Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз безпеки та каналів проникнення і несанкціонованого доступу до відомостей та програмного коду

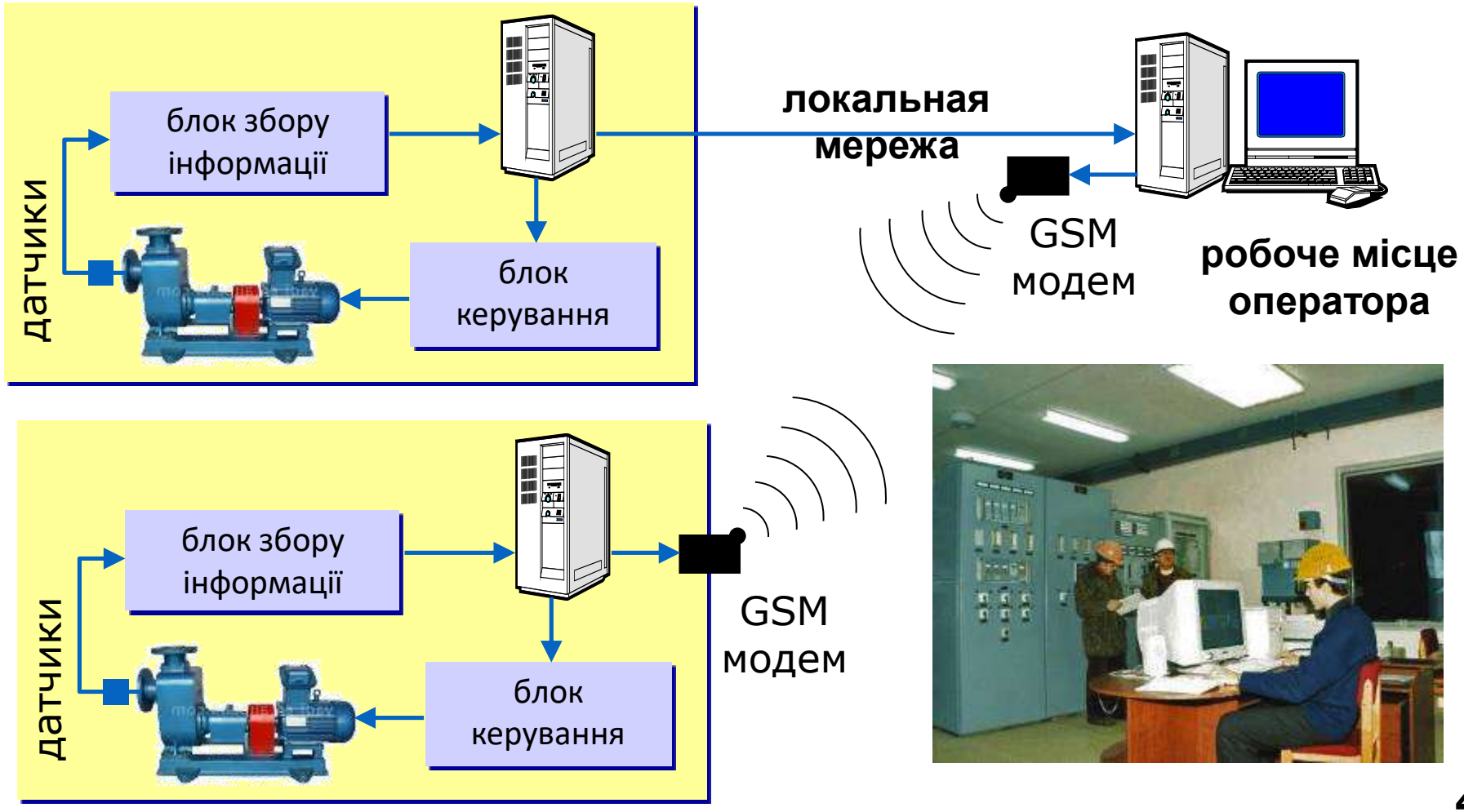
Загрози безпеці інформації в автоматизованих системах

Автоматизована система (АС) – це організаційно-технічна система, що реалізує інформаційну технологію і поєднує:

- *обчислювальну систему (ОС);*
- *фізичне середовище;*
- *персонал;*
- *інформацію, що обробляється*

Автоматизована система

Автоматизовані системи управління технологічними процесами



Практика

За прикладами розглянутих автоматизованих інформаційних систем, побудуйте інформаційну систему, яку використовуєте ви вдома.

Різновиди загроз

Залежно **від обсягів завданих збитків**, загрози інформаційній безпеці поділяють на:

- ***нешкідливі*** — не завдають збитків;
- ***шкідливі*** — завдають значних збитків;
- ***дуже шкідливі*** — завдають критичних збитків інформаційній системі, що призводить до повного або тривалого в часі припинення роботи ІС.

