Лекція 5
БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

План

1. Інформація як об'єкт захисту
2. Комп'ютерні злочини
3. Сервіси безпеки
4. Стандарти захисту інформації
5. Комп'ютерні віруси

5.1. Інформація як об'єкт захисту

Цінність інформації — основний критерій у прийнятті рішень щодо її захисту.

- ***Життєво важлива інформація*** - це інформація, наявність якої необхідна для функціонування організації.
- ***Важлива інформація*** - це інформація, що може бути замінена або поновлена, але процес її поновлення дуже важкий та пов'язаний з великими витратами.
- ***Корисна інформація*** - це інформація, яку важко поновити, але без якої Підприємство може продовжувати ефективне функціонування.
- ***Неістотна інформація*** - це інформація, що не потрібна для функціонування підприємства.

Інформаційна безпека (ІБ) – захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, здатних завдати збитків власникам або користувачам інформації.

Основні аспекти інформаційної безпеки

- ***Доступність*** – це можливість за прийнятий час одержати необхідну інформацію.
- ***Цілісність*** – це актуальність і несуперечність інформації, її захищеність від руйнації і несанкціонованої зміни.
- ***Конфіденційність*** - це захист інформації від несанкціонованого читання.

Доступність

Цілісність

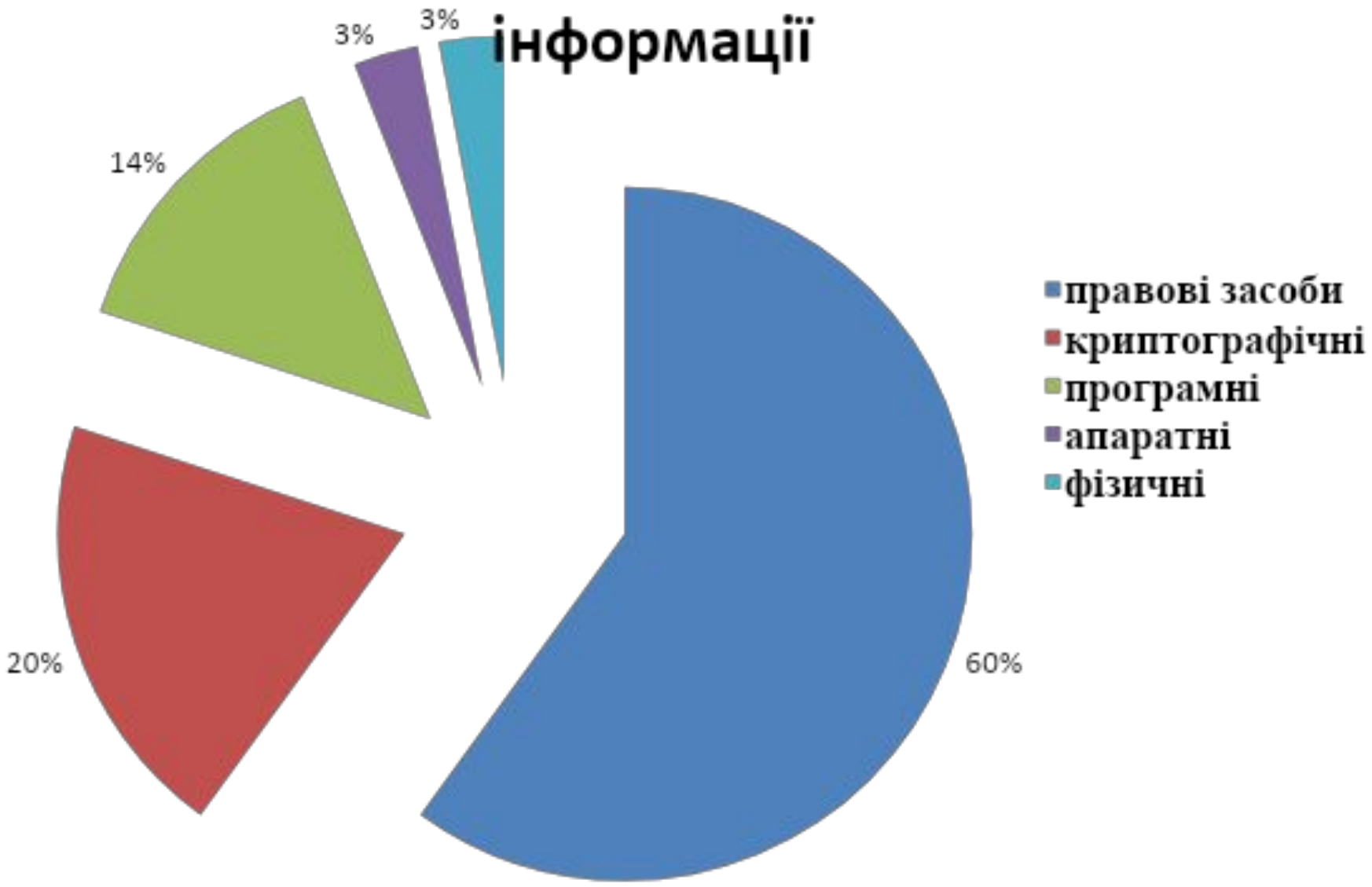
Конфіденційність

Засоби захисту інформації

Основні засоби захисту інформації:

