до службової таємниці кожного з підприємств.

Як і в попередньому випадку, використання криптоконтейнера (систем шифрування жорсткого диска) дозволить захистити таємну інформацію від злому.

**Причина 5 – Використання складних IT-інфраструктур**

Великі корпорації використовують комплексні системи захисту службових відомостей. Автоматизовані системи мають на увазі наявність декількох відділів безпеки і роботу понад п’яти системних адміністраторів, завдання яких полягає тільки в підтримці збереження комерційної таємниці.

Складність системи теж є ризиком витоку, адже одночасна робота кількох людей може бути незлагодженою. Наприклад, один адміністратор може впровадити або видалити правила розмежування доступу, а інший – забути внести дані прав доступу до серверів.

При використанні складних систем захисту інформації важливо грамотно розподіляти всі обов’язки і контролювати їх своєчасне виконання. В іншому випадку – створена система може нашкодити компанії.

Наприклад, можна розмежувати доступ співробітників служби безпеки до певних звітів і операцій в системі. Максимальне число повноважень надійніше довірити керівнику ІБ-служби.

**Причина 6 – Поломки техніки**

***Помилки в роботі ПЗ***

Всілякі збої в роботі програмного забезпечення виникають постійно. В момент появи уразливості захищені файли ризикують стати перехопленими хакером. Важливо вчасно виявляти всі неполадки в роботі встановлених програмних і апаратних компонентів. За працездатність і взаємодію всіх модулів захисту відповідальний адміністратор безпеки.

В результаті збою в базі даних втрачається значна кількість важливої документації. Відновлення жорстких дисків – це складне завдання, що не дає гарантії повернення втрачених відомостей.

***Збої в роботі серверного обладнання***

Безпечніше зберігати всю інформацію з використанням хмарних сховищ. Cloud-платформи підвищують швидкість обробки інформації. З їх допомогою кожен співробітник зможе отримати доступ до потрібних файлів з будь-якого пристрою. Система шифрування використовується віддаленим сервером, тому немає необхідності захищати канали передачі.

Збої на серверах постачальника послуг можуть траплятися через природні катаклізми або через масивні хакерські атаки. Як правило, власники хмарних платформ завжди зберігають архівовані резервні копії вмісту акантів користувачів, тому збої швидко вилучаються без втрати важливих документів.

***Поломка технічних засобів захисту***

Для збереження комерційної таємниці рекомендується захищати не тільки операційні системи і гаджети, але і весь периметр офісного приміщення, а також зону контролю вуличних комунікацій. Для цих цілей використовуються заглушки на вікна, ущільнювачі архітектурних конструкцій (для запобігання прослуховувань), пристрої для екранування і зашумлення (для неможливості перехоплення радіохвиль), інші гаджети.

Через поломку одного з таких пристроїв виникає канал витоку інформації, що стає доступним зловмисникові для перехоплення секретних даних.

У разі поломки комп'ютерів і інших засобів обробки даних, їх необхідно відремонтувати в сервісному центрі. Винос гаджета за межі приміщення і передача його сторонній людині (навіть якщо він не зацікавлений в отриманні службової таємниці) є можливою причиною витоку. Департамент безпеки компанії не може контролювати гаджети, поки вони знаходяться за межами фірми.

**Причина 7 – Витік з технічних каналів передачі даних**

**Канал витоку даних** – це фізичне середовище, всередині якого не контролюється поширення таємної інформації. На будь якому підприємстві, що використовує комп'ютери, серверні стійки, мережі, є канали витоку. З їх допомогою зловмисник може отримати доступ до комерційної таємниці.

***Існують наступні канали витоку:***

**Мовний.** Конкуренти часто використовують прослуховувачі та інші закладки, за допомогою яких відбувається крадіжка таємниці.

**Віброакустичний.** Цей канал витоку виникає в процесі зіткнення звуку з архітектурними конструкціями (стінами, підлогою, вікнами). Вібраційні хвилі можна зчитати і перевести в мовної текст. За допомогою спрямованих мікрофонів на відстані до 200 метрів від приміщення зловмисник може зчитати розмову, в якій фігурує службова інформація.

**Електромагнітний.** В результаті роботи всіх технічних засобів виникає магнітне поле. Між апаратними елементами передаються сигнали, що можна вважати спеціальним обладнанням на великих відстанях і отримати секретні дані.

**Візуальний.** Приклад появи візуального каналу крадіжки – це проведення нарад і конференцій з неприкритими вікнами. З сусіднього будинку зловмисник

може легко переглянути всю інформацію. Також можливі варіанти використання відеозакладок, які передають картинку того, що відбувається конкурентам.

***Для захисту технічних каналів витоку рекомендується використовувати:***

- *Тепловізор. З*а допомогою такого девайса можна просканувати всі стіни і частини інтер'єру на наявність закладних пристроїв (жучків, відеокамер).
- *Пристрої, що заглушають подачу сигналу радіочастот*.
- *Засоби захисту архітектурних конструкцій* – ущільнювачі для вікон, дверей, підлоги і стелі. Вони ізолюють звук і унеможливлюють зчитування вібраційних хвиль з поверхні будівлі.
- *Пристрої для екранування і зашумлення.* Вони використовуються для захисту електромагнітного каналу витоку.

Також слід заземлити всі комунікації, що виходять за межі приміщення і контрольованої зони (труби, кабелі, лінії зв'язку).

Існує кілька дієвих способів, що допоможуть знизити ризик витоку і розголошення інформації. Підприємство може використовувати всі методи захисту або тільки кілька з них, адже система безпеки повинна бути економічно вигідною. Збитки від втрати секретної інформації не можуть бути менше вартості впровадження та підтримки системи безпеки.

**Шифрування.** *Шифрування* – це простий і дієвий метод захисту комерційної таємниці. Сучасні алгоритми шифрування використовують світові стандарти в області криптографії (шифри AES, ГОСТ), двосторонній обмін ключами (з його допомогою хакер не зможе зламати шифр навіть після отримання доступу до каналу передачі), еліптичні криві для генерації захисту. Такий підхід робить злом шифрованого повідомлення неможливим для стандартних комп'ютерів.

Переваги використання шифрування з метою запобігання витоку комерційної інформації:

*Простота застосування.* Реалізація шифрування проводиться спеціальним ПЗ. Програма повинна бути встановлена на всі комп'ютери і мобільні пристрої, в яких циркулює секретна інформація. Роботу додатка налаштовує системний адміністратор або адміністратор безпеки. Таким чином, звичайному користувачеві автоматизованих систем не потрібно вчитися використовувати систему захисту. Всі файли шифруються і дешифруються автоматично в рамках корпоративної мережі.

У разі необхідності передачі важливих електронних документів за межі комерційної мережі вони будуть зберігатися на флеш-носії, хмарному носії або в клієнтській пошті виключно в зашифрованому вигляді. Недолік – без спеціального ПЗ працівник не зможе переглянути вміст файлу.

*Високий ступінь надійності.* З використанням потужних обчислювальних алгоритмів криптографії зловмисникові складно перехопити секретні повідомлення або трафік фірми, а розшифровка, без знання відкритого і закритого ключа, неможлива.

Відзначимо, що шифрування є не єдиним варіантом захисту таємниці від всіх можливих атак. Працівники здатні без проблем прочитати вміст електронних документів в рамках комерційної мережі, тому ризик несанкціонованого розголошення третім особам залишається. Використання криптографії є невід'ємною частиною функціоналу кожної комплексної системи безпеки.

**Контроль персоналу**

Якщо технічні засоби легко контролювати, то персонал є одним з найнебезпечніших джерел витоку. Людський фактор присутній завжди, і навіть співробітники відділу безпеки не завжди можуть встановити, від якого працівника може виходити загроза.

Як правило, пошук зловмисника серед персоналу виконується вже тоді, коли стали відомі перші випадки передачі даних конкурентам. Адміністратори безпеки перевіряють можливість перехоплення інформації технічними

каналами витоку, і, якщо всі канали надійно захищені, підозра падає на працівників.

Діяльність співробітників організації контролюється за допомогою систем обліку робочого часу. Це комплексне апаратне і програмне забезпечення, що документує точний час прибуття на роботу, час догляду, діяльність персоналу за комп'ютером, записує листування корпоративної пошти, проводить відеоспостереження і передає всі ці дані керівництву фірми або керівнику відділу безпеки. Далі вся отримана інформації аналізується і виявляється число працівників, які могли поширювати комерційну таємницю.

**Норми документування та передачі комерційної таємниці**

Захищати треба не тільки електронні документи, а й всю друковану документацію, що містить секретні відомості. Відповідно до Закону "Про зберігання і обробку відомостей, що містять комерційну таємницю", слід виконувати такі вимоги:

- Зберігати всі документи з комерційною таємницею виключно в окремих закритих приміщеннях, що охороняються цілодобово системами відеоспостереження або охоронцями.
- Доступ до службової таємниці можуть мати тільки співробітники, яким вона потрібна в процесі роботи.
- Запис про вилучення документа з архіву вноситься до реєстраційного журналу. Вказується точна дата, гриф документа та ініціали особи, яка здобула копію файлу. Аналогічні дії проводяться при поверненні об'єкта.
- Документ, що містить комерційну таємницю, не можна виносити за межі офісу без повідомлення про це керівника департаменту безпеки.
- Для передачі таємних документів між філіями підприємства використовується фельд'єгерська пошта – захищена кур'єрська передача документів особливої важливості.

**Контрольні запитання**

1. Поняття інформаційної безпеки.
2. Основні завдання інформаційної безпеки.
3. Фактори обумовлення інформаційних загроз.
4. Приклади внутрішніх загроз безпеці інформації.
5. Приклади зовнішніх загроз безпеці інформації.
6. Що таке хакерські атаки? Приклади.
7. Методи захисту від хакерських атак.
8. Що таке технологія інфраструктури відкритих ключів?
9. Особливість системи багатофакторної аутентифікації.
10. Особливість біометричних систем. Приклади.
11. Суть біометричного захисту даних.
12. Методи криптографічного захисту даних.
13. Призначення електронного підпису.
14. Аутентифікація та ідентифікація.

# ТЕМА 2. ІНФОРМАЦІЙНА СИСТЕМА ПЕРСОНАЛЬНИХ ДАНИХ

## 2.1. Нормативні документи захисту даних

В Україні розроблено і впроваджено наступні законодавчі та нормативні документи щодо захисту інформації, технічного захисту інформації, захисту персональних даних, електронного цифрового підпису, технічного захисту інформації:

- Закон України «Про захист персональних даних»;
- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України “Про телекомунікації”;
- Закон України «Про ліцензування видів господарської діяльності»;
- Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 №1126;
- Постанова Кабінету Міністрів України від 25.05.2011 №616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення»;
- Постанова Кабінету Міністрів України від 29.10.00 №1755 «Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу».
- Постанова Кабінету Міністрів України від 16.11.2016 №821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового

підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України».

- Постанова Кабінету Міністрів України від 21.06.17 №437 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації».
- Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 №1229.
- Постанова Кабінету Міністрів України від 13.03.02 №281 «Про деякі питання захисту інформації, охорона якої забезпечується державою».
- Постанова Кабінету Міністрів України від 29.03.06 №373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».
- Постанова Кабінету Міністрів України від 12.04.02 №522 «Порядок підключення до глобальних мереж передачі даних».
- Положення про порядок надання відомостей з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців, затверджено Наказом Державного комітету України з питань регуляторної політики та підприємництва 20.10.2005 №97, Зареєстровано в Міністерстві юстиції України 28 жовтня 2005 р. за №1294/11574.
- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 №93, зареєстровано в Міністерстві юстиції України 16.07.07 за №820/14087.

- Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 №87, зареєстровано в Міністерстві юстиції України 10.07.07 за №785/14052.
- Правила проведення робіт із сертифікації засобів захисту інформації, затверджені наказом Держспоживстандарту та Адміністрації Держспецзв'язку від 25.04.07 №75/91 та зареєстровані у Мін`юсті 14.05.07 №498/13765.
- Порядок формування реєстру організаторів державної експертизи у сфері технічного захисту інформації та реєстру експертів з питань технічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.04.08 №64.
- Порядок оновлення антивірусних програмних засобів, що мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 26.03.07 №45.
- Тимчасове положення про категоріювання об'єктів від 10.07.95 №35.
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації захисту інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
- НД ТЗІ 2.5-010-2003 Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу.
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі зміною №1, затвердженою наказом ДСТСЗІ СБ України 18.06.02 №37).
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
- НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
- НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
- НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації.

- НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

**В законі України “Про інформацію”** від 02.10.92 р. № 2657-XII (остання редакція від 21.12.2019) [34] визначаються основні терміни та положення про інформацію, який регулює відносини щодо створення, збирання, отримання, зберігання, використання, поширення, охорони, захисту інформації. Розглянемо такі основні 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, що 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 отримання, 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 громадянина до інформації;

– забезпечення рівних можливостей щодо створення, збирання, отримання, 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 громадянин має право на інформацію, що передбачає можливість вільного отримання, 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, що 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, отримані в результаті науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Правовий режим науково-технічної інформації визначається Законом України «Про науково-технічну інформацію», іншими законами та міжнародними договорами України, згода 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.

**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, 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 «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.

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"** №80/94-ВР від 05.07.1994 р., чинний (остання редакція від 19.04.2014) [35].

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;

– **власник 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 в 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 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 зі 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, що забезпечують банківську діяльність, встановлюються Національним банком України.

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

*Державний стандарт України* ДСТУ 3396.0-96 чинний від 01.01.1997 р. включає:

– захист інформації;

– технічний захист інформації;

– основні положення.

Цей стандарт встановлює об'єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин

усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

**Закон України Про криптографічний та технічний захист інформації.** Цей Закон визначає правові та організаційні засади криптографічного та технічного захисту важливої для держави, суспільства і особи інформації, що обробляється або озвучується на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, охорона якої забезпечується державою відповідно до законодавства, регулює відносини між суб’єктами у цій сфері.

## 2.2. Конфіденційність персональних даних

Необхідність забезпечення безпеки персональних даних в наш час – об’єктивна реальність. Сучасна людина не може самостійно протидіяти посяганню на його приватне життя. Підвищені технічні можливості щодо збору та обробки персональної інформації, розвиток засобів електронної комерції і соціальних мереж роблять необхідним вжиття заходів щодо захисту персональних даних.

Розглянемо декілька прикладів з повсякденного життя, коли порушуються права людини на конфіденційність персональних даних. Буває так, що при оформленні дисконтної картки в магазині покупець вказує такі відомості: прізвище, номер телефону, електронна адреса, а потім отримує повідомлення і листи абсолютно з інших магазинів, в яких навіть ніколи не бував. Тобто магазин, без згоди покупця, передав його дані третім особам. Якщо газета друкує ПІБ і суми виграшу переможців лотереї без їх відома, чи об'єднання співвласників багатоквартирного будинку вивішує на під’їзді списки боржників і суму їх боргу – це приклади «нешкідливих» витоків. Крадіжка персональних даних може завдати правовласнику відчутної

матеріальної шкоди, якщо мова йде про кредитні картки або інформацію про банківські заощадження. Зловмисники, які володіють достатніми технічними знаннями, викрадають реквізити банківських карт (скімінг) або імітують сайти фінансових установ, щоби змусити користувача показати свою особисту інформацію (фішинг). Насправді, часто навіть важко встановити джерело витоку персональних даних внаслідок високої інформатизації сучасного суспільства.

Держава на законодавчому рівні вимагає від організацій та фізичних осіб, які обробляють персональні дані, забезпечити їх захист. Законодавство України в області захисту персональних даних ґрунтується на Конституції України, міжнародних договорах України, Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та інших нормативних документах.

Метою Українського законодавства у сфері захисту персональних даних є забезпечення захисту прав і свобод громадянина при обробці його персональних даних, в тому числі захисту прав на недоторканність приватного життя, особисту і сімейну таємницю. Законодавством регулюються відносини, пов’язані з обробкою персональних даних, що здійснюється державними органами влади, органами місцевого самоврядування, юридичними особами та фізичними особами.

Відповідно до Закону, персональні дані – будь-яка інформація, за допомогою якої можна однозначно ідентифікувати фізичну особу. До персональних даних відносяться: прізвище, ім’я, по батькові; рік, місяць, дата і місце народження; адреса; сімейний, соціальний, майновий стан; освіта, професія, доходи, інша інформація, що належить суб’єкту.

Операторами персональних даних є державний орган, юридична або фізична особа, які організують і (або) здійснюють обробку персональних даних, а також визначають цілі і зміст обробки персональних даних.

**Обробка персональних даних** – дії (операції) з персональними даними, включаючи збір, систематизацію, накопичення, зберігання, уточнення (оновлення, зміну), використання, поширення (в тому числі передачу), знеособлення, блокування, знищення персональних даних.

**Інформаційна система персональних даних** (далі ІСПД) – інформаційна система, що представляє собою сукупність персональних даних, що містяться в базі даних, а також інформаційних технологіях і технічних засобах, що дозволяють здійснювати обробку таких персональних даних з використанням засобів автоматизації або без використання таких засобів [7].

Регуляторами називаються органи державної влади, уповноважені здійснювати заходи щодо контролю і нагляду щодо дотримання вимог закону України «Про захист персональних даних».

Україна в питанні захисту персональних даних спирається на міжнародний досвід. Але в державі поки немає достатньої законодавчої бази і системи, здатної ефективно працювати в сучасних умовах.

## 2.3. Захист персональної інформації

***1. Правові засади захисту персональних даних.***

У 2005 році Україна ратифікувала Конвенцію 1981 року Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Серед основних зобов'язань держави за зазначеним документом є також прийняття нормативно-правових актів, що повинні сприяти захисту персональних даних. У зв'язку з цим Верховною Радою України 01.06.2010 року прийнято Закон України «Про захист персональних даних», що визначив:

- поняття персональних даних – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована (наприклад: інформація про працівника є базою персональних даних, оскільки

особиста справа, трудові книжки, копії паспорта, документів про освіту зберігаються та обробляються роботодавцем);

- поняття власник бази персональних даних – фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних; яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедуру їх обробки, якщо інше не визначено законом;

- поняття розпорядник бази персональних даних – фізична або юридична особа, яка є власником бази персональних даних, або за законом має право обробляти ці дані;

- необхідність реєстрації бази персональних даних в Державному реєстрі баз персональних даних;

- вимоги до обробки персональних даних власника та розпорядниками баз персональних даних, як загальні вимоги до організаційних та технічних заходів із захисту персональних даних під час їх обробки в базі персональних даних (згода суб'єкта персональних даних, порядок використання і поширення персональних даних та порядок доступу до персональних даних третіх осіб та ін.);

- необхідність контролю за дотриманням законодавства про захист персональних даних,

- відповідальність за порушення законодавства про захист персональних даних.

З метою забезпечення виконання громадянами, органами державної влади та місцевого самоврядування, підприємствами, установами, організаціями, незалежно від форм їх власності, вимог Закону України «Про захист персональних даних» Верховною Радою України:

- прийнято Закон України «Про внесення змін до деяких законодавчих актів в Україні щодо посилення відповідальності за порушення законодавства про захист персональних даних» № 3454-VI від 2 червня 2011 року;

- внесено зміни до Кодексу України про адміністративні правопорушення.

*2. Реєстрація баз персональних даних.*

2.1. База персональних даних підлягає державній реєстрації шляхом внесення відповідного запису уповноваженим державним органом з питань захисту персональних даних до Державного реєстру баз персональних даних.

