# Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами. Основні причини загострення проблеми безпеки інформаційних технологій. Інформація та інформаційні відносини.


1.Яке суспільство називають інформаційним?

2.Яка система називається інформаційною?

3.Для чого ми захищаємо інформацію?

4.Де ми захищаємо інформацію?

5.Як ми захищаємо інформацію?

# Пригадайте

# Хто володіє інформацією- той володіє світом

**Натан Майер Ротшильд**

# Історія виникнення інформаційної безпеки

I етап — до 1816 року — характеризується використанням природно утворюваних засобів інформаційних комунікацій.

II етап — починаючи з 1816 року — пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку.

III етап — починаючи з 1935 року — пов'язаний з появою засобів радіолокації і гідроакустики.

IV етап — починаючи з 1946 року — пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів).

V етап — починаючи з 1965 року — обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж.

VI етап — починаючи з 1973 року — пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань.

**Захист інформації** – це комплекс заходів, направлених на забезпечення інформаційної безпеки

## 30 листопада

Міжнародний день захисту інформаціїї

# Види інформації, які підлягають захисту

**Конфіденційна інформація** - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням.



**Таємна інформація** - інформація, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

**Інформація з обмеженим доступом** - інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону.

**Доступ до інформації** - можливість одержання, оброблення інформації, її блокування та порушення цілісності.

**Санкціонований доступ до інформації** – це доступ до інформації, що не порушує встановлені правила розмежування доступу


**Несанкціонований доступ до інформації** - доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.

# Автоматизація бізнесу.
# Для чого автоматизують підприємства?

Чого прагне кожен керівник?

Звичайно ж, процвітання своєї справи.

Тому, підприємці зупиняють свій вибір на автоматизації бізнесу.


Програма виконує багато процесів замість співробітників, що знижує кількість помилок, а як наслідок мінімізує збитки.

# Основними перевагами автоматизації є:

1. Збільшення пропускної здатності або продуктивності.
2. Підвищення якості та передбачуваності якості.
3. Підвищена надійність, процесів або продуктів.
4. Підвищення узгодженості продукції.
5. Скорочення прямих людських витрат на робочу силу та видатків.

# Основними недоліками автоматизації є:

1. Загрози безпеці / уразливості (кібератака).
2. Непередбачувані / надмірні витрати на розробку.
3. Висока ціна.

# Причини загострення проблеми безпеки інформаційних технологій.

- Відомо, що російські хакери з 1994 по 1996 рік вчинили майже 500 спроб проникнення в комп’ютерну мережу Центрального банку Росії. В 1995 році ними було викрадено 250 мільярдів рублів (ITAP-TAPC, AP, 17 вересня 1996 року). Кожен комп’ютерний злочин завдає шкоди приблизно в 200 тисяч доларів.


- Невідомі “жартівники” скористалися принципами роботи онлайнової енциклопедії Wikipedia для розповсюдження шкідливого програмного забезпечення – нової модифікації вірусу Blaster.

# Причини загострення проблеми безпеки інформаційних технологій.

- Британський спеціаліст з інформаційних технологій Максвелл Парсонс отримав 2,5 року ув’язнення за злам банкоматів за допомогою MP3-плеєра і спеціального програмного забезпечення. Таким чином він отримував конфіденційну інформацію про банківські рахунки клієнтів для клонування кредитних карток.


- Одна студентка втратила стипендію в 18 тисяч доларів у Мічиганському університеті через те, що її сусідка по кімнаті скористалася їх спільним системним паролем і відправила від імені своєї жертви електронний лист із відмовою від стипендії.

# Чому виникла проблема захисту інформації? Які чинники вплинули на це?

# Проблема захисту інформації у автоматизованих системах (АС) визначається наступними чинниками:

- високими темпами зростання засобів обчислювальної техніки і зв’язку, розширенням областей використання електронно-обчислювальних машин (ЕОМ);
- **залученням в процес інформаційної взаємодії все більшого числа людей і організацій;**
- концентрацією великих обсягів інформації різного призначення і приналежності на електронних носіях;
- **наявністю інтенсивного обміну інформацією між учасниками цього процесу**;
- зростанням числа кваліфікованих користувачів обчислювальної техніки і можливостей по створенню ними програмно-технічних впливів на систему;
- **розвитком ринкових відносин (в області розробки, постачання, обслуговування обчислювальної техніки, розробки програмних засобів, в тому числі засобів захисту);**
- ставленням до інформації, як до товару, переходом до ринкових відносин, з властивою ним конкуренцією і промисловим шпигунством, в області створення і збуту (надання) інформаційних послуг

# Інформаційні відносини

Найважливішими компонентами інформаційної діяльності є:

- Інформація та інформаційні системи;
- суб’єкти – учасники інформаційних процесів;
- правові відносини виробників – споживачів інформаційної продукції;

**Інформаційні відносини** – це можливість доступу суб’єктів інформаційної безпеки до об’єктів, що визначаються певними правилами

# Об'єкт інформаційних відносин

**Об’єкт** – пасивний компонент системи, який зберігає, приймає або передає інформацію. Доступ до об'єкту означає доступ до інформації, яка міститься в ньому.

У якості **об'єктів інформаційної безпеки** [information security object] необхідно розглядати:

- інформацію та інформаційні ресурси,
- носії інформації,
- процеси обробки інформації.

До **соціальних об'єктів інформаційної безпеки** звичайно відносять:

- Особистість, колектив, суспільство, державу, світове товариство.

# Суб'єкт інформаційних відносин

**Суб’єкт** – це активний компонент інформаційної системи, який може стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи.


До суб'єктів інформаційної безпеки [information security subject] відносяться:

- держава, що здійснює свої функції через відповідні органи;
- громадяни, суспільні або інші організації і об'єднання.

Під *інформаційним середовищем* розуміють сферу діяльності суб’єктів, пов’язану із створенням, обробленням й споживанням інформації.

# Безпека інформаційних технологій

Слово "безпека" латинського походження - secure (securus). Потім в англійській мові воно отримало написання "security".

“Безпека" - це відсутність небезпеки; стан діяльності, при якій з певною ймовірністю виключено заподіяння шкоди здоров'ю людини, будівель, приміщень та матеріально-технічних засобів у них.

**Інформаційна безпека (Information Security)** — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

# Інформаційна безпека (Information security)

Під ***безпекою інформації*** розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, здатних завдати шкоди безпосередньо даним, їхнім власникам і користувачам інформації та інфраструктурі, що підтримує інформаційну безпеку.

# Види інформаційної безпеки

- Інформаційна безпека держави
- Інформаційна безпека суспільства
- Інформаційна безпека організації
- Інформаційна безпека особистості

# Принципи інформаційної безпеки


- Конфіденційність
  - лише уповноважені користувачі можуть ознайомитись з інформацією
- Цілісність
  - лише уповноважені користувачі можуть модифікувати інформацію
- Доступність
  - уповноважені користувачі можуть отримати доступ до інформації, не очікуючи довше за заданий (малий) час

# Інформаційна безпека

***Інформаційна безпека*** **- це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації.**

***Інформаційна безпека*** **— це комплекс заходів, для захисту даних та інформаційної системи від випадкових або навмисних пошкоджень та несанкціонованого доступу.**