Залежно **від результату шкідливих дій**, загрози інформаційній безпеці можна поділити на такі види:

- ***отримання доступу*** до секретних або конфіденційних даних;
- ***порушення або повне припинення*** роботи комп'ютерної інформаційної системи;
- ***отримання доступу до керування*** роботою комп'ютерної інформаційної системи.

Різновиди загроз

Розглядають й інші класифікації загроз:

- ***за метою*** (зловмисні, випадкові),
- ***за місцем виникнення*** (зовнішні, внутрішні),
- ***за походженням*** (природні, техногенні, зумовлені людиною)

Шкідливі програми, їх види та принципи дії

Для **шкідливих комп'ютерних програм характерно**:

- ***швидке розмноження*** шляхом приєднання своїх копій до інших програм, копіювання на інші носії даних, пересилання копій комп'ютерними мережами;
- ***автоматичне виконання деструктивних дій***:

Деструктивні дії комп'ютерних вірусів

- **Поява на екрані** комп'ютера **непередбачених повідомлень** або зображень
- **Динамік** комп'ютера **відтворює** непередбачені **звукові сигнали**
- **Несанкціоноване відкриття** та закриття лотка для читання дисків
- **Мимовільний запуск** будь-яких програм
- **Програми**, які раніше працювали правильно, **починають** працювати **повільно** та збоїти
- **Запит паролів** програмами, до яких він не потрібний, і до яких він не встановлювався
- **Несанкціоновані зміни файлів та папок**, зникнення файлів та папок
- **ОС завантажується повільно** або взагалі не завантажується
- Виконується більш часто, ніж зазвичай, звернення до жорсткого диска
- У роботі комп'ютера відбуваються **часті зависання та збої**.
- З комп'ютера **здійснюється несанкціоноване надсилання поштових повідомлень**
- Встановлена на **комп'ютері антивірусна програма** повідомляє про **наявність підозрілих файлів** у системі
- Встановлений на комп'ютері **мережевий екран повідомляє** про спроби несанкціонованого доступу якоїсь програми до мережі
- **Відхилення комп'ютера** виникають у певний день, у певний час

Шкідливі програми, їх види та принципи дії

За рівнем небезпечності дій шкідливі програми розподіляють на:
безпечні — проявляються відео- та звуковими ефектами, не змінюють файлову систему, не ушкоджують файли й не виконують шпигунських дій;
небезпечні — призводять до перебоїв у роботі комп'ютерної системи:
зменшують розмір доступної оперативної **пам'яті**,
перезавантажують комп'ютер тощо;
дуже небезпечні — знищують дані з постійної та зовнішньої пам'яті, виконують шпигунські дії тощо.

Шкідливі програми, їх види та принципи дії

За **принципами розповсюдження та функціонування** шкідливі програми розподіляють на:

• **комп'ютерні віруси** — програми, здатні саморозмножуватися та виконувати несанкціоновані деструктивні дії на ураженому комп'ютері.

Серед них виділяють:

- **дискові** (завантажувальні) віруси — розмножуються копіюванням себе у службові ділянки дисків та інших змінних носіїв, яке відбувається під час спроби користувача зчитати дані з ураженого носія;
- **файлові віруси** — розміщують свої копії у складі файлів різного типу. Як правило, це файли готових до виконання програм з розширенням імені **exe** або **com**. Однак існують так звані макровіруси, що уражують, наприклад, файли текстових документів, електронних таблиць, баз даних тощо;