2.2. Реєстрація баз персональних даних здійснюється за заявочним принципом шляхом повідомлення.

2.3. Заявка про реєстрацію бази персональних даних подається власником бази персональних даних до уповноваженого державного органу з питань захисту персональних даних.

Заявка повинна містити:

- звернення про внесення бази персональних даних до Державного реєстру баз персональних даних;

- інформацію про власника бази персональних даних;

- інформацію про найменування і місцезнаходження бази персональних даних;

- інформацію про мету обробки персональних даних у базі персональних даних;

- інформацію про інших розпорядників бази персональних даних;

- підтвердження зобов'язань щодо виконання вимог захисту персональних даних, встановлених законодавством про захист персональних даних.

2.4. Уповноважений державний орган з питань захисту персональних даних в порядку, затвердженому Кабінетом Міністрів України,:

- повідомляє заявнику не пізніше наступного робочого дня з дня надходження заявки про її отриманні;

- приймає рішення про реєстрацію бази персональних даних протягом десяти робочих днів з дня надходження заявки.

Власник бази персональних даних видається документ встановленого зразка про реєстрацію бази персональних даних в Державному реєстрі баз персональних даних.

2.5. Уповноважений Державний орган з питань захисту персональних даних відмовляє в реєстрації бази персональних даних, якщо заявка про реєстрацію не відповідає встановленим вимогам.

2.6. Власник бази персональних даних зобов'язаний повідомляти уповноважений державний орган з питань захисту персональних даних про кожну зміну відомостей, необхідних для реєстрації відповідної бази, не пізніш як протягом десяти робочих днів з дня настання таких змін.

2.7. Уповноважений Державний орган з питань захисту персональних даних протягом десяти робочих днів з дня надходження повідомлення про зміну відомостей, необхідних для реєстрації відповідної бази, повинен прийняти рішення щодо зазначених змін і повідомити про це власнику бази персональних даних.

*3. Порядок обробки персональних даних у базах персональних даних.*

3.1. Порядок обробки персональних даних встановлює загальні вимоги до організаційних та технічних заходів захисту персональних даних під час їх обробки у базах персональних даних власниками та розпорядниками баз персональних даних. Обробка персональних даних може здійснюватися повністю або частково в інформаційній (автоматизованій) системі та / або у формі картотеки персональних даних.

3.2. Захист персональних даних покладається на власника бази персональних даних. Розпорядник бази персональних даних здійснює обробку персональних даних відповідно до закону або на підставі укладеного з власником бази персональних даних договору в письмовій формі з метою і в обсязі, визначеними договором. На дії власника і / або розпорядника бази персональних даних поширюються усі вимоги щодо захисту персональних даних від незаконної обробки, а також від незаконного доступу до них.

3.3. Власник або розпорядник бази персональних даних дає суб'єкту персональних даних інформацію про мету обробки персональних даних до моменту отримання згоди від суб'єкта персональних даних.

3.4. Власник бази персональних даних зберігає персональні дані у строк не більше, ніж це необхідно, відповідно до мети їх обробки, якщо інше не передбачено законодавством.

3.5. Власник бази персональних даних визначає:

- мету обробки, склад персональних даних у базі персональних даних та її місцезнаходження;

- порядок внесення змін, оновлень, використання, поширення, знеособлення, знищення персональних даних у базі персональних даних;

- відповідальну особу або структурний підрозділ;

- порядок захисту персональних даних, в тому числі від незаконної обробки та незаконного доступу до них.

3.6. Відповідальна особа або структурний підрозділ відповідно до покладених завдань:

- забезпечує ознайомлення працівників власника і розпорядника бази персональних даних з вимогами законодавства про захист персональних даних, зокрема щодо їхнього обов'язку не допускати розголошення будь-яким способом персональних даних, що їм були довірені, або що стали їм відомі у зв'язку з виконанням службових, професійних чи трудових обов'язків;

- забезпечує організацію обробки персональних даних працівниками власника і розпорядника бази персональних даних відповідно до їх професійних, службових або трудових обов'язків в обсязі, необхідному для виконання таких обов'язків;

- організовує роботу з обробки запитів щодо доступу до персональних даних суб'єктів відносин, пов'язаних з обробкою персональних даних;

- забезпечує доступ суб'єктів персональних даних до власних персональних даних;

- інформує керівника власника і розпорядника бази персональних даних про заходи, необхідні для приведення складу персональних даних та процедури їх обробки у відповідність до закону;

- інформує керівника власника і розпорядника бази персональних даних про порушення встановлених процедур з обробки персональних даних.

3.7. Власник бази персональних даних веде облік:

- фактів надання та позбавлення працівників права доступу до персональних даних та їх обробки;

- спроб і фактів несанкціонованих та / або незаконних дій з обробки персональних даних.

3.8. Власник бази персональних даних може розмежувати режими доступу працівників до обробки персональних даних в базі персональних даних відповідно до їх професійними, трудовими чи службовими обов'язками.

3.9. Знищення персональних даних здійснюється способом, що виключає подальшу можливість поновлення цих персональних даних.

3.10. Власник бази персональних даних обробляє персональні дані в складі інформаційної (автоматизованої) системи, в якій забезпечується захист персональних даних від незаконної обробки, а також від незаконного доступу до них відповідно до вимог закону України «Про захист персональних даних»

та відповідно до вимог нормативно-законодавчих актів з питань технічного захисту інформації.

*4. Забезпечення захисту персональних даних в інформаційній (автоматизованій) системі.*

4.1. Власник бази персональних даних повинен створити умови для захисту в інформаційній (автоматизованій) системі персональних даних і забезпечити захист цих персональних даних від незаконної обробки, а також від незаконного доступу до них.

4.2. Умови для захисту персональних даних залежать від конкретних реальних загроз, природи персональних даних, що обробляються, технології обробки інформації і типу інформаційної системи, в рамках якої обробляються персональні дані.

4.3. Забезпечення умов для захисту в інформаційній (автоматизованій) системі персональних даних не вирішується реалізацією певної сукупності заходів, а це постійний процес, який включає:

- розробку політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них, виходячи з характеристик діяльності організації, цілей, процесів і процедур, істотних для управління ризиком небажаних подій щодо обробки персональних даних з урахуванням серйозності наслідків таких небажаних подій. Політика захисту персональних даних від незаконної обробки, а також від незаконного доступу до них, повинна бути узгоджена з загальною політикою інформаційної безпеки організації і з контекстом стратегічного управління ризиками організації;

- впровадження політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них і забезпечення функціонування заходів, процесів і процедур захисту персональних даних;

- оцінювання та, по можливості, вимір продуктивності процесів захисту персональних даних відповідно до прийнятої політики, цілям і практичного досвіду, підготовка пропозицій щодо коригуючих заходів;

- вживання коригувальних і запобіжних дій щодо захисту персональних даних на підставі результатів внутрішніх перевірок, періодичний перегляд політики захисту персональних даних, постійне вдосконалення заходів;

4.4. У разі, коли обробка персональних даних здійснюється в інформаційній (автоматизованій) системі, створюється комплексна система захисту інформації відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 р №373.

4.5. Комплексна система захисту інформації забезпечує захист персональних даних від незаконної обробки, а також від незаконного доступу до них, відповідно до плану захисту інформації в системі, що містить:

- завдання захисту персональної інформації, класифікації персональної інформації, опис особливостей технології обробки інформації;

- модель загроз для персональних даних в системі;

- вимоги щодо захисту персональних даних та правила доступу до них;

- перелік документів, згідно з якими здійснюється захист інформації в інформаційній системі.

4.6. Для захисту персональних даних важливо, щоби організаційні заходи і використовувані засоби захисту, що визначають рівень захисту, відповідали реальним конкретним загрозам, даних, що обробляються, і процесам, обробки даних, що виконуються. Повинні братися до уваги ймовірні ризики небажаних подій і серйозність наслідків таких небажаних подій. Чим вище ризики, тим суворіші заходи захисту повинні бути реалізовані.

4.7. Якщо обробка персональних даних здійснюється в інформаційній (автоматизованій) системі, в якій створюється комплексна система захисту інформації, оцінка ризиків небажаних подій для персональних даних, що обробляються в автоматизованій системі, є складовою частиною оцінки ризиків відповідно до рекомендацій згідно з нормативним документом НД ТЗІ 1.1- 002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу". Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 №22.

4.8. До основних факторів, що впливають на рівень необхідного захисту, відносяться:

- увага, що приділяється суспільством до оброблюваних даних;

- рівень поінформованості персоналу власника та / або розпорядника бази персональних даних щодо інформаційної безпеки, захисту персональних даних, поваги до авторських прав, тощо;

- тип інформаційно-телекомунікаційної системи, в рамках якої обробляються персональні дані.

*5. Обробка персональних даних.*

5.1. Власник бази персональних даних здійснює обробку персональних даних в картотеках в порядку, описаному в розділі 4, з урахуванням наступних вимог:

- документи, що містять персональні дані, формуються у справи залежно від мети обробки персональних даних;

- справи з документами, що містять персональні дані, повинні мати внутрішні описи документів із зазначенням мети обробки і категорії персональних даних;

- картотеки зберігаються в приміщеннях (шафах, сейфах), захищених від несанкціонованого доступу.

5.2. Двері в приміщеннях (шафах, сейфах) повинні бути обладнані замком або контролем доступу.

*6. Відповідальність за порушення законодавства про захист персональних даних.*

6.1. З метою забезпечення виконання громадянами, органами державної влади та місцевого самоврядування, підприємствами, установами, організаціями незалежно від форм власності вимог Закону України «Про захист персональних даних», Верховною Радою України прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних » №3454-VI від 2 червня 2011 року, яким внесено зміни до Кодексу України про адміністративні порушення.

6.2. 1 липня 2012 роки за порушення у сфері захисту персональних даних на громадян, посадових осіб, громадян-суб'єктів підприємницької діяльності покладається адміністративна відповідальність.

6.3. До адміністративної відповідальність громадяни, посадові особи, громадяни-суб'єктів підприємницької діяльності притягуються за наступні види діянь:

- неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються, тягне за собою накладення штрафу згідно чинного законодавства;

- неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних, тягне за собою накладення штрафу згідно чинного законодавства;

- ухилення від державної реєстрації бази персональних даних тягне за собою накладення штрафу згідно чинного законодавства;

- недотримання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них, тягне за собою накладення штрафу згідно чинного законодавства;

6.4. Незаконний збір, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, караються (згідно чинного законодавства):

- штрафами;

- виправними роботами;

- арештом або обмеженням волі.

Ті самі дії, вчинені повторно, або якщо вони завдали істотної шкоди правам, свободам та інтересам особи, – караються (згідно чинного законодавства):

- штрафами;

- виправними роботами;

- арештом або обмеженням волі.

*7. Створення умов для обробки персональних даних на підприємстві.*

7.1. З моменту прийняття Закону України «Про внесення змін до деяких законодавчих актів України посилення відповідальності за порушення законодавства про захист персональних даних» № 3454-VI від 2 червня 2011 року норми Закону України «Про захист персональних даних» перестають бути суто декларативними, а перетворюються в дієвий правовий інструмент в руках держави, так як порушення законодавства у сфері захисту персональних даних веде до адміністративної або кримінальної відповідальності.

7.2. На виконання вимог Закону України «Про захист персональних даних» та з метою недопущення правопорушень у сфері захисту персональних

даних на підприємстві необхідно створити систему управління персональними даними, що об'єднує організаційні та технічні заходи щодо створення умов роботи з персональними даними.

7.3. На етапі створення системи управління персональними даними на підприємстві необхідно здійснити наступні організаційні заходи:

- визначити мету обробки і склад персональних даних у базі персональних даних. Як правило, на підприємстві може бути три бази персональних даних – база працівників, база контрагентів (клієнтів), база засновників;

- розробити і затвердити Порядок обробки персональних даних у базах персональних даних підприємства;

- призначити окремого виконавця або структурний підрозділ, відповідальний за відомості, що містять персональні дані, які забезпечать створення і функціонування на підприємстві комплексної системи захисту інформації в інформаційній (автоматизованій) системі від незаконної обробки та незаконного доступу, а також контроль за виконанням вимог законодавства щодо захисту персональних даних;

- провести реєстрацію баз персональних даних, що функціонують на підприємстві, в Державному реєстрі баз персональних даних;

- забезпечити оформлення письмової згоди суб'єктів персональних даних на обробку їх персональних даних у базах персональних даних підприємства, якщо створені умови щодо захисту інформації;

- забезпечити оформлення письмового зобов'язання працівників підприємства не допускати розголошення персональних даних, що їм довірені або стали їм відомі у зв'язку з виконанням професійних і трудових відносин;

- створити комплексну систему захисту інформації, що забезпечує захист персональних даних в інформаційній (автоматизованій) системі;

- розробити і затвердити необхідні положення, інструкції та інші розпорядчі документи, відповідно до яких буде забезпечуватися захист персональних даних у базах персональних даних підприємства.

7.4. Створення комплексної система захисту інформації, що забезпечить захист персональних даних в інформаційній (автоматизованій) системі від незаконної обробки, а також від незаконного доступу до них здійснюється відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 року №373 та іншими нормативно-законодавчими документами в галузі технічного захисту інформації.

## 2.4. Європейська система захисту персональних даних

Проблема захисту персональних даних з кожним роком стає все більш актуальним не лише в Україні, а й в усьому світі. Із стрімким розвитком сучасних інформаційних технологій, ідентифікація фізичної особини є необхідною до надання багатьох послуг: надання кредитів, виплата допомоги, оплата комунальних послуг, робота з банківськими установами, оплата товару через інтернет тощо. Оскільки більшість подібних послуг надається через мережу та видалений доступ і без особистої присутності, можна із упевненістю сказати, що вимоги до захисту та безпеки персональних даних мають бути більш жорсткими.

Розглядаючи поняття персональні дані, необхідно сказати, що це інформація, що здатна ідентифікувати особу. Такими даними є: прізвище, ім'я, по батькові; дата, рік, місяць, місце народження; адреса реєстрації або прописки; номер паспорта і картки соціального страхування; відомості про соціальний та сімейний стан; власність на майно, освіта, професія, доходи.

Останнім часом з'явилося багато інших персональних даних: номера кредитних і дебетових банківських карт, PIN-коди, логіни та паролі від різних сервісів (наприклад, особистої пошти), дані GPS-приймача зі смартфону, що дозволяють відстежити переміщення користувача та інше.

Злочини про крадіжку даних були поширені в другій половині XX століття в США. Найчастіші випадки стосувалися використання медичних та інших даних для отримання рецептурних препаратів шляхом обману. В Європі крадіжки персональних даних найчастіше використовувалися для надсилання фіктивних рахунків і отримання державних дотацій чи допомоги.

Для боротьби із шахрайством в багатьох країнах на законодавчому рівні розроблялися нові вимоги безпеки до компаній, що працюють з персональними даними. Цей процес носить постійний характер, оскільки інформаційні технології розвиваються і, разом з ними, з'являються все нові вимоги щодо забезпечення безпеки інформації. З іншого боку, такий розвиток штовхає злочинців на винахід нових методів розкрадання даних.

Оскільки Україна підтримує курс європейського розвитку, розглянемо розвиток системи захисту персональної інформації в ЄС. Європейське законодавство вже більше двох десятиліть удосконалює систему захисту персональних даних. В 1995 році на території Європи введена директива, що зобов'язує країни, які входять до складу ЄС, забезпечити захист персональних даних громадян. Кожна європейська країна ухвалила свої закони про захист персональних даних, що найчастіше не збігалися із законами інших країн ЄС. Багато міжнародних компаній, що передають дані через кордон, стали зазнавати великі труднощі, що пов'язані з дотриманням законів різних країн. Саме тому в 2012 році було вирішено створити загальний регламент по захисту персональних даних на території ЄС (General Data Protection Regulation – GDPR), що прийшов на зміну існуючої колись директиви [3].

Після декількох років переговорів регламент було затверджено 25 травня 2016 року. У травні 2018 року набуло чинності нове положення про захист

даних. У числі нововведень — заборона на збір персональних даних компаніями і державою без дозволу з боку фізичної особи. Виключення допускаються тільки в тому випадку, якщо в країні існують законодавчі акти, що зобов’язують до передачі інформації.

Протягом двох років, до 25 травня 2018 року, усі компанії, що зберігають, передають і обробляють особисті дані європейців, зобов'язані були забезпечити безпеку таких даних відповідно до положень GPDR. Варто відзначити, що це також стосується компаній, що перебувають за межами країн ЄС, що працюють із персональними даними громадян європейських країн (наприклад, України).

Крім європейської системи захисту персональних даних, кожна країна пройшла свій шлях створення системи захисту персональних даних. Наприклад, у Німеччині перший закон у сфері захисту персональних даних був прийнятий ще в 1970 році. А через сім років з'явився перший федеральний закон, що захищає персональні дані громадян Німеччини. Його переглянули в 1990 році, адаптувавши під нові реалії. Головною метою закону став захист недоторканності приватного життя при використанні персональних даних.

Прикладом може служити і Франція. У процесі створення системи французьке суспільство пройшло через спробу тотального контролю за громадянами, але зуміло зберегти демократичні принципи. В 1978 році уряд прийняв Закон "Про обробку даних, файлах даних та індивідуальних свободах" у якому, крім визначення основних понять, встановлено покарання за порушення. Правопорушники штрафуються, а також можуть отримати тюремний строк до 5 років. Франція строго стежить за захистом прав і свобод своїх громадян. Будь-які порушення в області персональних даних висвітлюються в пресі. Франція – прекрасний приклад країни з розвинутою системою захисту персональної інформації, що базується на якісному законодавстві і активно бореться з порушеннями, накладаючи великі штрафи.

В Англії профільний закон був прийнятий у 1984 році, в якому крім основних положень, вказувалися вимоги до структур, що збирають і

обробляють персональну інформацію. Кожний з таких користувачів зобов'язаний повідомити про інформацію, що збирає, і в яких цілях. Для цього уряд створив спеціальний "Реєстр захисту даних". Невиконання цієї вимоги карається законом. Особливо жорстко у Великобританії карають за втрату або витік персональних даних.

Ще одним прикладом може бути Польща. Закон про захист персональних даних, що адаптує польське законодавство регламенту щодо захисту персональних даних усіх осіб у межах ЄС та Європейської економічної зони (RODO), набув чинності 25 травня 2018 року. Серед нововведень Закону про захист даних – заборона на збір персональних даних компаніями і державою без дозволу з боку фізичної особи. Винятки допускаються лише в тому випадку, якщо в країні існують законодавчі положення, що зобов’язують до передачі інформації. *Польща є однією з перших країн у Європейському союзі, яка змогла повністю адаптувати національну правову систему до положень про захист персональних даних.* Наприклад, кожний громадянин має можливість отримати детальну інформацію про цілі обробки своїх даних фінансовими установами та способі їх використання, включаючи право на отримання пояснення, на якій підставі банк вирішив відмовити у видачі кредиту. Організовано також якісний захист персональних даних у секторі освіти, медичній галузі, на всіх робочих місцях у державних та інших установах.

Також важливим для держав Європейського союзу є те, що підтверджувати дозвіл на обробку персональних даних можна не з 13 років, а лише з 16 років. На компанії з європейськими представництвами накладається ряд обмежень. Їм неможна виконувати обмін даними з іншими підрозділами, якщо не виконуються правила по захисту даних. Також неможна передавати інформацію владі США та іншим країнам. Прикладом для України також є наступні держави – Литва, Латвія, Естонія.

Слід зазначити, що в ЄС новий GPDR регламент привів до масового переходу інформаційних структур європейських підприємств у хмарні сховища.

Щоб краще зрозуміти причини такої масової міграції, необхідно знати, що в GPDR усі підприємства діляться на дві основні категорії:

- контролери даних – це підприємства, діяльність яких містить у собі збір персональних даних, їх передачу, а також роботу з ними.

Основні вимоги до таких компаній полягають у дотриманні правил, що стосуються згоди громадян на зберігання, обробку і передачу їх персональних даних;

- оброблювачі даних – це підприємства, що зберігають персональні дані безпосередньо на своїх серверах. Такі компанії зобов'язані забезпечити високий рівень інформаційної безпеки даних – від обмеження фізичного доступу до обладнання, де зберігається інформація, до жорстких вимог їх резервного копіювання та налагодження брандмауерів. Забезпечення цих стандартів – складний і коштовний процес.

Для багатьох компаній витрати на відповідність вимогам GDPR у якості оброблювача даних є дуже великими, тому більшість європейських підприємств переводять свої інформаційні системи в хмарні сховища.

Захист персональних даних українців знаходиться на критично низькому рівні. Лише у 2011 році в Україні набув чинності Закон України «Про захист персональних даних» [3], згідно з нормами якого фізичні і юридичні особи (підприємства, установи і організації всіх форм власності), органи державної влади або органи місцевого самоврядування, фізичні особи – підприємці, що обробляють персональні дані, тобто відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікованою (ст.2 Закону), повинні зареєструвати бази персональних даних у спеціальному реєстрі баз даних, роботу якого контролює Державна служба з питань захисту персональних даних.

Якщо на підприємствах створюються відомості про працівників, клієнтів та осіб, з якими компанія співробітничає або продає авіаквитки, туристичні послуги, проводить опитування, то таке підприємство зобов’язане

зареєструвати таку базу даних. У випадку ж невиконання або неналежного виконання фізичними і юридичними особами вимог Закону України «Про захист персональних даних» передбачено покарання і адміністративна відповідальність за порушення законодавства про захист персональних даних» [3]. Кримінальна відповідальність відповідно до даного закону передбачена у випадку незаконного збору, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконної зміни такої інформації.

Усі персональні дані українців, починаючи з номера мобільного телефону і закінчуючи адресою проживання, сьогодні не захищені. Наприклад, багато користувачів неодноразово одержували СМС від різних служб таксі, магазинів, у яких ніколи не бували – це означає, що ваші особисті дані було продано. Характерно те, що спеціальне законодавство, розроблене в Україні для збереження й захисту персональних даних, фактично діє тільки в тому випадку, коли витік інформації походить із якихось державних установ і підприємств. Відповідальність може настати, тільки якщо власник цих даних звернувся в правоохоронні органі. Дуже небезпечна ситуація зараз існує у використанні баз персональних даних системи Мінздраву України, що легко викрасти, бо вони практично не захищені.

Проблема в Україні ще збільшується тим, що громадяни добровільно передають свої дані при одержанні різних дисконтних карт та інших випадках, не замислюючись про можливі наслідки. Будь-який витік персональних даних приносить серйозні фінансові неприємності. Ви будете здивовані, якщо на ваше ім'я було оформлено кредит. Але відповідальність нести вам. Добре, якщо доведеться довести, що не ви брали кредит, але морально ви постраждаєте.

За даними компанії Searchinform, провідного виробника засобів від витоків даних у СНД, – більше 32% українських витоків інформації пов'язано з персональними даними. Проконтролювати в Україні, як саме зберігаються та обробляються персональні дані, досить складно і майже не можливо.

Таким чином, система захисту персональних даних в Україні потребує державного моніторингу та реформування на законодавчому рівні. В умовах неухильно зростаючого рівня кіберзлочинності у світі та низького рівня інформаційної культури громадян, а також відсутності розуміння ними всіх можливих кіберзагроз, необхідно на державному рівні забезпечити захист громадян від витоку персональних даних. Вести боротьбу з кіберзлочинністю з використанням персональних даних можна тільки на основі системного підходу на усіх рівнях.

Проблемою безпеки персональних даних повинно займатися не тільки відомство омбудсмена, але й структури, пов'язані з безпекою і правоохоронною діяльністю держави [3].

**Контрольні питання**

1. Види конфеденційної інформації?
2. Заходи формування режиму інформаційної безпеки.
3. Що не належить до основних аспектів інформаційної безпеки?
4. Що не належить до зовнішніх загроз інформаційної безпеки?
5. Що входить до комплексної системи захисту інформації?
6. Інформаційна безпека – це?
7. Коли доцільно не робити жодних дій щодо виявлених ризиків?
8. Яка категорія є найбільш ризикованою з огляду на ймовірне шахрайство та порушення безпеки?
9. Що відносять до персональних даних?
10. Система управління персональними даними.

# ТЕМА 3. ЗАХИСТ ІНФОРМАЦІЇ В МОБІЛЬНИХ ПРИСТРОЯХ

## 3.1. Інформаційна безпека мобільних та дистанційних телекомунікацій

Широке застосування мобільних пристроїв і технології хмарних сховищ висуває підвищені вимоги до безпеки мобільних і дистанційних телекомунікацій, збереження і захисту корпоративних даних, в тому числі від несанкціонованого поширення цієї інформації. При використанні технології хмарних сховищ за моделлю на віддалених серверах і центрах опрацювання даних провайдера зберігається критично важлива для підприємства інформація, наприклад фінансовий звіт. Багато керівників дублюють її на своїх персональних мобільних пристроях, що знижує рівень інформаційної безпеки підприємства. В цьому випадку потрібно передбачити заходи щодо захисту або знищення цих даних при втраті або крадіжці мобільного пристрою. Передача інформації по незахищених каналах зв'язку також може привести до катастрофічних наслідків.

За статистикою 2019 р. спостерігалося подальше посилення загроз інформаційній безпеці для власників як особистих, так і корпоративних мобільних пристроїв. Аналітики цієї компанії відзначають низький рівень інформаційної безпеки корпоративних користувачів навіть у випадках не самих складних атак. Число небезпечних програм за 2019 рік в 4 рази перевищило їх число за попередні п'ять років, а самі програми стали витонченішими і складнішими. Особливу небезпеку становлять шкідливі програми для пристроїв па основі операційної системи Android.

За відкритими даними, лише за перші три квартали 2019 року кількість шкідливих програм для мобільних пристроїв на основі ОС Android наблизилося

до 750. Поряд з SMS-троянськими програмами особливу небезпеку для корпоративних користувачів представляють DDoS-атаки. Зросли як їх число, так і потужність. На думку фахівців, "основну групу ризику в нашій країні складуть компанії нафтогазової галузі, енергетики, а також сектори важкого машинобудування, інжинірингу та добувної промисловості".

Мобільні засоби часто використовуються поза контрольованої зони корпоративного зв'язку. Вони є об'єктами крадіжки і зараження шкідливими програмами з метою викрадення грошових коштів або цінної інформації, здійснення хакерських атак, спрямованих на нанесення економічної або моральної шкоди компанії. Щоб захиститися від таких загроз, недостатньо антивірусних програм, що встановлюються на мобільні пристрої. Убезпечити може тільки комплексна система забезпечення інформаційної безпеки корпоративного класу.

Одним з рішень захисту трафіку мобільних пристроїв є послуга оператора зв'язку "Мобільний VPN". В цьому випадку весь трафік мобільних пристроїв передається по закритих каналах оператора зв'язку і не потрапляє в Інтернет, що виключає ризик перехоплення нею зловмисниками.

Для мобільних користувачів інформаційна безпека забезпечується:

- готовими рішеннями, які встановлюються на мобільний апарат, щоби обмежити можливість витоку інформації;

- засобами, що надають захищене взаємодія співробітників з офісом компанії;

- засобами, що дозволяють реалізувати віртуальне робоче місце на мобільному терміналі з можливістю централізованого управління його безпекою;

- ефективним застосуванням вже існуючих сертифікованих засобів захисту.

Як відповідь на серйозну і обґрунтовану стурбованість з приводу безпеки мобільних пристроїв з'явилися нові комплексні захисти всього периметра інформаційної інфраструктури з урахуванням мобільності.

## 3.2 Загрози втрати конфіденційної інформації з мобільних пристроїв

Перш за все, всім користувачам, які користуються мобільними телефонами, а особливо смартфонами, дуже важливо розуміти, що той пристрій, який вони носять у себе у кишені, це повноцінний комп'ютер з функцією постійного доступу до мережі Інтернет, мікрофоном, камерою, GPS-навігатором і приєднаним до нього одним або декількома різними гаманцями. Тобто, є власний мобільний рахунок у оператора і додатково прив'язана банківська карта. Всі ці рахунки можуть бути використані зловмисникам.

Хочу звернути Вашу увагу на те, що для смартфонів характерні ті ж самі загрози, що і для персональних комп'ютерів, оскільки телефон, по суті, і є комп'ютером. Це обумовлює і можливість запуску "троянських" програм, і шпигунство за Вами, і крадіжку конфіденційної інформації, крадіжку грошей з Ваших мобільних рахунків.

**"Троянські" програми.**

Розглянемо проблему дещо ширше. Якими можливостями володіють троянські програми для мобільних пристроїв? На жаль, нам властиво не думати про безпеку мобільних пристроїв. І якщо на комп'ютері використання антивірусу є вже нормою, то на мобільних пристроях це все ж ще щось екзотичне. Сьогодні існує величезна кількість загроз: віруси, троянські програми, мережеві хробаки, рекламні модулі орієнтовані на абсолютно різні платформи для мобільних пристроїв.

**Шпигунські програми.** Ці програми відносяться до класу легальних шпигунських програм. Зверніть увагу – «легальних» шпигунських програм.

Що мається на увазі? Це програми, що можна вільно придбати. У програм є технічна підтримка, власний сайт, офіційний власник, програму можна досить просто видалили з приладу. Тільки подумайте, подібну програму можна вільно придбати, встановити на пристрій користувача і спокійно за ним стежити. Тобто перехоплювати інформацію про всі здійснені дзвінки, показувати вміст sms-листування, показувати інформацію про відвідувані сайти, знімати за допомогою камери телефону оточуючу ситуацію, визначати Ваше місцерозташування, сканувати bluetooth чи Wi-Fi оточення, включати мікрофон і записувати інформацію про все навкруги. Встановлення подібного додатку на телефон користувача, по суті, дозволяє шпигувати за ним всюди, адже телефон практично завжди з нами. Слідкувати можна не лише в плані дій в самому телефоні, але і за безпосереднім оточенням користувача – реальним життям, де він перебуваєте, що бачить, що говорить.

**Історія розвитку мобільних вірусів**

Дещо про історію розвитку мобільних вірусів. Перші мобільні віруси не можна було навіть назвати повністю вірусами, це були більше шкідливі sms-повідомлення, тобто на телефон користувача приходило певне sms-повідомлення і якщо його відкрити – це призводило до збою роботи телефону і могла призвести до зависання телефону, була спроможна «обнулити» телефонну книгу, здійснити певний дзвінок, тобто телефон виконував певну не потрібну користувачу функцію. Далі з’явились реальні віруси і хробаки. Перші віруси з’явились ще для комунікаторів на операційних системах Palm OS, Windows CE, Windows Mobile. Далі їм на заміну прийшов Symbian, для якого також було створено досить багато шкідливих програм, повноцінних хробаків, що мали можливість розповсюджуватись від одного пристрою до іншого використовуючи bluetooth з’єднання і виконувати шкідливі дії.

Цікаво, що тоді розповсюдження хробаків було в основному побудовано на методах соціальної інженерії. Наприклад смартфон на базі Symbian, заражений хробаком, що розповсюджується через bluetooth. Радіус дії bluetooth

передачі 10-15 метрів, при цьому автоматичної передачі не відбувається. Тобто заражений смартфон сканував оточення знаходив інші телефони із увімкненим bluetooth і намагався їм розіслати копії себе. Що ж відбувалось на стороні яка приймала? Звичайний користувач перебував у метро чи кафе і бачив на телефоні пропозицію прийняти певний файл. Ця ситуація була не висвітлена у ЗМІ і звичайної цікавості вистачало щоби прийняти файл, тим більше він міг цікаво називатись. Людина приймала файл, відкривала його із цікавості і якщо приймаючий прилад був на базі Symbian, хробак активізовувався, заражав пристрій і потім заражав інших, виконуючи нову розсилку.

Перші модифікації вірусу просто розмножувались і наносили певну шкоду, блокуючи деякі додатки у смартфоні. Більш пізніші модифікації хробака вже намагались заробляти кошти зловмисникам, тобто вірус розповсюджувався так само через bluetooth, але вже мав нову функцію – відправка sms на платні номери. Для цього зловмисники реєстрували короткі платні номери при відправці sms-повідомлень, за відправлення яких з користувача знімаються певні кошти. І троянська програма з Вашого зараженого пристрою відправляла sms-повідомлення, а зловмисники таким чином отримували зиск.

У подальшому мобільні пристрої почали володіти все більшою можливістю з'єднання з Інтернет. З початку це були WAP та GPRS з'єднання, потім з'явились 3G мережі, далі повноцінні Wi-Fi точки. В теперішній час є дуже багато місць де не підключаючись через свого GSM-оператора можна отримати доступ до глобальної мережі через Wi-Fi, що присутній практично всюди: в офісах, метро, кафе, вдома і т.д.

Маючи доступ до Інтернет хробаки отримали можливість, перш за все, більш швидко розповсюджуватись через електронну пошту, веб-сайти і наносити більш суттєву шкоду, адже вони вже могли не тільки відправляти платні sms-повідомлення, але й красти дані кредитних карток про акаунти в соціальних мережах, електронній пошті і т.д. Віруси для мобільних пристроїв

отримали всі ті властивості, що притаманні класичним шкідливим програмам для персональних комп'ютерів.

Для того щоби провести аналогію, можна зазначити, що існує багато "троянських" програм, що заражаючи телефон, перетворюють його на бота і формують цілу бот-мережу. Існують бот-нети на основі мобільних пристроїв. Так, у 2012 році у Китаї був виявлений бот-нет, що складався із 1,5 мільйона заражених пристроїв. Кожен із цих пристроїв міг або відправити sms-повідомлення на певний номер, або провести DDoS-атаку, СПАМ-розсилку. Таким чином DDoS-атаки на сайти можуть проводитись не тільки з заражених комп'ютерів, але й з заражених смартфонів, які по суті є тими самими комп'ютерами, але які ми постійно носимо з собою.

Класичні віруси для мобільних пристроїв, в основному, не розробляються. Переважно для мобільних пристроїв розробляють троянські програми, рекламні модулі, бекдор програми (які дозволяють обійти автентифікацію).

Варто розуміти, що шкідливі програми створюються для всіх операційних систем, на які можна встановити додаткове програмне забезпечення. Тобто якщо у Ваш телефон можна встановити додаткові програми, значить туди може потрапити шкідлива програма. Якщо вона не потрапить туди самостійно, автоматично, то програма може зробити це з Вашою допомогою через методи соціальної інженерії. Наприклад, Вам запропонують встановити цікаву гру, а це виявиться і гра, і шкідлива програма. Або взагалі вона не буде маскуватись під гру, а просто почне надсилати sms-повідомлення на короткі номери. Тільки пристрої з повною забороною на встановлення додаткового ПЗ є захищеними. Віруси, у широкому сенсі, для операційної системи iOS (мобільна операційна система від Apple), на жаль, існують і у досить великій кількості.

Тут скоріше стоїть питання яким чином ці шкідливі програми можуть проникнути на Ваш мобільний пристрій. І в цьому плані служба App Store дійсно більш захищена ніж служба Google Play Market. Але тут є і зворотня

сторона. Як правило, користувачі мобільнихпристроїв iPhone не готові до того що їх прилади можуть заражатись вірусами. Якщо для Android-пристроїв хоча б частина юзерів користуються антивірусами, то у разі виникнення епідемії вони можуть бути захищені набагато швидше. Користувачі ж операційної системи iOS пристроїв змушені будуть чекати поки служба Apple випустить оновлення операційної системи, що усуне вразливість.

Ще один аспект загроз для користувачів мобільних телефонів полягає у моделі роботи з платними послугами, що можуть бути не зовсім зрозумілі користувачу. Тобто Вас можуть ввести в оману попросивши набрати певний номер, надіслати sms-повідомлення. У всіх цих випадках з мобільного рахунку знімаються певні кошти. Також дуже популярною є послуга sms-підписок, коли користувачу пропонують підписатись на певний сервіс за допомогою sms-повідомлень. Це може бути все що завгодно: підписка на он-лайн гру, певний сайт, будь-який сервіс, який вимагає регулярну оплату. У подальшому користувач може забути про це. Оскільки він лише один раз погоджується, а потім ініціювання зняття коштів буде відбуватись вже оператором. З вашого рахунку періодично буде зніматись певна сума коштів і ви цього можете навіть не помічати. Інколи ми просто не пам’ятаємо на що підписалися, а, можливо, і взагалі цього не робили – бо це зробила "троянська програма". Тому варто бути дуже обережним під час використання коротких sms-повідомлень при замовленні послуг через них. Не дзвоніть на не знайомі номери і уважно контролюйте послуги, на які Ви підписуєтесь. Інколи підписка на послугу може коштувати 5 гривень, а вже за те, щоби відписатись потрібно заплатити 25 грн. Тому, варто бути якомога більш уважними і не користуватись підозрілими сервісами.

**Контрольні запитання**

1. Головна характеристика троянської програми.
2. Шпигунські програми – це?
3. Які загрози через використання мобільних пристроїв?
4. Як проникають на мобільний телефон вірусні програми?
5. Яка шкода від вірусів?

# ТЕМА 4. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

## 4.1. Методи захисту інформації

Система управління інформаційною безпекою ґрунтується на трьох фундаментальних принципах управління:

• принцип розімкнутого керування;

• принцип компенсації;

• принцип зворотнього зв'язку.

За принципом розімкнутого управління створюються власні політики безпеки, виконання яких контролюється відповідальними особами. В даний час більшість компаній виділяє для особи, відповідальної за розробку і реалізацію політик ІБ, позицію CISO (Chief Information Security Officer) – керівника відділу IT-безпеки або директора по IT-безпеки. Як правило, CISO очолює керуюча рада з питань інформаційної безпеки.

Принцип компенсації має на увазі, що в разі виникнення будь-яких відхилень від розробленої політики безпеки або зовнішніх факторів (а це неминуче, оскільки компанії розвиваються, з'являються нові загрози, приходять і йдуть нові співробітники, з'являються нові програмні продукти) необхідно негайно вносити відповідні корективи в алгоритм управління, що компенсували б негативний результат зовнішніх впливів.

Тому для компаній дуже важливо не тільки розглядати інциденти, що вже відбулися, але і будувати систему проактивного захисту, здатної відбити атаки до того, як з'являться проблеми, і навіть до того, як стане відомо про потенційні проблеми та слабкі місця.

Дуже важливо дотримуватися принципу зворотнього зв'язку, що дозволяє управляти ІБ по замкнутому колу. За цим принципом будуються багато систем ІБ.

Наявність ланки зворотнього зв'язку в системі управління інформаційною безпекою дозволяє не тільки виявити окрему загрозу, але і відреагувати на цілий ряд подій, на перший погляд ніяк не пов'язаних між собою. У цьому можуть допомогти продукти, що забезпечують централізоване зіставлення даних журналів подій з мережевих пристроїв і систем безпеки в режимі реального часу, автоматично зіставляючи дані і виділяючи події і загрози безпеці, що вимагають прийняття рішучих заходів, такі як Check Point Eventia Analyzer.