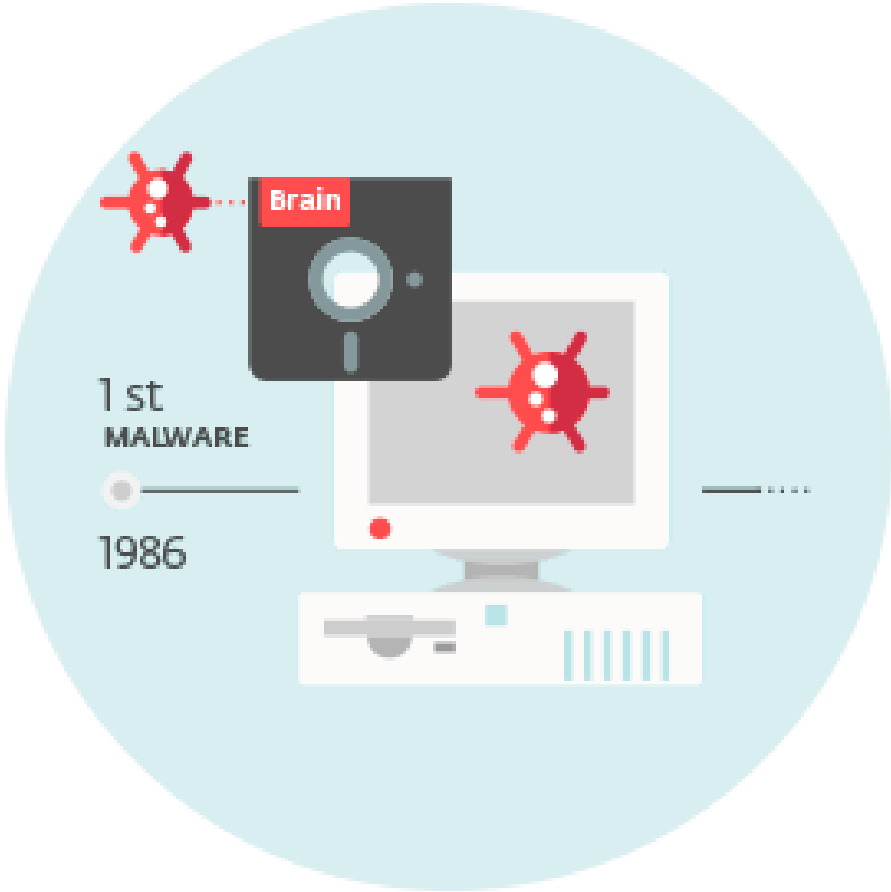
• **хробаки (черв'яки) комп'ютерних мереж** — пересилають свої копії комп'ютерними мережами з метою проникнення на віддалені комп'ютери. Більшість черв'яків поширюються, прикріпившись до файлів електронної пошти, електронних документів тощо.

Шкідливі програми, їх види та принципи дії

- **троянські програми** — програми, що проникають на комп'ютери користувачів разом з іншими програмами, які користувач «отримує» комп'ютерними мережами або на змінному носії;
- **рекламні модулі, або Adware** (англ. Ad — скорочення від advertisement — оголошення, реклама, ware — товар), — програми, що вбудовуються у браузер користувача для показу реклами під час перегляду веб-сторінок.
- інші — **руткіти** (англ. root — кореневий каталог у Linux, kit — набір інструментів), **експлойти** (англ. exploit — експлуатувати, використовувати для власної вигоди), **бекдори** (англ. back door — чорний хід), **завантажувачі** (англ. downloader — завантажувач) тощо.

Коротка історія

Першим зафіксованим **комп'ютерним вірусом** був **Pakistani Brain** на початку 1986 року. Ця шкідлива програма на комп'ютері інфікувала завантажувальний сектор дискети, **розповсюдившись глобально за декілька тижнів**.



У яких випадках програму називають комп'ютерним вірусом?

Комп'ютерні віруси

Brain, Jerusalem, ILOVEYOU, MyDoom, WannaCry, Zeus, Flashback, MyDoom, Sobig, BlackEnergy, DarkTequila, SQL Slammer, Chernobyl, SirCam, Melissa, Code Red, Conficker, SoBig, Petya.A.

https://threatmap.checkpoint.com/

Практика

Зі списку запропонованих вірусів оберіть один та надайте його характеристику:
Brain, Jerusalem, ILOVEYOU, MyDoom, WannaCry, Zeus, Flashback, MyDoom, Sobig, BlackEnergy, DarkTequila, SQL Slammer, Chernobyl, SirCam, Melissa, Code Red, Conficker, SoBig, Petya.A.

Назва вірусу	Дата поширення	Розробник	До якої групи вірусів належить	Принцип дії	Наслідки

Основні джерела і шляхи реалізації загроз безпеки та каналів проникнення і несанкціонованого доступу до відомостей та програмного коду

- комп'ютерні віруси та шкідливе програмне забезпечення (Malware);
- інтернет-шахрайство;
- несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем;
- **Соціальна інженерія**
- DDoS-атаки (Distributed Denial of Service);
- «крадіжка особистості» (Identity Theft)
- **Екран-вуайерізм**
- **Інтернезія**
- спам-розсилки;
- **Нігерійські листи**
- **Номофобія**
- **Овершерер**
- Крадіжка коштів;
- бот-мережі (botnet);
- **Соціальне похмілля**
- **Теорія лайків**
- **Цифровий детокс**
- Хеппіслепінг

Практика

У Енциклопедія Інтернет-загроз від компанії https://www.eset.com/ua розгляньте Інтернет-загрози, які спрямовані на домашніх користувачів. Розглянь одну із загроз, що не розглядалися під час заняття, опиши її.