Побудова систем ІБ з урахуванням перерахованих принципів дозволяє використовувати існуючі методи оптимізації для покращення різних показників якості системи, таких як стійкість управління, швидкість реакції на існуючі та невідомі загрози

Розробка комплексу організаційних засобів захисту інформації повинна входити в компетенцію служби безпеки.

Найчастіше фахівці з безпеки:

- розробляють внутрішню документацію, що встановлює правила роботи з комп'ютерною технікою та конфіденційною інформацією;
- проводять інструктаж і періодичні перевірки персоналу;
- ініціюють підписання додаткових угод до трудових договорів, де вказана відповідальність за розголошення або неправомірне використання відомостей, що стали відомі по роботі;
- розмежовують зони відповідальності, щоби виключити ситуації, коли масиви найбільш важливих даних знаходяться в розпорядженні одного із співробітників;
- організують роботу в загальних програмах документообігу і стежать, щоби критично важливі файли не зберігалися поза мережевих дисків;
- впроваджують програмні продукти, що захищають дані від копіювання або знищення будь-яким користувачем, в тому числі топ-менеджментом організації;

• складають плани відновлення системи на випадок виходу з ладу з якихось причин.

Якщо в компанії немає виділеної ІБ-служби, виходом стане запрошення фахівця з безпеки на аутсорсинг. Віддалений співробітник зможе провести аудит ІТ-інфраструктури компанії і дати рекомендації по її захисту від зовнішніх і внутрішніх загроз. Також аутсорсинг в ІБ передбачає використання спеціальних програм для захисту корпоративної інформації.

На практиці використовують кілька груп методів захисту, в тому числі:

• перешкода на шляху передбачуваного викрадача, що створюють фізичними і програмними засобами;

• управління, або надання впливу на елементи, що захищається системи;

• маскування, або перетворення даних, зазвичай – криптографічними способами;

• регламентація, або розробка нормативно-правових актів і набору заходів, спрямованих на те, щоби спонукати користувачів, які взаємодіють з базами даних, до належної поведінки;

• примус, або створення таких умов, при яких користувач буде змушений дотримуватися правил поводження з даними;

• спонукання, або створення умов, що мотивують користувачів до належного поведінці.

Кожен з методів захисту інформації реалізується за допомогою різних категорій засобів. Основні засоби – організаційні та технічні.

**Регламент щодо забезпечення інформаційної безпеки** – внутрішній документ організації, що враховує особливості бізнес-процесів і інформаційної інфраструктури, а також архітектуру системи.

Захистити інформацію від несанкціонованого доступу можна за допомогою апаратно-програмних, програмних, біометричних, технічних і адміністративних засобів.

*Апаратно-програмні засоби:*

• спеціальні криптографічні плати, що вбудовуються в комп'ютер, за допомогою яких інформацію можна зашифрувати, створити електронний підпис, а також аутентифікувати користувача (аутентифікація — процес ідентифікації користувачів, пристроїв або будь-якої іншої одиниці, що бере участь в інформаційному обміні, перед початком якого треба мати дозвіл на доступ до даних);

• SmartCard — магнітна картка для зберігання секретного ключа, шифрування паролей;

• пристрої ActivCard для введення паролей, де пароль не вводиться, а розраховується (динамічний пароль), а також SmartReader для зчитування паролей. В цих пристроях всередині вмонтовано мікропроцесор, у пам'яті якого зберігається секретний код. Пароль, що вводиться користувачем (чотири цифри), в комп'ютері перераховується, тобто створюється спеціальний код.

*Програмні заходи:*

• вбудовані у програми функції захисту даних. Наприклад, система Netware після трьох спроб користувача ввійти в мережу з неправильним паролем блокує ідентифікатор цього користувача, і тільки адміністратор мережі має змогу розблокувати доступ;

• спеціальні криптографічні розробки. За принципом побудови існуючі засоби захисту інформації можна поділити на два типи:

• засоби, в основі роботи яких лежать симетричні алгоритми для побудови ключової системи і системи аутентифікації;

• засоби, основу роботи яких складають асиметричні алгоритми, що застосовуються для тих самих цілей.

У засобах першого типу обов'язковою є наявність центру розподілу ключів, що відповідає за їх створення, розповсюдження та вилучення. При цьому носії ключової інформації передаються абонентам із використанням фізично захищених каналів зв'язку. Ключі мають змінюватися досить часто, кількість абонентів має бути значною, тому ці засоби негнучкі та дорогі.

Питання аутентифікації вирішується довірою користувачів один одному, цифровий підпис неможливий. Центр розподілу ключів контролює всю інформацію. Захист інформації дуже низький.

У засобах другого типу ключі для шифрування автоматично генеруються, розповсюджуються і вилучаються для кожного сеансу зв'язку. Функції служби розповсюдження ключів виконує сертифікаційний центр, де користувач реєструється, встановлюється його аутентифікація, після чого ключі вилучаються. В таких засобах можливими є організація цифрового підпису та його перевірка. Протокол встановлення аутентичного зв'язку відповідає певному стандарту. Аутентифікація є простою та суворою. При простій аутентифікації відбувається обмін паролями між абонентами, які встановили зв'язок, із подальшою перевіркою відповідності цих паролів еталонним. При суворій аутентифікації кожен абонент має два криптографічних ключі — секретний, відомий тільки даному абоненту, та відкритий — той, що передається в банк. Використовуючи секретний ключ і спеціальний алгоритм, абонент формує цифровий підпис — послідовність бітів, яка однозначно відповідає документу, що підписується. Перевірка відповідності підпису виконується за допомогою відкритого ключа.

*Біометричні засоби:*

- візерунки сітчатки ока;
- відбитки пальців; ·
- геометрія руки; ·
- динаміка підпису.

*Адміністративні заходи.*

– систему електронних перепусток для персоналу і відвідувачів;
– системи відеоспостереження та відеореєстрації, що, дають змогу вести цілодобовий візуальний нагляд як за периметром об'єкта, так і всередині з можливістю запису інформації на відеомагнітофон або комп'ютер;

- • розподіл доступу до інформації. Тут необхідним є чітке визначення осіб, які мають право на ту чи іншу інформацію. Наприклад, програмісти не повинні мати доступу до баз даних, а користувачі — до програмного забезпечення;
- систематичний аналіз мережевого протоколу роботи, блокування спроб введення паролів декілька разів;
- ретельний підбір співробітників, навчання, стажування, тренування. Кандидат повинен мати хороші характеристики з попередніх робочих місць, не мати нахилу до зловживання наркотиками та алкоголем, не мати вагомих заборгованостей, не виявляти доброзичливості до наймачів.

**Технічні заходи.**

Поділяються на такі групи:

1) заходи захисту від прослуховування, що включають:

- встановлення фільтрів на лініях зв'язку;
- обстеження приміщень із метою виявлення підслуховуючих пристроїв;
- використання звукопоглинаючих стін, стелі, підлоги;
- застосування систем віброакустичного й акустичного зашумлення для захисту мовної інформації від прослуховування за допомогою акустичних мікрофонів, стетоскопів, лазерних та інфрачервоних систем відбору інформації;

2) заходи захисту від електромагнітного випромінювання, куди входять: ·

- використання оптоволоконного кабелю;
- застосування захисної плівки на вікнах;
- користування захищеними дисплеями;
- заходи захисту від поновлення вилучених даних.

## 4.2 Організаційні засоби захисту інформації

На вершині СУІБ знаходиться директор з ІБ, який очолює керуючий комітет з ІБ – колегіальний орган, призначений для вирішення стратегічних питань, пов'язаних із забезпеченням ІБ. Директор з ІБ несе відповідальність за всі процеси управління ІБ, в число яких входять: управління інцидентами і моніторинг безпеки, управління змінами та контроль захищеності, інфраструктура безпеки (політики, стандарти, інструкції, процедури, плани та програми), управління ризиками, контроль відповідності вимогам , навчання (програма підвищення обізнаності).

Створення даної структури управління є метою впровадження стандарту ISO 27001/17799 в організації. Один з основних принципів тут – «прихильність керівництва». Це означає, що така структура може бути створена тільки керівництвом компанії, яке розподіляє посади, відповідальність і контролює виконання обов'язків. Іншими словами, керівництво організації будує відповідну вертикаль влади, а точніше модифікує існуючу для задоволення потреб організації в безпеці. СУІБ може створюватися тільки зверху вниз.

Іншим основним принципом є залучення до процесу забезпечення ІБ всіх співробітників організації, які мають справу з інформаційними ресурсами – «від директора до прибиральниці». Необізнаність конкретних людей, які працюють з інформацією, відсутність програми навчання по ІБ, – одна з основних причин непрацездатності конкретних систем управління.

Не менш важливо і те, що в основі будь-якого планування заходів з ІБ повинна бути оцінка ризиків. Відсутність в організації процесів управління ризиками призводить до неадекватності прийнятих рішень і невиправданих витрат. Іншими словами, оцінка ризиків є тим фундаментом, на якому тримається СУІБ.

Настільки ж фундаментальним принципом є «впровадження і підтримка СУІБ власними руками». Залучення зовнішніх консультантів на всіх етапах

впровадження, експлуатації та вдосконалення СУІБ в багатьох випадках цілком виправдано. Більш того, це є одним з механізмів контролю, описаних в стандарті ISO 17799. Проте створення СУІБ руками зовнішніх консультантів неможливо за визначенням, тому що СУІБ – це сукупність організаційних структур, яка формуються керівництвом організації і процесів, що реалізуються її співробітниками, які належним чином поінформовані про свої обов'язки і навчені навичкам поводження з інформацією та її захисту. СУІБ коштує чималих грошей, але ні за які гроші не можна купити досвід і знання.

Використання системного підходу дозволить уникнути зайвих витрат на доопрацювання, а можливо, і повного перебудування системи інформаційної безпеки в майбутньому. Побудова фінансових і математичних моделей систем ІБ, оцінка загроз та їх наслідків, класифікація інформації, облік активів – все це повинно використовуватися при розробці системи інформаційної безпеки. Правильна оцінка ризиків дозволяє істотно знизити витрати на інформаційну безпеку.

Існує велика кількість рекомендацій та документів, що регламентують питання побудови систем інформаційної безпеки.

Можливість централізованого управління є найважливішою вимогою для ефективної і безперервної роботи системи інформаційної безпеки. Наприклад, технологія Check Point SMART, що реалізує централізоване управління, дозволяє легко керувати найскладнішими системами, істотно знижуючи як витрати на адміністрування, так і кількість помилок, що допускаються персоналом. Використання ж «клаптикового» методу побудови системи інформаційної безпеки робить її в підсумку некерованою, слабо контрольованою і марною.

Система управління інформаційною безпекою (Information Security Management System) є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проєктування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. Систему складають

організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Основними цілями інформаційної безпеки є:

• конфіденційність інформації, тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб;

• неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;

• цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), що полягає в її існуванні в неспотвореному вигляді (незмінному по відношенню до деякого фіксованого її стану);

• доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до цікавить їх;

• мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів;

• облік усіх процесів, пов'язаних з ризиками.

Досягнення заданих цілей здійснюється в ході рішення наступних завдань:

• введення в систему термінів інформаційної безпеки;

• класифікації інформаційних ресурсів підприємства;

• визначення власників процесів, відповідальних за інформаційну безпеку;

• розробки спектра ризиків інформаційної безпеки і проведення їх експертних оцінок;

• визначення групи доступу до інформаційних ресурсів;

• розробки системи управління ризиками інформаційної безпеки (методи і їх оцінка);

• складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;

• здійснення заходів інформаційної безпеки і періодичного контролю за станом ризиків;

• забезпечення фізичної безпеки і безпеки персоналу;

• розробки вимог до інформаційної системи з точки зору інформаційної безпеки;

• контролінгу інформаційної безпеки на підприємстві.

Виділяються чотири стадії реалізації системи управління інформаційною безпекою:

1) формування політики в галузі ризиків;

2) аналіз бізнес-процесів;

3) аналіз ризиків;

4) формування цільової концепції.

Формування політики в галузі ризиків визначає принципи управління ними для всього підприємства в цілому. Ці принципи базуються на цілях підприємства, його стратегії, також на вимоги, що пред'являються законом і стандартами в області інформаційної безпеки. Фактором ефективності системи управління інформаційною безпекою є її побудова на базі міжнародних стандартів ISO / IEC 17799: 2005 та ISO / IEC 27001: 2005.

Стандарт ISO / IEC 17799: 2005 визначає принципи і являє собою довідник по розробці, впровадженню, супроводу і покращення системи управління інформаційною безпекою, а також описує механізми визначення цілей контролю і його засобів в наступних областях:

• політика безпеки (встановлення принципів управління і засобів забезпечення захисту інформації);

• управління безперервністю бізнес-процесів (запобігання втручанню в ділові операції і захист процесів обробки інформації від наслідків серйозних несправностей або катастроф);

• дотримання правових норм (виняток порушень кримінального та цивільного права, встановлених законом зобов'язань, регулятивних або контрактних зобов'язань, а також вимог з безпеки);

• організація активів і ресурсів (управління захистом інформації всередині організації);

• фізична безпека і безпека навколишнього середовища (запобігання несанкціонованого доступу, пошкодження та проникнення в службові приміщення або втручання в ділову інформацію);

• класифікація та управління активами (виявлення і захист інформаційних активів);

• захист персоналу (зниження ризиків, пов'язаних з помилкою оператора, крадіжкою, шахрайством або зловживанням використання обладнання);

• управління доступом (контроль доступу до інформації);

• управління засобами зв'язку та експлуатацією устаткування (коректне і безпечне функціонування засобів обробки інформації);

• розробка та обслуговування систем (впровадження засобів захисту в інформаційні системи).

Стандарт ISO / IEC 27001: 2005 встановлює вимоги до системи управління інформаційною безпекою підприємства, являє собою довідник по визначенню, мінімізації та управління небезпеками і загрозами, яким може піддаватися інформація, і розроблений з метою забезпечення допомоги у виборі ефективних і адекватних засобів для його захисту. Застосування стандарту ISO / IEC 27001: 2005 на підприємстві дозволяє:

• встановити вимоги і цілі в області інформаційної безпеки;

• гарантувати впевненість в тому, що управління ризиками в області інформаційної безпеки є ефективним, а також те, що діяльність підприємства відповідає законодавству та іншим нормативним документам;

• реалізувати процес контролю за впровадженням системи управління інформаційною безпекою;

• ідентифікувати і відстежувати існуючі процеси управління інформаційною безпекою;

• керівництву підприємства визначити стан процесів управління захистом інформації;

• внутрішнім і зовнішнім аудиторіям встановити рівень відповідності політики безпеки регламентам;

• забезпечити партнерів і постачальників відповідною інформацією про стандарти, процедури та політиці підприємства.

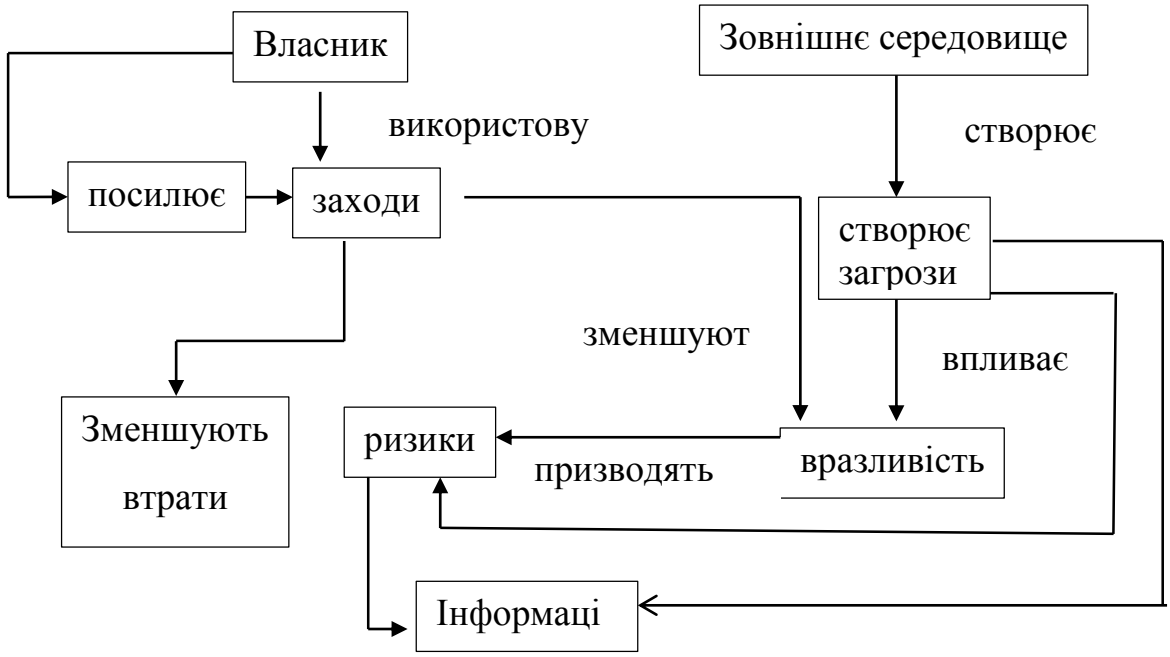


Рис. 4.1. Модель системи інформаційної безпеки підприємства

Модель системи інформаційної безпеки підприємства – це сукупність зовнішніх і внутрішніх факторів, їх вплив на стан інформаційної безпеки підприємства і забезпечення зберігання ресурсів. На рис. 4.1 представлено модель системи інформаційної безпеки підприємства, в якій представлені напрямки впливу між наступними факторами:

• загрозами інформаційній безпеці, що характеризуються ймовірністю виникнення і реалізації;

• вразливістю системи інформаційної безпеки, що впливає на ймовірність реалізації загрози;

• ризиками, що відображають завдання шкоди в результаті реалізації загрози інформаційній безпеці.

Інформація та матеріальні ресурси, що необхідно захищати, називаються об'єктами захисту. До них відносяться:

• мовна інформація;

• інформація, що зберігається і обробляється за допомогою засобів зв'язку у вигляді різних носіїв;

• документи на паперових носіях;

• технічні засоби зв'язку та інформатизації;

• приміщення, призначені для обговорення, обробки і зберігання інформації;

• інформаційні системи в цілому, включаючи системи зв'язку;

• документація на технічні та програмні засоби зв'язку і інформатизації;

• програмні засоби.

Загрози, з якими може зіткнутися підприємство, класифікуються за своєю природою їх виникнення, тобто загрози випадкового або навмисного характеру, і по тому, як вони ставляться до захищається, тобто зовнішні і внутрішні загрози.

Джерелами зовнішніх загроз є:

• діяльність конкурентів по перехопленню важливої інформації;

• навмисні дії по руйнуванню, знищенню або модифікації інформації;

• ненавмисні дії співробітників сторонніх організацій, що призвели до відмови в роботі елементів системи;

• стихійні лиха і катастрофи, аварії, екстремальні ситуації.

До джерел внутрішніх загроз належать:

• відсутність координації діяльності підрозділів підприємства в сфері захисту інформації;

• навмисні дії персоналу по знищенню або модифікації інформації;

• ненавмисні помилки персоналу, відмови технічних засобів і збої в інформаційних системах;

• порушення встановлених регламентів збору, накопичення, зберігання, обробки, перетворення, відображення і передачі інформації.

**Порушення можуть бути декількох видів.**

*Організаційно-правові порушення* – порушення, пов'язані з відсутністю єдиної узгодженої політики підприємства в сфері захисту інформації, невиконанням вимог нормативних документів, режимом доступу, зберігання та знищення інформації.

*Організаційні види порушень* включають несанкціоноване отримання доступу до баз і масивів даних, несанкціонований доступ до активного мережевого обладнання, серверів, некоректне вбудовування засобів захисту і помилки в управлінні ними, порушення в адресності розсилки інформації при веденні інформаційного обміну.

*Фізичні види порушень* – пошкодження апаратних засобів автоматизованих систем, ліній зв'язку та комунікаційного обладнання, крадіжки або несанкціоноване ознайомлення зі змістом носіїв інформації, їх розкрадання.

*До радіоелектронним видам порушень* відносяться впровадження електронних пристроїв перехоплення інформації, отримання інформації шляхом перехоплення і дешифрування інформаційних потоків, фотографування моніторів, нав'язування неправдивої інформації в локальних обчислювальних мережах, передачі даних і лініях зв'язку.

Для протидії загрозам і припинення порушень на підприємствах організовується процес управління ризиками, який є основою системи інформаційної безпеки підприємства.

Побудова ефективної системи інформаційної безпеки – це комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час.

З точки зору процесного підходу систему інформаційної безпеки підприємства можна уявити як процес управління ризиками (рис. 4.2), що включає в себе наступні складові.

**1. Опис бізнес-процесів.** Виконується коригування та аналіз бізнес-процесів. За критеріями, що визначаються в ході формування політики в галузі ризиків, здійснюється ідентифікація бізнес-процесів.

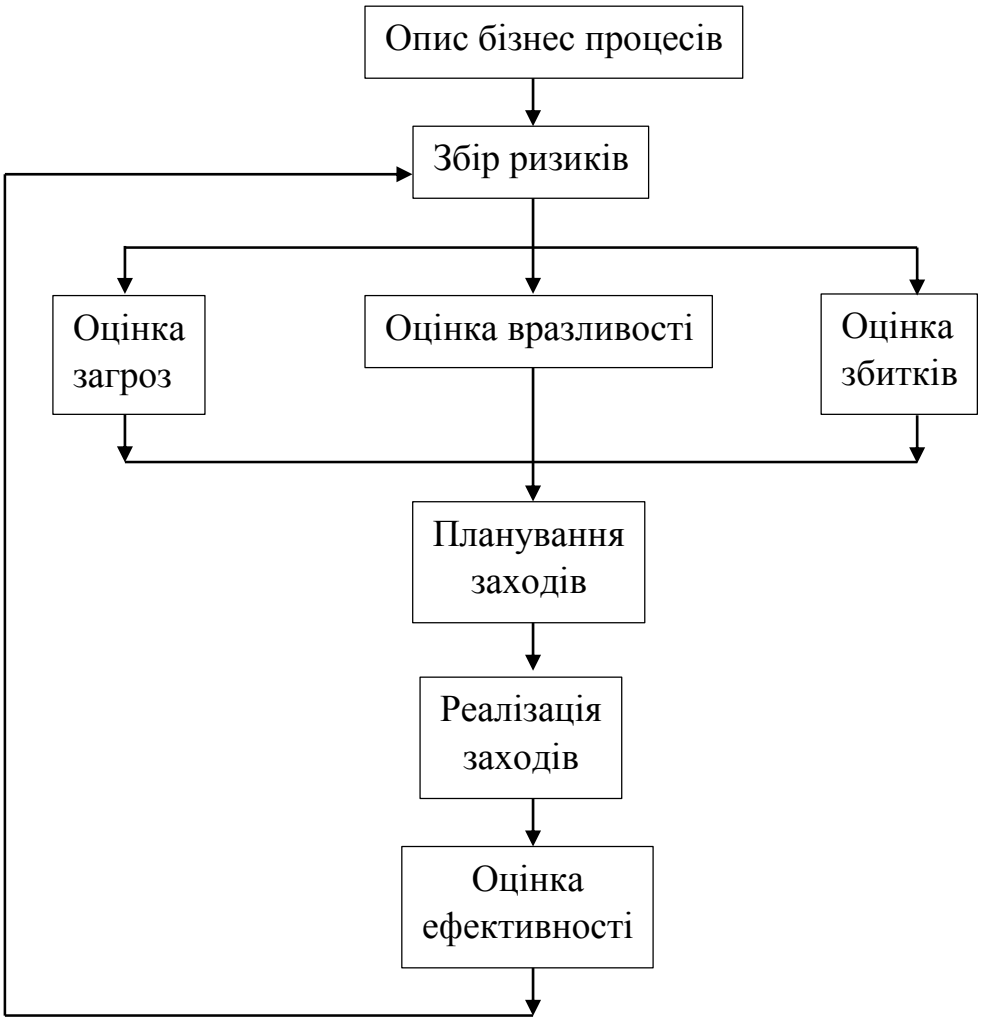


Рис. 4.2. Модель процесу управління ризиками для системи інформаційної безпеки

**2. Збір ризиків.** Проводиться для виявлення ступеня схильності підприємства загрозам, що можуть завдати істотної шкоди. Для цього здійснюється аналіз його бізнес-процесів і опитування експертів предметної

області. Результатом (виходом) даного процесу вважається класифікаційний перелік всіх потенційних ризиків.

До стандартних ризиків інформаційної безпеки відносяться:

- вилучення конфіденційної інформації з локальних місць;
- навмисна зміна інформації з метою знищення;
- копіювання важливих документів і передача конкуренту;
- незаконне проникнення в корпоративну мережу;
- знищення через технічні причини.

**3. Оцінка ризиків.** Визначаються характеристики ризиків і ресурси інформаційної системи. Основним результатом (виходом) даного процесу є перелік всіх потенційних ризиків з їх кількісними і якісними оцінками шкоди і можливості реалізації, а додатковим – перелік ризиків, що не будуть відслідковуватися на підприємстві.

Процес оцінки ризиків складається з наступних кроків:

- опис об'єкту і заходів захисту;
- ідентифікація ресурсу і визначення його кількісних показників;
- аналіз загроз інформаційної безпеки;
- оцінка вразливостей;
- оцінка існуючих і передбачуваних засобів забезпечення інформаційної безпеки.

**4. Планування заходів.** Метою планування заходів по мінімізації ризиків є визначення термінів та переліку робіт по виключенню або мінімізації збитку в разі мінімізації ризику.

Виділяються наступні види заходів з інформаційної безпеки:

- організаційні;
- правові;
- організаційно-технічні;
- програмні;
- інженерно-технічні.

**5. Реалізація заходів.** Під реалізацією заходів щодо мінімізації ризиків маються на увазі виконання запланованих робіт, контроль якості отриманих результатів і термінів. Результатом даного процесу є виконані роботи по мінімізації ризиків і час їх проведення.

**6. Оцінка ефективності.** Оцінка ефективності системи управління інформаційною безпекою – системний процес отримання та оцінки об'єктивних даних про поточний стан системи, дії і події, що відбуваються в ній, що встановлює рівень їх відповідності певним критеріям.

Цілями процесу є:

- оцінка поточного рівня ефективності системи;
- локалізація "вузьких" місць в системі;
- оцінка відповідності системи підприємства існуючим стандартам в області інформаційної безпеки;
- вироблення рекомендацій та регламентів щодо забезпечення безпеки об'єктів захисту.

Результати процесу можуть використовуватися в цілях аудиту для підготовки підприємства до сертифікації за стандартом ISO / IEC 27001: 2005.

## 4.3. Технічні системи захисту даних

Система захисту інформації, що обробляється з використанням технічних засобів, будується за певними принципами. Це обумовлено необхідністю протидії цілої низки загроз безпеки інформації.

Основним принципом протидії загрозам безпеки інформації, є превентивність вжитих заходів захисту, так як усунення наслідків прояви загроз вимагає значних фінансових, часових і матеріальних витрат.

Диференціація заходів захисту інформації в залежності від її важливості та частоти і ймовірності виникнення загроз безпеки є наступним основним принципом протидії загрозам.

До принципів протидії загрозам також відноситься принцип достатності заходів захисту інформації, що дозволяє реалізувати ефективний захист без надмірного ускладнення системи захисту інформації.

Протидія загрозам безпеки інформації завжди носить агресивний характер по відношенню до користувачів і обслуговуючого персоналу автоматизованих систем. За рахунок накладання обмежень організаційного і технічного характеру. Тому, одним із принципів протидії загрозам є принцип максимальної дружності системи забезпечення інформаційної безпеки. При цьому слід врахувати сумісність створюваної системи протидії загрозам безпеки інформації з операційною та програмно-апаратною структурою автоматизованої системи і сформованими традиціями установи.

Важливість реалізації цього принципу заснована на тому, що додавати до функціонуючої незахищеної автоматизованої системи засобами захисту інформації складніше і коштовніше, ніж початкове проєктування і побудова захищеної системи.

З принципу декомпозиції механізму впливу загроз безпеки інформації випливає принцип самозахисту і конфіденційності системи захисту інформації, що полягає в застосовності принципів протидії загрозам до самої системи захисту і дотримання конфіденційності реалізованих механізмів захисту інформації в автоматизованій системі. Реалізація даного принципу дозволяє контролювати цілісність системи захисту інформації, управляти безпекою через адміністратора безпеки, відновлювати систему захисту при її компрометації і відмовах устаткування.

Засоби захисту інформації, присутні в даний час на ринку, умовно можна розділити на декілька груп:

- ✓ активні і пасивні технічні засоби, що забезпечують захист від витоку інформації по різним фізичним параметрам, що виникають при застосуванні засобів її обробки;

- ✓ програмні та програмно-технічні засоби, що забезпечують розмежування доступу до інформації на різних рівнях, ідентифікацію та аутентифікацію користувачів;
- ✓ програмні та програмно-технічні засоби, що забезпечують захист інформації і підтвердження її справжності при передачі по каналах зв'язку;
- ✓ програмно-апаратні засоби, що забезпечують цілісність програмного продукту і захист від несанкціонованого його копіювання;
- ✓ програмні засоби, що забезпечують захист від впливу програм-вірусів і інших шкідливих програм;
- ✓ фізико-хімічні засоби захисту, що забезпечують підтвердження автентичності документів, безпеку їх транспортування і захист від копіювання.

Окремо виділяються захищені загальносистемні програмні продукти, що виключають можливість використання декларованих програмних можливостей. Таких систем поки ще не дуже багато.

Сюди ж віднесені і спеціальні пристрої – міжмережеві екрани: для забезпечення захисту корпоративних мереж від вторгнення з глобальних інформаційних мереж типу Internet.

В даний час засоби і системи, призначені для захисту інформації та підтвердження її справжності при передачі по каналах зв'язку і, в першу чергу, криптографічні пристрої, виробляються більш ніж 700 закордонними фірмами. Для захисту конфіденційної інформації, що передається по каналах зв'язку можуть використовуватися скремблери (обробляють і шифрують сигнал) і шифратори (перетворення n-розрядного коду в k-розрядний код). Для захисту конфіденційної інформації в каналах радіосистем зв'язку призначені пристрої фірми Simens (Німеччина), Grundy & Pirtners (Великобританія).

Ряд фірм випускає криптографічні пристрої орієнтовані на роботу в мережах, наприклад, шифратор ScaNet фірми Dowty Network Systems (Великобританія), шифратор Datacryptor-64 фірми Racal Datacom (США) для користувачів мережі з пакетною комутацією по протоколу X.25 МККТТ. Фірма

NFT (Норвегія) розробила серію криптомодулів зі швидкостями до 10 Мбіт/с, призначених для засекречування потоків і застосування в локальних мережах. Фірма Xerox (США) створила блок високоякісного шифрування даних Xerox Encription Unit, що забезпечує захист особливо секретної інформації, в локальній мережі. Фірма PE Systems (США) поставляє систему GILLAROO для передачі цифрового підпису та захисту секретної інформації, переданої в мережах і каналах зв'язку. Фірма Calmes Semiconductor Inc. (США) виробляє кріптопроцессор СЛ34С168 для блочного шифрування на швидкості до 300 Кбіт/с. За останній час запропоновані нові алгоритми шифрування, наприклад NEWDES і FEAL, розраховані на шифрування потоків зі швидкостями до 1 Гбіт/с.

Останнім часом все більш широке поширення на ринку програмно-апаратних засобів захисту інформації отримують системи запобігання несанкціонованого копіювання програмних продуктів типу "HASP-ключів".

Основою багатьох сучасних систем охорони приміщень і захисту від несанкціонованого доступу до інформації служать електронні ідентифікаційні пристрої. Прикладом такого пристрою є автоматичний ідентифікатор, вироблений американською фірмою DALLAS SEMICONDUCTOR. Ідентифікатор може бути вбудований в брелок, візитну картку, перепустка. В залежності від варіанту застосування автоматичний ідентифікатор може використовуватися з різними додатковими пристроями: електронними замками, комп'ютерами.

Наявність в ідентифікаторі змінної пам'яті дозволяє використовувати його для широкого класу додатків, наприклад, для зберігання особистих, періодично змінюваних ключів шифрування користувача; для зберігання інформації про стан особового рахунку користувача для розрахункових систем; для зберігання інформації про дозволений час проходу в пропускних системах. Використання ідентифікатора разом з електронними замками дає широкі можливості по керуванню доступом користувачів в режимні приміщення: централізоване

оперативне стеження за проходом в приміщення, дистанційне керування допуском, гнучке встановлення правил допуску в приміщення (наприклад, по певних днях і годинах).

Ще кілька слів про новітні технології, що засновані на використанні фізико-хімічних властивостей матеріалів і забезпечують підтвердження автентичності документів, безпеку їх транспортування і захист від копіювання. Це спеціальні тонкоплівкові матеріали зі змінною кольоровою гамою на основі технології Advateg, що наносяться на документи і предмети або голографічних мітки. Вони дозволяють однозначно ідентифікувати достовірність об'єкта і контролювати несанкціонований доступ до них. Крім того, на основі технології Advateg розроблені спеціальні конверти, пакети і інший пакувальний матеріал, що дозволяє гарантувати конфіденційність документів і матеріальних засобів при їх транспортуванні навіть за звичайними поштовим каналах.

Група технічних засобів захисту інформації поєднує апаратні і програмні засоби. Основні:

• резервне копіювання і віддалене зберігання найбільш важливих масивів даних в комп'ютерній системі – на регулярній основі;

• дублювання і резервування всіх підсистем мереж, що мають значення для збереження даних;

• створення можливості перерозподіляти ресурси мережі в випадках порушення працездатності окремих елементів;

• забезпечення можливості використовувати резервні системи електроживлення;

• забезпечення безпеки від пожежі або пошкодження обладнання водою;

• установка програмного забезпечення, що забезпечує захист баз даних та іншої інформації від несанкціонованого доступу.

В комплекс технічних заходів входять і заходи щодо забезпечення фізичної недоступності об'єктів комп'ютерних мереж, наприклад, такі практичні способи, як обладнання приміщення камерами і сигналізацією.

## 4.4 Механізми інформаційної безпеки

Існують наступні концептуальні механізми інформаційної безпеки:

- Ідентифікація та аутентифікація;
- Контроль і управління доступом;
- Протоколювання і аудит;
- Шифрування;
- Контроль цілісності;
- Екранування.

Для надійного захисту інформації необхідна комплексна реалізація всіх перерахованих механізмів. Деякі з них можуть бути реалізовані в більш повній мірі, інші – ні. Захист інтелектуальної власності, в першу чергу, залежить від реалізації механізму ідентифікації і аутентифікації.

***Ідентифікатор*** – унікальний набір символів, що відповідає об'єкту або суб'єкту в даній системі.

***Ідентифікація*** – розпізнавання учасника процесу інформаційної взаємодії перед тим, як до нього будуть застосовані аспекти інформаційної безпеки.

***Пароль*** – секретний набір символів, що дозволяє підтвердити відповідність суб'єкта пред'явленому ідентифікатору.

***Аутентифікація*** – забезпечення впевненості в тому, що учасник інформаційної взаємодії ідентифікований вірно.

***Профіль*** – набір установок і конфігурацій для даного суб'єкта чи об'єкта, що визначає його роботу в інформаційної системі.

***Авторизація*** – формування профілю прав для конкретного учасника інформаційної взаємодії.

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

- щось, що він знає (пароль, криптографічний ключ і т.п.);

- щось, чим він володіє (електронний ключ, смарт-карта і т.п.);
- щось, що є частина його самого (свої біометричні дані).

Аутентифікація буває односторонньою (зазвичай суб'єкт доводить свою справжність системі) і двосторонньою (взаємною). Розглянемо її особливості.

1. **Ідентифікація та аутентифікація**

Надійна ідентифікація і аутентифікація не можлива через цілу низку причин. В інформаційної системі між сторонами може не існувати довіреної маршруту: це означає, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими і використаними для перевірки автентичності.

Майже всі аутентифікаційні сутності можна дізнатися, вкрасти або підробити.

Є протиріччя між надійністю аутентифікації, з одного боку, і зручностями суб'єкта з іншого. Так, з міркувань безпеки, необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію.

Чим надійніший засіб захисту, тим він коштовніше.

**2. Парольна аутентифікація**

Головна перевага парольної аутентифікації – простота. Недолік – найслабший засіб перевірки автентичності.

Основні порушення при створенні і використанні паролів:

- простий пароль;
- використання стандартних значень з будь-якої документації, що ніколи не забути;
- запис пароля там, де його можна прочитати, підглянути і т.д.;
- передавання пароля іншому співробітнику.

Заходи, що дозволяють підвищити надійність парольного захисту:

- накладання технічних обмежень (довжина, використання букв, цифр, знаків);
- управління терміном дії паролів;

- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему;
- навчання користувачів;
- використання програмних генераторів паролів, які ґрунтуючись на деяких правилах, можуть створювати складні, але легкі для запам’ятовування паролі;
- одноразові паролі.

### 3. Одноразові паролі

Маємо односторонню функцію f (функція, обчислити зворотню якої за прийнятний час не представляється можливим). Ця функція відома і користувачеві, і серверу аутентифікації.

Маємо секретний ключ K, відомий тільки користувачеві.

На етапі початкового адміністрування користувача функція f застосовується до ключу K n-раз, після чого результат зберігається на сервері.

Після цього процедура перевірки автентичності користувача виглядає наступним чином:

– сервер надсилає на призначену для користувача систему число (n-1);

– користувач застосовує функцію f до секретного ключа K (n-1) раз і надсилає результат по мережі на сервер аутентифікації;

– сервер застосовує функцію f до отриманого від користувача значенням і порівнює результат з раніше збереженої величиною.

У разі збігу справжність користувача вважається встановленою, сервер запам'ятовує нове значення (надісланий користувачем) і зменшує на одиницю лічильник (n).

Оскільки функція f необоротна, перехоплення пароля і отримання доступу до сервера аутентифікації, не дозволяють дізнатися секретний ключ K і передбачити наступний одноразовий пароль.

Інший підхід до реалізації одноразових паролів полягає в генерації нового пароля через невеликий проміжок часу (наприклад, кожні 60 секунд), для чого

можуть використовуватися програми або smart-карти. Для цього необхідно виконання умов:

1. Сервер аутентифікації повинен знати алгоритм генерації паролів і асоційовані з ним параметри;
2. Годинники клієнта і сервера повинні бути синхронізовані.

Аутентифікація з використанням токенів можлива в таких випадках:

- На запит системи токен пред'являє їй секретне значення, що служить для підтвердження автентичності. Один раз, перехопивши цю відповідь, зловмисник може імітувати відповідь токена.
- Токен і система мають загальну, синхронізовану систему генерації одноразових паролів. На запит системи токен видає пароль, дійсний для даного проміжку часу. Система генерує в цей час свій варіант пароля, що і порівнює з отриманим.
- Токен зареєстрований в системі (вона знає його секретний параметр). Для аутентифікації вона формує випадкову величину, яку токен перетворює з використанням свого параметра. Система виконує аналогічне перетворення і порівнює результат з отриманим від токена. В цьому випадку перехоплення запиту і відповіді нічого не дає зловмиснику. І синхронізація токена і системи не потрібна.

Варіанти використання токена спільно з паролем:

- Пароль служить для доступу до токена, що без пароля не діє.
- Пароль разом з параметром токена служать основою для вироблення одноразових паролів.
- Токен генерує відповідь системі на запит з випадковою величиною на основі свого параметра і пароля користувача.

**4. Аутентифікація за допомогою біометричних даних**

Біометрія являє собою сукупність автоматизованих методів ідентифікації і аутентифікації людей на основі їх фізіологічних і поведінкових характеристик.

До числа фізіологічних характеристик належать особливості:

- відбитків пальців,
- сітківки та рогівки очей,
- геометрія руки та обличчя.

До поведінкових характеристик відносяться:

- динаміка підпису,
- стиль роботи з клавіатурою.

До характеристик, що включають фізіологію і поведінку, відносять аналіз особливостей голосу і розпізнавання мови.

У загальному вигляді робота з біометричними даними організована таким чином. Спочатку створюється і підтримується база даних характеристик потенційних користувачів. Для цього біометричні дані користувача знімаються, обробляються, і результат обробки (званий біометричним шаблоном) заноситься в базу даних. При цьому вихідні дані, такі як результат сканування пальця або рогівки, як правило, не зберігаються.

Надалі для ідентифікації та одночасно аутентифікації користувача процес зняття і обробки повторюється, після чого проводиться пошук в базі даних шаблонів.

У разі успішного пошуку особистість користувача і його достовірність вважаються встановленими. Для аутентифікації досить зробити порівняння з одним біометричних шаблоном, обраним на основі попередньо введених даних.

Зазвичай, біометрію застосовують разом з іншими аутентифікатором, такими як smart-карти. Іноді біометрична аутентифікація служить для активізації smart-карт – в цьому випадку біометричний шаблон зберігається на тій же карті.

Біометрія схильна тим же загрозам, що і інші методи аутентифікації.

Біометричний шаблон порівнюється не з результатом первісної обробки характеристик користувача, а з базою даних, що знаходиться в місці порівняння.

Біометричні методи не є більш надійними, чим база даних шаблонів.

Слід враховувати різницю між застосуванням біометрії на контрольованій території і в "польових" умовах.

Біометричні дані людини змінюються, так що база шаблонів потребує супроводу.

Але головна небезпека полягає в тому, що якщо біометричні дані виявляться скомпрометовані, доведеться як мінімум проводити істотну модернізацію всієї системи.

## 4.5 Методи визначення рівня інформаційного ризику

До одного з методів визначення рівня інформаційного ризику належить *аналіз інформаційних ризиків*. Аналіз інформаційних ризиків – процес комплексної оцінки захищеності інформаційної системи кількісними і якісними показниками. Однією з основних проблем аналізу інформаційних ризиків є оцінка вартості (ціни) ризиків. На даний момент не існує єдиної методики. Причини цього – відсутність достатнього обсягу статистичних даних про ймовірності реалізації конкретної загрози, неоднозначність оцінок вартості інформаційного ресурсу (матеріальних і нематеріальних). У цих умовах поширені якісні методи оцінки ризиків, засновані на експертних оцінках. Такий підхід ускладнює можливості моделювання ризикової ситуації і не дозволяє говорити про об'єктивність результату. У літературі визначають наступні чинники, що впливають на величину ризику.

**1. Міра тяжкості наслідків**, що можна виміряти у відсотковому відношенні від вартості ресурсу, якщо вона фіксована. Наприклад, якщо збиток в межах до 10% вартості ресурсу, то тяжкість наслідків низька, в інтервалі 11-30% - помірна, 31-80% - критична, більше 81% - катастрофічна.

а) Трудовитрати, необхідні для виправлення наслідків інциденту і залежні від вартості одного інциденту і кількості інцидентів за оцінюваний період. Трудовитрати на виправлення наслідків одного інциденту складаються з

трудовитрат на діагностування, документування, виправлення, повідомлення про результати.

б) Матеріальні збитки (втрачена вигода).

в) Репутаційний збиток.

**2. Оцінка ймовірності реалізації загрози** ранжується за шкалою від 1 до 5 (дуже низька, низька, середня, висока, дуже висока). Ймовірність залежить від рівня вразливості ресурсу до загрози та ефективності управління.

• Вразливість процесу, для якого ключова інформація є або входом, або виходом. Шкала включає значення низький, середній, високий. Вразливість означає наявність передумов для створення іншої загрози.

• Частка інцидентів, спровокованих загрозою, і спричинили збитки, в загальній кількості інцидентів, спровокованих даної загрозою, за минулий період. Шкала включає значення дуже низький (0-19%), низький (20-39%), середній (40- 60%), високий (61-80%), дуже високий (81-100%).

• Ефективність керування ранжується за шкалою від 1 до 5 згідно за класифікатором рівнів зрілості університету Carnegie Mellon. Відповідність понять ефективність управління і рівня зрілості компанії наведено в таблиці (табл. 4.1).

Проблема інформаційної безпеки для застосування зазначеної вище шкали підтверджується дослідженням компанії PricewaterhouseCoopers (PwC) на основі аналізу 21 підприємства і 68 проєктів. Організації з низькою ефективністю переважно володіють 1-2 рівнями зрілості. Організації з високою ефективністю володіють 3, 4, 5 рівнями зрілості. Крім того, аналітиками компанії PwC виявлено, що підвищення рівня зрілості дає істотне покращення результатів проєктів (30% компаній покращили свої результати більш ніж на 25%) [13].

Граничні значення у всіх цих випадках підбираються для кожного випадку індивідуально. Оцінка очікуваних втрат від конкретної загрози, на увазі застосування експертних оцінок і шкал, що містять лінгвістичні змінні,

може бути здійснена за допомогою теорії нечітких множин. Відомо застосування методу нечітких множин при оцінці ефективності інвестиційних проектів [24].

Таблиця 4.1

Оцінка рівня зрілості за класифікатором університету Carnegie Mellon

| Рівень зрілості | Критерії |
|---|---|
| 1 | Проблема формально не висувається |
| 2 | Проблема вирішується на основі практичних дій. Питання щодо ефективності захисту не розуміється. Серйозних порушень не відбувалося |
| 3 | Часткове впровадження стандартам і рекомендаціям. Приділяється увага питанням документування |
| 4 | Актуальні питання вимірювання параметрів, що характеризують режим інформаційної безпеки. Застосування кількісних методів аналізу ризиків |
| 5 | Ставляться і вирішуються різні варіанти оптимізаційних задач в області інформаційної безпеки |

## 4.6 Управління ризиками інформаційної безпеки

**(**сімейство стандартів ISO / IEC 27000**)**

В основі організації, планування й здійснення практичних дій щодо забезпечення безпеки є аналіз концепції загрози, оцінка характеру реальних і потенційних внутрішніх/зовнішніх небезпек і загроз, кризових ситуацій, а також інших несприятливих факторів. Система реальних і потенційних загроз не є постійною; загрози можуть з’являтися й зникати, наростати й зменшуватися, при цьому змінюватиметься їхня значимість для безпеки.

Друге видання скасовує та замінює перше видання (ISO 31000: 2009), що було технічно переглянуто.

Основні зміни в порівнянні з попереднім виданням:

• - огляд принципів управління ризиками, що є ключовими критеріями його успіху;

• - виділення окремого керівництва з боку вищого керівництва і інтеграція управління ризиками, починаючи з управління організацією;

• - акцентування на ітеративну природу управління ризиками, відзначаючи, що новий досвід, знання і аналіз можуть привести до перегляду елементів процесу, дій і засобів контролю на кожній стадії процесу;

• - раціоналізація контенту з наданням більшої уваги підтримці моделі відкритих систем у відповідності з різними потребами і контекстами.

Цей документ призначений для використання людьми, які створюють і захищають цінності в організаціях шляхом управління ризиками, прийняття рішень, постановки і досягнення цілей і підвищення ефективності.

Багато організацій стикаються із зовнішніми і внутрішніми факторами і впливами, які заважають впевнено досягати своїх цілей.

Управління ризиками носить ітеративний характер і допомагає організаціям визначати стратегію, досягати мети і приймати обґрунтовані рішення.

Управління ризиками є частиною управління і лідерства і має основоположне значення для управління організацією на всіх рівнях. Це сприяє вдосконаленню систем управління.

Управління ризиками є частиною всієї діяльності, пов'язаної з організацією, і включає взаємодію з зацікавленими сторонами.

Управління ризиками враховує зовнішній і внутрішній контекст організації, включаючи поведінку людини і культурні фактори.

Управління ризиками засноване на принципах, структурі і процесі, викладених в цьому документі, як показано на рис. 4.1. Ці компоненти можуть

вже існувати повністю або частково всередині організації, проте їх може знадобитися адаптувати або покращити, щоби управління ризиками було ефективним, дієвим і послідовним.

Управління безпекою великих організацій, що використовують інформаційні та телекомунікаційні технології, рекомендується здійснювати на основі стандартів BS 7799/ISO 17799 ISO/IEC 27001. На сьогодні активно використовується стандарт ISO 17799 і відбувається поступовий перехід до стандартів серії 27001. Управління безпекою націлено на захист усіх складових, що сприяють здійсненню бізнес-процесу, який організовано на підприємстві (рис. 4.1).

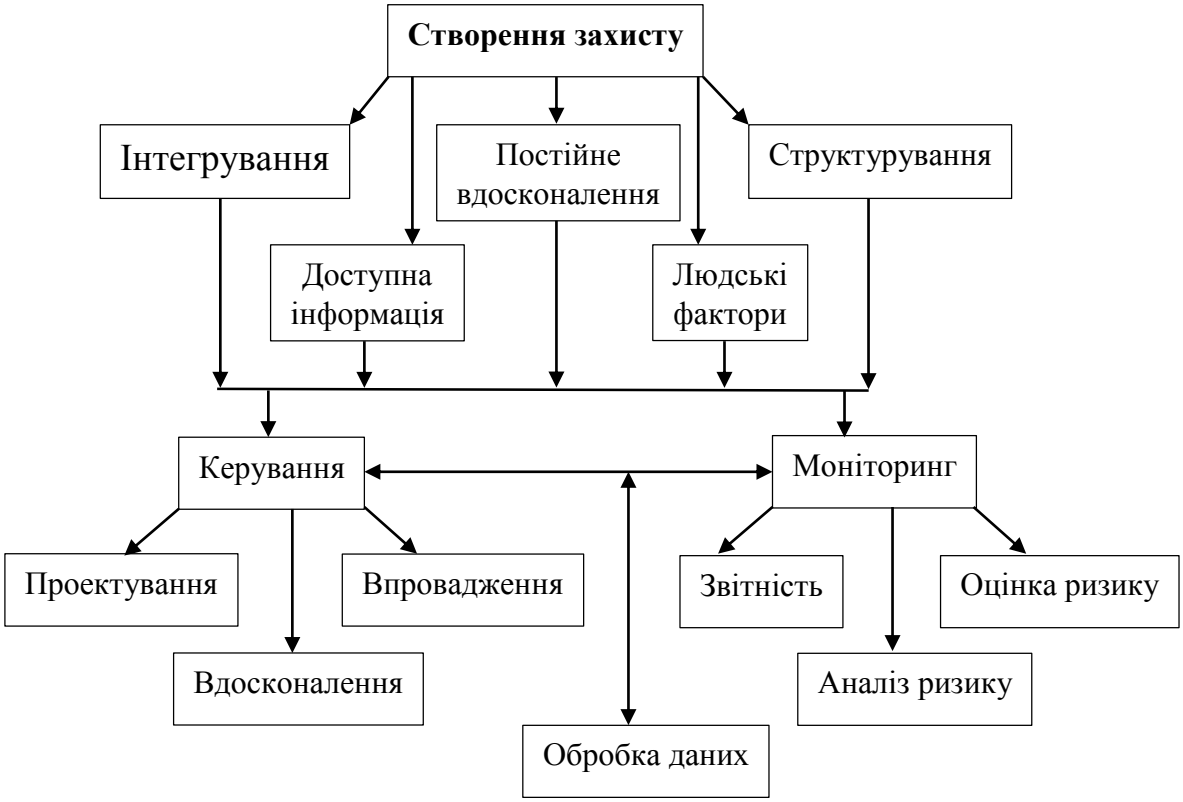


Рис 4.1. Принципи, структура і процес управління безпекою

Серія 27001 являє собою модель системи менеджменту в сфері інформаційної безпеки (СМІБ, Information Security Management System, ISMS). Як і будь-яка сучасна система менеджменту, СМІБ – це набір організаційних заходів і процедур управління і вона не є, по суті, технічним стандартом. В

основі стандарту полягає процесний підхід до розробки, реалізації, експлуатації, моніторингу, аналізу, супроводу та покращанню СМІБ організації. Він складається зі створення та використання системи процесів управління, що взаємопов'язані у безперервному циклі планування, використання, перевірки та покращання СМІБ (рис. 4.1, частина бізнес-процесу). Додатково в групі стандартів рекомендовано перелік механізмів захисту інформації програмно-технічного рівня, що можуть використовуватися на різних стадіях здійснення бізнес-процесу (рис. 4.2, частина технології).

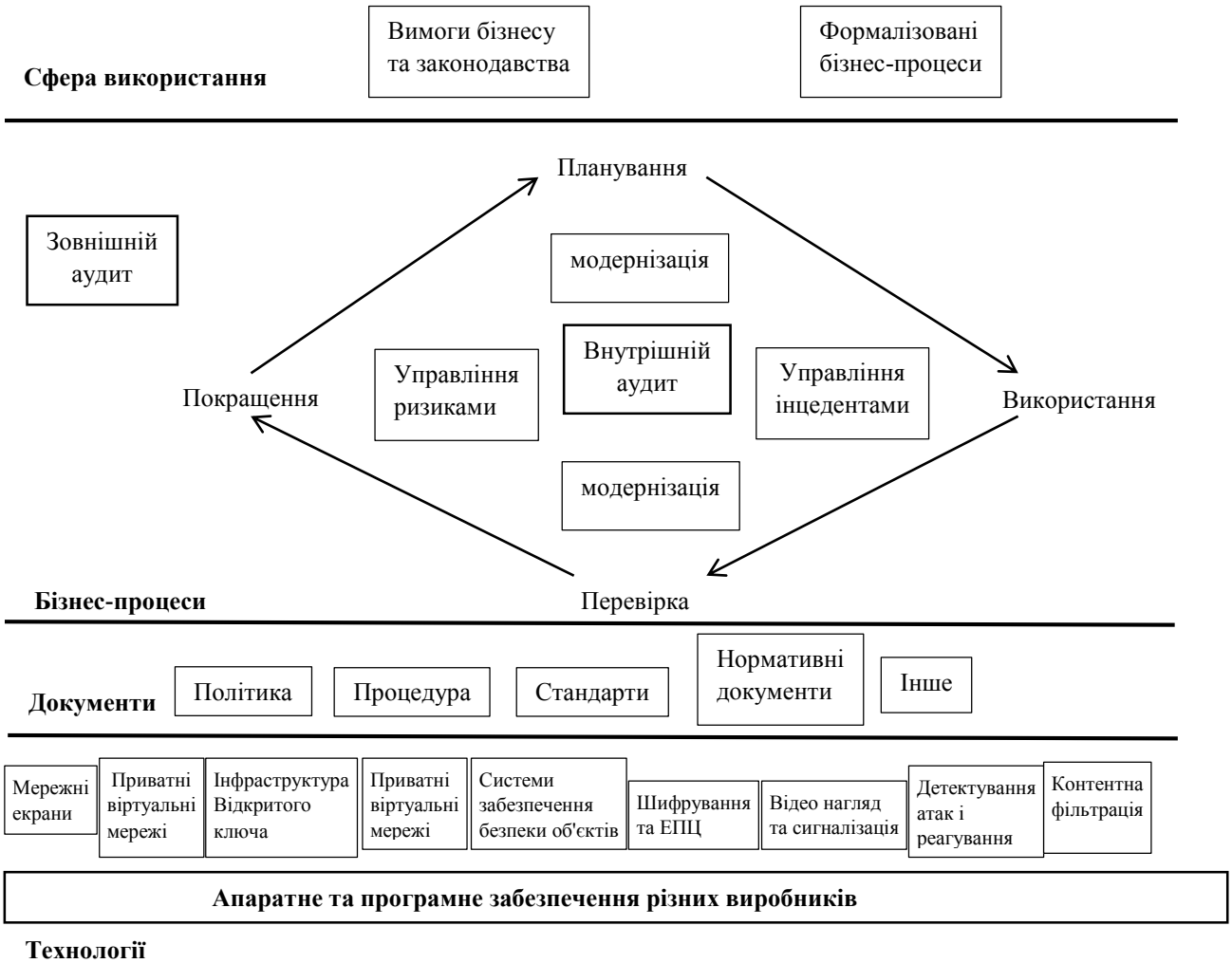


Рис. 4.2. Загальна схема управління безпекою бізнес-процесів на основі телекомунікацій

В Україні діють наступні стандарти по технічному захисту інформації:

– ДСТУ 3396.0-96. "Захист інформації. Технічний захист інформації. Основні положення". Цей стандарт встановлює об'єкт, мету, організаційні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) і державі, а також категорії нормативних документів системи ТЗІ.
– ДСТУ 3396.1-96. "Захист інформації. Технічний захист інформації. Порядок проведення робіт". Стандарт встановлює вимоги до порядку проведення робіт з технічного захисту інформації.
– ДСТУ 3396.2-96. "Захист інформації. Технічний захист інформації. Терміни й визначення". Даний стандарт встановлює терміни й визначення понять у сфері технічного захисту інформації.

Серед міжнародних стандартів про інформаційну безпеку найбільш відомим є британський – BS 7799, розроблений Британським інститутом стандартів (*British Standards Institution – BSI*). Стандарт BS 7799 складається із двох частин.

Серія стандартів з менеджменту інформаційної безпеки ISO / IEC 27000 розробляється технічним комітетом ISO / IEC JTC 1 підкомітетом SC 27.

Система менеджменту інформаційної безпеки (СМІБ) містить в собі вимоги щодо реалізації та вдосконалення систем управління захистом інформації і ґрунтується на моделі PDCA (Plan-Do-Check-Act):

- створення – ідентифікація активів, менеджмент ризиків;
- впровадження – етап реалізації відповідних заходів з управління безпекою;
- перевірка – моніторинг і аналіз;
- дія – підтримання в робочому стані і покращення.

Виходячи з цього видно, що крім розробки правил управління і забезпечення безпеки, не менш важливо забезпечити циклічність всіх процесів з управління безпекою, щоби всі процедури послідовно проходили етапи моделі

PDCA. Саме це говорить про відповідність системи управління стандарту ISO 27001 і свідчить про готовність до сертифікації СМІБ.

Виконання вимог стандарту ISO / IEC 27001 головним чином дозволяє мінімізувати ризики втрат активів підприємства / організації, а отже скоротити фінансові втрати.

Стандарт ISO / IEC 27001 призначений для сертифікації систем інформаційної безпеки.

Сертифікація системи менеджменту інформаційною безпекою (сертифікація СМІБ) – ефективне управління бізнес-процесами організації, інформаційними ризиками, а також свідоцтво про стійкий розвиток і надійність компанії, що в свою чергу дає позитивне ставлення бізнес-партнерів.

СМІБ відповідно до стандарту ISO / IEC 27001 – це частина загальної системи менеджменту компанії.

Сімейство стандартів ISO 27000 включає в себе наступні документи, що стосуються систем менеджменту ІБ:

ISO / IEC 27001 Information security management systems. Requirements – Системи менеджменту інформаційною безпекою. Вимоги.

ISO / IEC 27000 Information security management systems. Overview and vocabulary – Системи менеджменту інформаційної безпеки. Огляд і термінологія.

ISO / IEC 27003 Information Security Management Systems. Guidance – Системи менеджменту інформаційної безпеки. Керівництво.

ISO / IEC 27004 Information security management. Measurement – Вимірювання ефективності системи менеджменту інформаційної безпеки.

ISO / IEC 27006 Requirements for bodies providing audit and certification of information security management systems – Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційною безпекою.

ISO / IEC 27007 Guidelines for Information Security Management Systems auditing (FCD) – Керівництво для аудиту СМІБ.

Основним механізмом СМІБ є періодичний аналіз ризиків інформаційної безпеки. Аналіз ризиків може здійснюватися на основі методів CORAS, CRAMM, Magerit, Mehari, Octave та інших. Аналіз ризиків має доповнюватися процедурами аудиту, що сприяє глибшому розумінню бізнес-процесів, які опановані в організації. Аудит може проводитися, наприклад, на основі стандарту CobiT (Control Objectives for Information and related Technology, цілі управління для інформаційних та суміжних технологій).

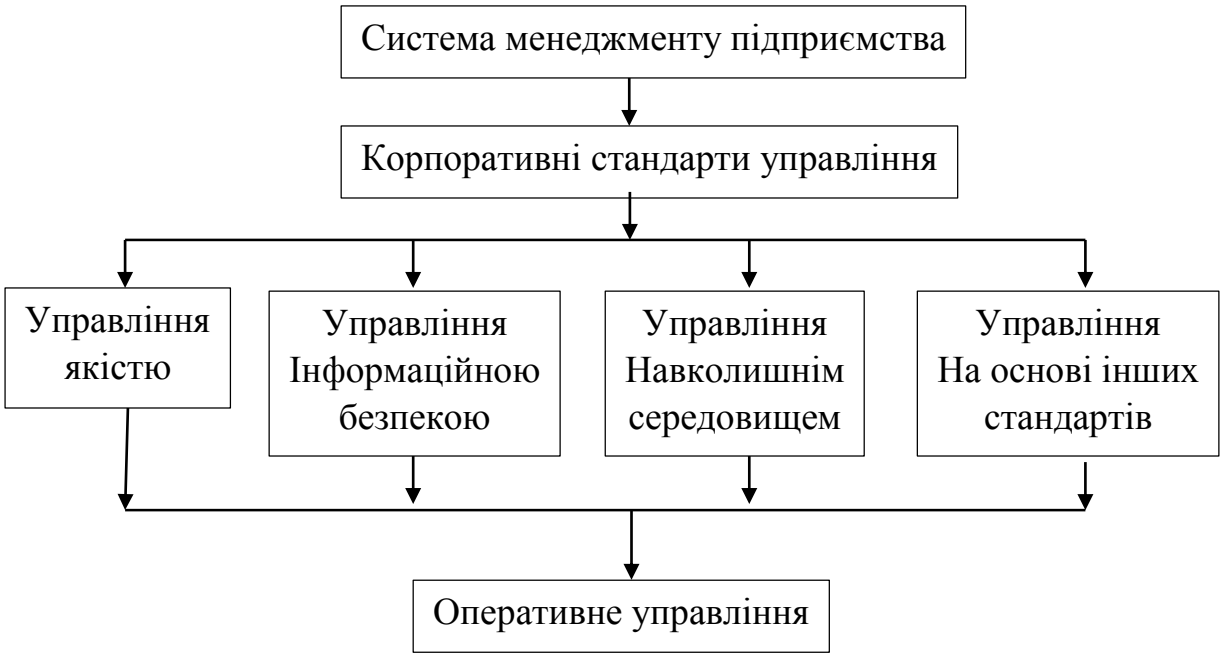


Рис. 4.3. Місце системи управління інформаційною безпекою в системі менеджменту організації

Верхівка керівництва організації також здійснює процес управління СМІБ прийняттям рішень на основі результатів аналізу ризиків, результатів внутрішнього аудиту й інших механізмів СМІБ. З погляду процесів управління, СМІБ належить до загальної системи менеджменту організації та надає додаткові механізми управління щодо забезпечення захисту критичної інформації (рис. 4.3). Положення управління інформаційною безпекою формують політику безпеки організації — позицію керівництва щодо питань з

захисту процесів накопичення, зберігання, передачі та знищення інформаційних цінностей, відповідності й організаційним зобов'язанням.

**Контрольні запитання**

1. Що визначає міжнародний стандарт ISO / IEC 17799: 2005?
2. Організаційні засоби захисту інформації.
3. Що таке принцип компенсації?
4. Які використовують засоби захисту інформації?
5. Що таке механізм ідентифікації?
6. Що таке механізм аутентифікації?
7. Які паролі потрібно використовувати?
8. Як відбувається біометрична аутентифікація?

# ТЕМА 5. КІБЕРЗЛОЧИННІСТЬ

## 5.1. Характеристика кіберзлочинності

**Кіберзлочин** – дія, що порушує закон, який вчинено з використанням інформаційно-комунікаційних технологій (ІКТ) і/або націлене на мережі, системи, дані, веб-сайти і/або технології, або сприяє вчиненню злочину. Кіберзлочин відрізняється від традиційного злочину тим, що він «не визнають фізичні або географічні кордони» і можуть відбуватися з меншими зусиллями, більшою легкістю і з більшою швидкістю, ніж традиційні злочини (хоча це залежить від виду кіберзлочинів і виду традиційного злочину, з яким вони порівнюється).

Коли ІКТ є частиною способу вчинення злочину, кіберзлочинність включає в себе традиційний злочин (наприклад, шахрайство і крадіжку), вчинення якого тим чи іншим чином сприяють мережа Інтернет та цифрові технології.

Кіберзлочини вчиняються фізичними особами, групами осіб, комерційними організаціями і державами. Хоча ці суб'єкти можуть застосовувати схожі тактичні методи (наприклад, використовувати шкідливе програмне забезпечення) і атакувати схожі цілі (наприклад, комп'ютерну систему), вони мають різні мотиви і наміри при здійсненні кіберзлочинів.

Зловмисники, які здійснювали кіберзлочини, націлювалися на фізичних осіб і вимагали від них невеликі суми грошей, але потім стали націлюватися на комерційні підприємства, компанії і організації і, нарешті, на інших суб'єктів в приватному і державному секторах, що надають важливі послуги (наприклад, лікарні). Атака з використанням вірусу-вимагача у 2017 році торкнулася приблизно 150 країн, в тому числі понад 80 організацій NHS (Національної служби охорони здоров'я) [1] в одній тільки Англії, спричинило за собою

скасування майже 20 000 записів на прийом; 600 клінік лікарів загальної практики були змушені повернутися до паперового документообігу, а п'ять лікарень переадресовували карети швидкої допомоги в інші лікарні, оскільки більше не могли надавати термінову медичну допомогу.

Кіберзлочинність є одним з видів транснаціональної злочинності, виконавці і жертви якої можуть перебувати в будь-якій точці світу, де є підключення до мережі Інтернету. У зв'язку з цим слідчим, який веде розслідування кіберзлочинів, найчастіше потрібен транскордонний доступ до даних і обмін ними. Це завдання може бути виконано у разі, якщо запитувані дані зберігаються постачальниками послуг і приймаються заходи, що дозволяють правоохоронним органам отримувати доступ до даних.

*Основними правовими проблемами* при розслідуванні кіберзлочинів і судових переслідуваннях кіберзлочинців є:

- ✓ різні правові системи, існуючі в різних країнах;
- ✓ відмінності в національних законодавствах про кіберзлочинність;
- ✓ відмінності в нормах доказового права і кримінального судочинства (наприклад, в процедурах отримання доступу до цифрових доказів правоохоронними органами; наприклад, на підставі законного розпорядження, такого як ордер на обшук, або без нього);
- ✓ відмінності в охопленні та географічної застосовності регіональних і багатосторонніх договорів про боротьбу з кіберзлочинністю;
- ✓ відмінності в підходах до захисту даних і дотримання прав людини.

Кіберзлочинці часто використовують як технічні, так і соціальні підходи до скоєння злочинів. Деякі види кіберзлочинів важко запобігти, однак користувачі технологій можуть робити певні дії, щоб захистити себе (у якійсь мірі) від кіберзлочинності. Інтерпол [28] розміщує численні керівництва з інформування громадськості та профілактики злочинності на своєму веб-сайті. Проте, навіть маленькі дії здатні привнести великі зміни.

*Поради, які слід враховувати при підключенні до мережі Інтернет.*

- ✓ Регулярно оновлюйте операційну систему і встановлене програмне забезпечення.
- ✓ Регулярно видаляйте програмне забезпечення, яке ви більше не використовуєте.
- ✓ Використовуйте антивірусну програму, розроблену компанією з надійною репутацією.
- ✓ Не завантажуйте програмне забезпечення, фільми або музику з сайтів загального доступу – вони часто мають шкідливу програму.
- ✓ Не завантажуйте вкладення і не натискайте на посилання від невпізнаних відправників.
- ✓ Не надавайте особисту інформацію на невідомих веб-сайтах.
- ✓ Підтвердіть правильність адресу веб-сайту при введенні фінансової інформації.

## 5.2. Стан кіберзлочинності в Україні

Сучасні процеси цифрової трансформації економіки пов’язані з розвитком бізнес-моделей, що використовують цифрові платформи. Фактично протягом останнього десятиріччя відбувається революція платформ. Особливістю цифрових платформ є об’єднання різних груп споживачів, виробників, власників ресурсів на одному віртуальному майданчику. Вітчизняний цифровий капітал перебуває на стадії формування, але вже спостерігається велика кількість позитивних прикладів, оскільки можливості розвитку цифрової економіки в Україні пов’язані з розширенням використання цифрових платформ, що є точками зростання сучасної інформаційної економіки, при цьому перспективним напрямом розвитку цифрових платформ виступає технологія блокчейн (ланцюжок блоків транзакцій) [2].

Організована кіберзлочинність може бути асоційована не тільки з проблемами інформаційної безпеки, але й із загрозами для державної безпеки,

військово-промислового і виробничого комплексів, інфраструктури життєзабезпечення. Характеризуючи стан організованої злочинності у сфері економіки, доцільно виділяти її в окрему категорію для вивчення злочинності саме у сфері «цифрової економіки». Оцінка впливу цифрової економіки на національну та світову економіку дозволяє констатувати, що актуальним залишається суцільна модернізація злочинності, що постійно вдосконалюється у рамках активної суцільної електронізації та цифровізації суспільства.

Найбільш поширеними напрямами загроз інформаційній безпеці є шахрайські шкідливі платіжні програми, що ускладнюють, порушують або блокують роботу банківських терміналів, використовуються для крадіжки даних громадян, взлому паролей від банківських карток для заволодіння коштами цих громадян, шахрайства у сфері електронної комерції та застосування інших кримінальних інструментів і послуг в різноманітніших сферах злочинної діяльності.

Зростання ділової активності із застосуванням хмарних технологіях, придбання товарів через мережу Інтернет, Інтернет-банкінгу, он-лайн розрахунки сприяють зростанню економічних злочинів із застосуванням ІТ-технологій.

До ефективних засобів протидії злочинності у сфері інформаційної безпеки пропонується розробка, створення та впровадження сучасних систем захисту інформації, а також вдосконалення існуючої законодавчої та нормативно-правової бази, здатної забезпечити протидію сучасним кіберзагрозам.

Для підвищення ефективності боротьби з кіберзлочинністю, розвинені країни світу ведуть відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Інциденти в сфері кібербезпеки позначаються на життєдіяльності споживачів інформаційних і багатьох інших послуг та кібератаки, націлені на різноманітні об’єкти інфраструктури систем електронних комунікацій чи управління технологічними процесами.

Розглядаючи стан кіберзлочинності у світі, необхідно сказати, що відповідно до даних рейтингу GCI-2019 [1], перші сходинки належать таким країнам: Великобританії, США, Франції. Україна станом на 2019 рік займала 54 місце серед 193 країн (табл. 5.1), піднявшись на 5 позицій (59 місце) у порівнянні із 2018 роком.

Таблиця 5.1.

Стан кіберзлочинності у світі у 2019 році

| Місце | Країна | Бал |
|---|---|---|
| 1 | Великобританія | 0,931 |
| 2 | США | 0,926 |
| 3 | Франція | 0,918 |
| 4 | Литва | 0,908 |
| 5 | Естонія | 0,905 |
| 29 | Польща | 0,815 |
| 53 | Молдова | 0,662 |
| **54** | **Україна** | **0,661** |
| 56 | Кіпр | 0,652 |

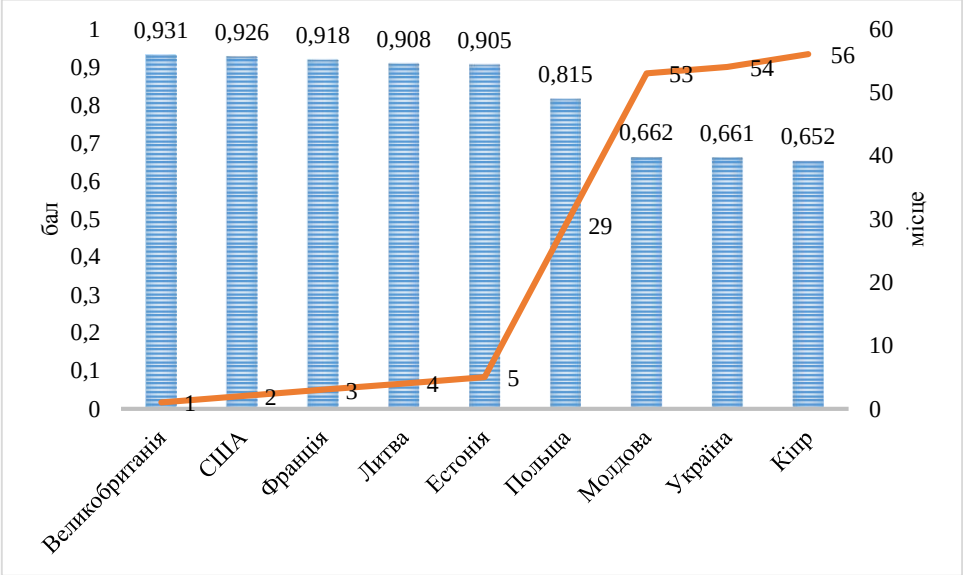


Рис. 5.1. Стан кіберзлочинності у світі у 2019 році

Позитивні зміни відбулися:

- у побудові законодавчої бази для гарантування кібербезпеки держави;
- стійкість державних ініціатив щодо підвищення кібербезпеки у сфері інформаційно-комунікаційних технологій;
- значне покращення кіберстійкості організацій за останній рік, незважаючи на збільшення більш ніж удвічі цілеспрямованих кібератак.

Але у порівнянні показників рейтингу GCI-2019 України з такими, як Литва, яка посіла 4 позицію, Естонія – 5, Грузія – 18, Казахстан – 40, Латвія – 44, Молдова – 53 (рис. 5.1), то система боротьби із кіберзлочинністю значно краще побудована, тобто кіберстійкість цих країн є вищою [1].

Рейтинг кіберзлочинності GCI-2019 побудовано на дослідженні основних показників, що відображають стан кібербезпеки в країні. Узагальнений індекс орієнтований на суспільні аспекти національної кібербезпеки, що здійснюються центральним урядом. Мета індексу полягає у вимірі готовності країн до запобігання кіберзагроз та готовності управляти ними і контролювати кібер-інциденти. Показники пов'язані з кібербезпекою і такими складовими інформаційного суспільства як електронна ідентичність, цифровий підпис та існування безпечного середовища для електронні послуги. Індекс має механізм оцінки та ранжування.

Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки посилюють спроможність України у сфері кібербезпеки і відповідають національним інтересам, для реалізації поглиблення співпраці з ЄС.

Кількість кіберзлочинів за статтею 361 з 2015 по 2019 роки суттєво зріс. Значний скачок відбувся у 2017 році, вірус Пєтя. Після цього кількість кіберзлочинів має тенденцію до зростання. Так, у 2017 році було зафіксовано 1 795 справ, у 2018 році – 1 023, у 2019 – 1 450, а за прогнозними розрахунками у 2020 році їх вже може бути 1 754 (рис. 5.2).

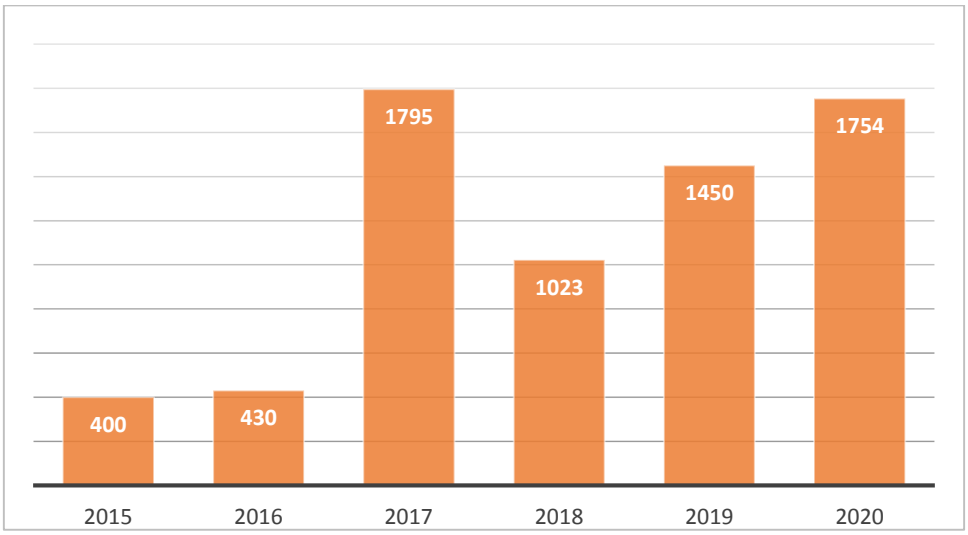


Рис. 5.2. Кількість кіберзлочинів у 2015-2020 роках

Забезпечення кібербезпеки можливо тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації. З метою вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та військових цілях країна має активізувати участь в організації спільних міжнародних проєктів з нарощування кібернетичного потенціалу.

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, що здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО.

Важливо підвищувати рівень обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання відповідних освітніх програм. За умов небезпек, що склалися нині у кіберпросторі, організаціям потрібно змінити ставлення до інформаційної безпеки. А для цього треба підвищувати обізнаність про важливість інвестування у кібербезпеку як невід'ємну складову будь-якої національної стратегії розвитку ІКТ.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту

інформації України CERT-UA функціонує для взаємодії з Cisco Talos Intelligence Group та іншими державами-членами CERT щодо питань подолання наслідків кібератак на інформаційну інфраструктуру, виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектору України та іноземних партнерів. Відповідно до закону "Про основні засади забезпечення кібербезпеки України" (2017), CERT-UA та Центр реагування на кіберзлочини координують заходи, спрямовані на оперативне реагування на кібератаки, а також контролюють впровадження контрзаходів, що передбачають мінімізацію вразливості систем зв'язку.

Україна бере участь у роботі Агентства ЄС з кібербезпеки, Європейського центру з досліджень і компетенції в сфері кібербезпеки, а також у навчаннях з реалізації Спільної оперативної схеми реагування ЄС і держав-членів на кібератаки.

Загалом усі заходи, що проводить світова спільнота у сфері кібербезпеки, – це спроба допомогти країнам вдосконалити цю сферу, а також мотивувати їх на вжиття заходів для покращення їхнього рейтингу, допомагаючи у такий спосіб підвищити загальний рівень кібербезпеки в усьому світі. Рейтинг "Глобального індексу кібербезпеки" допомагає аналізувати та використовувати найкращі засоби боротьби в IT-сфері для подолання та упередження кіберзлочинів та зростання стану їх кібербезпеки.

Потреба координації та переорієнтації наукових досліджень і розробок у сфері інформаційної безпеки, вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробка технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливу атаку та локалізацію джерел загрози є актуальною.

Ця проблема потребує ефективного і комплексного вирішення питань на національному, регіональному та міжнародному рівнях для запобігання кіберзлочинів. Лише співпраця між державами для запобігання постійним загрозам в Інтернеті і подолання проблем кібербезпеки забезпечить належний рівень захисту від сучасних інформаційних загроз.

Виходячи з міжнародного досвіду, оцінкою вартості інформаційного капіталу може бути ринкова капіталізація цифрових платформ, що поступово впроваджуються в Україні. Актуальним є питання безпеки особистих даних, збір великих масивів даних, дистанційна праця.

Сучасні світові тенденції поширення кіберзлочинності та посилення кібератак свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що у свою чергу зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Ситуація, що склалася на сьогоднішній день з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами, розробки інформаційних систем та методів, спрямованих на забезпечення кібербезпеки країни.

Необхідними задачами є розробка національної стратегії з кібербезпеки, що міститиме тактичні та стратегічні пріоритети і завдання у даній сфері для державних органів. Отже, питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, а тому потребує подальшого розгляду.

## 5.3. Боротьба із кіберзлочинами

Від комп’ютерних злочинів страждають всі країни світи. Національна кібербезпека України найбільше стикається з комп’ютерними злочинами в економічній, інформаційній та фінансово-кредитній сферах. Застосування сучасної системи електронного управління повітряним, автомобільним,

залізничним, річковим та морським рухом, поширення телекомунікаційної мережі в освіті, науці і практиці, впровадження системи електронних платежів, використання комп'ютерів у діяльності органів законодавчої, виконавчої, судової влади, правоохоронних органів та керуванні військами, розширили сферу діяльності для хакерів, кракерів (хто порушує безпеку системи), кібершахраїв та кібертерористів.

Із розвитком глобальних електронних комп'ютерних мереж набула поширення практика електронного промислового шпигунства. Саме тому проблеми розробки систем захисту та збереження приватної, державної, службової і комерційної таємниці набувають сьогодні особливого значення. Багато питань виникає у зв'язку з крадіжками різного роду послуг, зокрема, вторгнення до телефонних мереж та незаконна торгівля послугами зв'язку.

Мережа Інтернет широко використовують торговці піратським програмним забезпеченням, порнографією, зброєю та наркотиками для вчинення власних злочинних дій, обміну інформацією, координації дій тощо. Електронні комп'ютерні мережі, можуть стати й об'єктом нападу кібершахраїв та кібертерористів.

Сьогодні особлива увага приділяється саме питанням міжнародного співробітництва при запобіганні, протидії й розслідуванні комп'ютерних злочинів. У багатьох країнах світу для запобігання і протидії цим видам злочинів створені спеціалізовані кіберпідрозділи, що займаються виявленням, розслідуванням комп'ютерних злочинів та збором іншої інформації з цього питання на національному рівні. Саме спеціалізовані національні поліцейські підрозділи утворюють головне ядро сил протидії міжнародній комп'ютерній злочинності. Такі підрозділи вже створені і діють тривалий час у Сполучених Штатах Америки, Канаді, Великобританії, Німеччині, Індії, Китаї, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі, Японії та багатьох інших країнах світу.

Законом «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року законодавчо закріплені доктринальні засади забезпечення кібербезпеки нашої країни, а також закладені правові основи діяльності Національного координаційного центру кібербезпеки. Згідно з положеннями цього Закону Національний координаційний центр кібербезпеки є робочим органом Ради національної безпеки і оборони України, який здійснює координацію та контроль за діяльністю суб'єктів сектора безпеки й оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

У Законі «Про основні засади забезпечення кібербезпеки України» передбачено створення урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA. Основними її завданнями є:

- ✓ накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;
- ✓ надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;
- ✓ організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;
- ✓ взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;
- ✓ взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків;
- ✓ взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та

організаціями незалежно від форми власності, що провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

✓ опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

✓ сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України, у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Забезпечення функціонування діяльності CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог чинного законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Слід зазначити, що в багатьох провідних країнах світу вже сформовані і діють загальнодержавні системи кібернетичної безпеки критичної інфраструктури — як найбільш оптимальні організаційні структури, здатні в короткий проміжок часу швидко акумулювати сили та засоби різних державних і правоохоронних органів та установ приватного сектора для протидії кіберзагрозам, кібератакам, кіберзлочинам, кібершпигунству, кібертероризму. В США, Великій Британії, Канаді довгий час діють потужні кіберполіцейські структури (NIPS, FBI, FATF і тощо). Сьогодні в Сполучених Штатах Америки, Польщі та інших країнах світу створено кібервійська.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад

внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена Законом «Про основні засади забезпечення кібербезпеки України» та іншими законами України. Загальна декларація прав людини, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України фактично закладають міцний міждержавний правовий, організаційний, процедурний фундамент забезпечення кібербезпеки інформаційного простору в Україні, Європі і світі.

**Контрольні питання**

1. Що називають кіберзлочином?
2. Які основні правові проблемами при розслідуванні кіберзлочинів?
3. Найбільш поширені напрями загроз інформаційній безпеці.
4. Які закони для протидії кіберзлочинності існують в Україні?

# ТЕМА 6. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

## 6.1. Інформаційна безпека як інтегрована складова національної безпеки

Інформаційна безпека є інтегрованою складовою національної безпеки, що розглядають як пріоритетну функцію держави. Інформаційна безпеки, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій. Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об’єктивної та якісної інформації.

Рівень інформаційної безпеки держави, значною мірою, зумовлений рівнем її інформаційної інфраструктури. На жаль низький загальний рівень інформаційної інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його неконкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу

іноземним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що сьогодні трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованих на руйнування моральних цінностей, свідомості української нації [35].

Отже, національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, що становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури. Загрози національній безпеці України в інформаційній сфері – сукупність умов та чинників, що становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [35]. Як зазначено у Законі України “Про основи національної безпеки” однією з основних загроз інформаційній безпеці є “намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації” [37]. У Доктрині інформаційної безпеки України, визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ , а також мережу Інтернет; деструктивні інформаційні впливи, що спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [44].

З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних та потенційних загроз в інформаційному просторі України, Рада національної

безпеки і оборони України ухвалила рішення “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України”. У документі зазначено, що РНБО, враховуючи необхідність вдосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, вирішила: розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів; посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки; вжити заходів щодо забезпечення поширення у світі об’єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, через створення відповідного медіахолдингу для підготовки якісного конкурентоздатного інформаційного продукту; розробити порядок аналізу інформаційних матеріалів іноземних ЗМІ, що мають представництва в Україні, з метою впровадження дієвого механізму акредитації журналістів; вжити заходів до активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності [6].

Таким чином, інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політична ситуація у світі; внутрішньополітична ситуація в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо.

Загрози інформаційній безпеці здебільшого супроводжують виникнення й реалізацію загроз в економічний і політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційні сфері є передусім засобом досягнення інших цілей. Інформаційні загрози пов’язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі,

дискредитацією правоохоронної системи й органів державної влади загалом, заподіянням шкоди честі, гідності та ділової репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов щодо управління масовою свідомістю.

При цьому потенціал інформаційної сфери через її інтегрувальний характер і здатність «проникнення» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком виявів кіберзлочинності), однак успішно використовується представниками організованих злочинних співтовариств і політичними супротивниками нашої держави.


Рис. 6.1 Структура обмежень, що погіршують підприємницький клімат

Стратегічне інформаційне протистояння сьогодні становить небезпечний компонент гібридної війни, розгорнутої Росією проти України, причому головною загрозою інформаційній безпеці нашої держави сьогодні залишається

загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості з метою нав’язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності.

## 6.2. Доктрина інформаційної безпеки України

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Розглянемо особливості Доктрини «Інформаційної безпеки України» від 25 лютого 2017 року №47/2017.

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року №96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [8].

**Доктрина інформаційної безпеки України** (далі – Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року №287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

**Метою Доктрини** є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному

інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Доктрина базується на принципах дотримання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

**Національними інтересами України в інформаційній сфері** є:

*1) життєво важливі інтереси особи*:

✓ забезпечення конституційних прав і свобод людини на збір, зберігання, використання та поширення інформації;

✓ забезпечення конституційних прав людини на захист приватного життя;

✓ захищеність від руйнівних інформаційно-психологічних впливів;

*2) життєво важливі інтереси суспільства і держави*:

✓ захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

✓ захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

✓ всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

✓ забезпечення вільного обігу інформації, крім випадків, передбачених законом;

✓ розвиток та захист національної інформаційної інфраструктури;

✓ збереження і примноження духовних, культурних і моральних цінностей Українського народу;

- ✓ забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;
- ✓ вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;
- ✓ зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;
- ✓ розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;
- ✓ формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;
- ✓ створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;
- ✓ розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;
- ✓ безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;
- ✓ розвиток системи стратегічних комунікацій України;
- ✓ ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;
- ✓ забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;
- ✓ захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;
- ✓ формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

- ✓ розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

*Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері* є [8]:

- ✓ здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;
- ✓ проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;
- ✓ інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;
- ✓ інформаційне домінування держави-агресора на тимчасово окупованих територіях;
- ✓ недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;
- ✓ неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу (контентного елементу інформаційної та пропагандистської діяльності держави), недостатній рівень медіа-культури суспільства;

✓ поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

**Пріоритетами державної політики в інформаційній сфері** мають бути [8]:

1) *щодо забезпечення інформаційної безпеки*:

✓ створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

✓ удосконалення повноважень державних регуляторних органів, що здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

✓ законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, що загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

✓ визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

- ✓ оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, що не є підписантами зазначеної Конвенції;
- ✓ створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;
- ✓ розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;
- ✓ забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;
- ✓ розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;
- ✓ побудова дієвої та ефективної системи стратегічних комунікацій;
- ✓ розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;
- ✓ боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;
- ✓ посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;
- ✓ виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

✓ унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;

✓ проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;

✓ недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

*2) щодо забезпечення захисту і розвитку інформаційного простору України*, а також конституційного права громадян на інформацію:

✓ стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

✓ забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

✓ створення системи мовлення територіальних громад, що сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

✓ підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

✓ розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

✓ комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

- ✓ підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;
- ✓ удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;
- ✓ задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;
- ✓ повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;
- ✓ формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;
- ✓ пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

*3) щодо відкритості та прозорості держави перед громадянами*:

- ✓ розвиток механізмів електронного урядування;
- ✓ сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;
- ✓ інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;
- ✓ проведення реформи урядових комунікацій;
- ✓ розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;
- ✓ сприяння формуванню культури суспільної дискусії;

*4) щодо формування позитивного міжнародного іміджу України:*

- ✓ ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені;
- ✓ розвиток публічної дипломатії, у тому числі культурної та цифрової;
- ✓ активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;
- ✓ сприяння поширенню та розвитку системи іномовлення України;
- ✓ створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;
- ✓ постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;
- ✓ недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;
- ✓ реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»;
- ✓ участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;
- ✓ запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини» [8].

Таким чином, Доктрина інформаційної безпеки України передбачає постійний моніторинг загроз національним інтересам і національній безпеці в інформаційній сфері.

**Контрольні питання**

1. Інформаційна безпека як інтегрована складова національної безпеки.
2. Рівень інформаційної безпеки держави.
3. Загрози національній інформаційній безпеці України.
4. Мета і завдання Доктрини інформаційної безпеки України.
5. Національні інтереси України в інформаційній сфері.
6. Напрямки розвитку інформаційного суспільства держави.
7. Особливості розвитку системи стратегічних комунікацій України.
8. Завдання державної інформаційної політики щодо забезпечення інформаційної безпеки.
9. Особливості захисту технологічної інфраструктури забезпечення інформаційної безпеки України.
10. Боротьба з дезінформацією та деструктивною пропагандою інших країн.
11. Забезпечення захисту і розвитку інформаційного простору України.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Аналитический обзор инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств (второе полугодие 2012). М., Банк России, 2013. О. А. Мирсанова, А. В. Павлов. О двух подходах оценки информационных рисков 33
2. ГОСТ 27.310-95 Межгосударственный стандарт. Надежность в технике. Анализ видов, последствий и критичности отказов. М.: ИПК Изд-во стандартов, 2002.
3. ГОСТ Р 59901.12-2007 Менеджмент риска. Метод анализ риска и последствий отказов. М.: ФГУП «СТАНДАРТИНФОРМ», 2008.
4. Завгородний В.И. Информационная и экономическая безопасность предприятия // Прикладная информатика. 2006. № 2. С. 107—113.
5. Завгородний В.И. Системное управление информационными рисками. Выбор механизмов защиты // Проблемы управления. 2009. № 1. С. 53—58.
6. Зинкевич В., Штатов Д. Методы измерения операционного риска // Бухгалтерия и банки, 2006. № 12.
7. Львова А.В. Метод анализа и управления рисками безопасности защищенной информационной системы: диссертация на соискание степени кандидата технических наук / Московский энергетический ин-т (технический университет).
8. Модели зрелости: обзор и исследование. URL: pmi. ru/articles/files/18122007_Pujanova.pdf (дата обращения — 09.01.2014).
9. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Айти-Пресс, 2004. 384 с.
10. ISO/IEC 27001, ISO Guide 73:2002, ISO/IECTR18044:2018.Менеджмент информационной безопасности. (дата обращения — 15.12.2020). [Електронний ресурс]. – Режим доступу : URL: http://iso27.com/

11. SAE J1739:2000 Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery.
12. Bashir M., Christin N. Three case studies in quantitative information risk analysis. In Proceedings of the CERT/SEI Making the Business Case for Software Assurance Workshop. P. 77—86, Pittsburgh, PA, September 2008.
13. Burtescu E. Decision Assistance in Risk Assessment Monte Carlo Simulations. Informatica Economica. 2012. Vol. 16. № 4.
14. Isabel L. Nunes and Má rio Simo¨es-Marques. Applications of Fuzzy Logic in Risk Assessment — The RA_X Case // Centre of Technologies & Systems and Faculdade de Cieˆncias e Tecnologia, Universidade Nova de Lisboa, Portuguese Navy, Portugal, 2012.
15. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
16. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл
17. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
18. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.
19. Shang K. , Hossen Z.Applying Fuzzy Logic to Risk Assessment and Decision-Making // Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries. November 2013.
20. Boc K. , Vaculik J. , Vidrikova D. Fuzzy approach to risk analysis and its advantages against the qualitative approach // Proceedings of the 12th International Conference “Reliability and Statistics in Transportation and

Communication" // Transport and Telecommunication Institute, Lomonosova 1, LV-1019, Riga, Latvia.

21. Pokoradi L. Fuzzy logic-based risk assessment. [Електронний ресурс]. – Режим доступу : URL: http:// www.zmka.hu/docs/Volume1/Issue1/pdf/04poko.pdf (дата обращения — 25.12.2013).
22. The Security Risk Management Guide. Microsoft Corporation, 2006. [Електронний ресурс]. – Режим доступу : http://www.microsoft.com/technet/ security/topics/policiesandprocedures/secrisk/default (дата обращения — 09.01.2020).
21. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836
22. [Електронний ресурс]. – Режим доступу : https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11
23. Закон України Про криптографічний та технічний захист інформації [Електронний ресурс]. – Режим доступу : https://ips.ligazakon.net/document/NT1819
24. Угрозы информационной безопасности [Електронний ресурс]. – Режим доступу : https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/
25. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» [Електронний ресурс]. – Режим доступу : http://www.dut.edu.ua/uploads/l_1718_48052949.pdf
26. Актуальні проблеми управління інформаційною безпекою держави X Всеукраїнська науково-практична конференція [Електронний ресурс]. – Режим доступу : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf

27. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с. [Електронний ресурс]. – Режим доступу: https://cutt.ly/5ugjj6s
28. Інформаційна безпека України Наукові доповіді та тези учасників науково-технічної конференції 12-13 березня 2015 року [Електронний ресурс]. – Режим доступу : https://cutt.ly/IugjQBZ
29. Кавун С.В. Лабораторний практикум з навчальної дисципліни "Інформаційна безпека". Навчально-практичний посібник / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 256 с. (Укр. мов.)
30. Europol. (2018). Internet Organised Crime Threat Assessment 2018. [Електронний ресурс]. – Режим доступу : https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2018.
31. Europol. (2018). Public Awareness and Prevention Guides. [Електронний ресурс]. – Режим доступу : https://www.europol.europa.eu/activities-services/public-awareness-and-preventionguides
32. Fisher, Tim. (2018) Free and Public DNS Servers. Lifewire. [Електронний ресурс]. – Режим доступу : https://www.lifewire.com/free-and-public-dns-servers-2626062
33. Захист конфіденційну інформацію - персональних даних [Електронний ресурс]. – Режим доступу https://cutt.ly/iuggGRH
34. Закон України «Про інформацію» - [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12
35. Закон України Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР від 05.07.1994 р., [Електронний ресурс]. – Режим доступу :https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

36. Global Cybersecurity Index (GCI) 2018 [Електронний ресурс]. – Режим доступу : https://www.itu.int/en/ITU-D/ Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.
37. Рибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. – с.57-62
38. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.zakon3.rada.gov.ua/laws/ show/514/2009
39. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик. [Електронний ресурс] – Режим доступу: http://www.justinian.com.ua/article.php?id=3222
40. "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: http://www.zakon5.rada.gov.ua /laws/ show/n0004525-14. 1
41. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.
42. Доктрини «Інформаційної безпеки України» від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. – Режим доступу : https://zakon3.rada.gov.ua/laws/show/47/2017?lang=ru

Навчальне видання

**Гребенюк** Андрій Миколайович
**Рибальченко** Людмила Володимирівна

# ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Навчальний посібник

Редактор *О.М. Врублевська*
Комп’ютерна верстка *А.В. Самотуга*

Формат 60х84 1/16. Ум. друк. арк. . Обл.-вид. арк. .
Тираж пр. Зам. № .