- *фізичні* (створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних зловмисників до компонентів ІС та інформації);
- *апаратні* (пристрої, які вмонтовуються в блоки електронних систем обробки і передачі даних для внутрішнього захисту апаратно-технічного забезпечення ІС);
- *програмні* (вмонтовані до складу ПЗ для виконання функцій захисту його функціонування);
- *апаратно-програмні*;
- *криптографічні* (методи шифрування даних з метою їх захисту під час передавання);
- *організаційні* (підбір, перевірка та навчання персоналу ІС).

Питома вага форм захисту комп'ютерної інформації



Політика безпеки

Політика безпеки - це комплекс законів, правил та норм поведінки, що визначають, яким чином підприємство обробляє, захищає та поширює інформацію.

Політика безпеки повинна розроблятися індивідуально для кожної конкретної ІС. Як правило вона реалізується *у чотири етапи.*

- ***Етап 1. Реєстрація ресурсів, які підлягають захисту***. Захищати потрібно не тільки дані, апаратне і ПЗ, а й персонал, документацію та витратні матеріали.
- ***Етап 2. Визначення потенційних загроз для кожного ресурсу***. До класичних загроз відносяться: несанкціонований доступ до інформаційних ресурсів, ненавмисне розкриття інформації, відмова в обслуговуванні певними сервісами, мережеві атаки, комп'ютерні віруси, логічні бомби, “троянські коні”, засоби пригальмовування обміну даними в мережах, апаратні збої, крадіжки, природні катаклізми.
- ***Етап 3. Оцінка ймовірності появи кожної загрози та можливі втрати від неї.*** Результатом проведення цього аналізу є класифікація загроз на малонебезпечні, небезпечні та критичні.
- ***Етап 4. Прийняття рішень щодо захисту ІС***. Слід враховувати, що вартість засобів захисту від загрози не повинна перевищувати збитків від неї.

Інформація має цінність, тому для ефективного її збереження необхідно знати, в чому саме ця цінність полягає та яка небезпека їй загрожує.

- якщо цінність інформації втрачається при її розкритті, то вважають, що існує ***небезпека порушення таємності інформації***;
- якщо цінність інформації втрачається при зміні або знищенні інформації, то вважають, що існує ***небезпека для цілісності інформації;***
- якщо цінність інформації в її оперативному використанні, то вважають, що існує ***небезпека порушення доступності інформації;***
- якщо цінність інформації втрачається при збоях у системі, то вважають, що існує ***небезпека втрати стійкості до помилок.***

Класи загроз інформації

- порушення конфіденційності;
- порушення цілісності (логічної і фізичної);
- порушення доступності або відмова в обслуговуванні;
- порушення здатності до спостереження або керованості;
- несанкціоноване використання інформаційних ресурсів.

Дестабілізуючий фактор (ДФ) - це подія, наслідком якої може бути загроза інформації.

ДФ може виникати на будь якому етапі життєвого циклу ІС. Усі відомі ДФ можна поділити на такі типи:

- ***кількісна недостатність*** - фізична нестача компонентів ІС;
- ***якісна недостатність*** - недосконаліть конструкції або організації компонентів ІС;
- ***відмова елементів*** - порушення працездатності елементів;
- ***збій елементів*** — тимчасове порушення працездатності елементів;
- ***помилки елементів*** – неправильне виконання елементами своїх функцій;
- ***стихійні лиха***;
- ***зловмисні дії***;
- ***побічні явища.***

5.2. Комп'ютерні злочини

Комп'ютерний злочин - це злочин, де комп'ютер безпосередньо є об'єктом або знаряддям здійснення правопорушень у суспільних сферах, пов'язаних із використанням обчислювальної техніки.

Комп'ютерні злочини умовно можна поділити на дві категорії:

- злочини, що пов'язані з втручанням у роботу комп'ютерів;
- злочини, що використовують комп'ютери як необхідні технічні пристрої.

Злочини, що пов'язані з втручанням у роботу комп'ютерів

- несанкціонований доступ у комп'ютерні мережі і системи, банки даних з метою шпигунства та диверсій з метою комп'ютерного розкрадання або з хуліганських мотивів;
- введення в ПЗ "логічних бомб", що спрацьовують за певних умов;
- розроблення і поширення комп'ютерних вірусів;
- злочинна недбалість під час розроблення, виготовлення та експлуатації ПЗ, що призводить до тяжких наслідків;
- підробка інформації (інформаційних продуктів) і здача замовникам непрацездатних програм;
- розкрадання інформації (порушення авторського права і права володіння програмними засобами і базами даних).

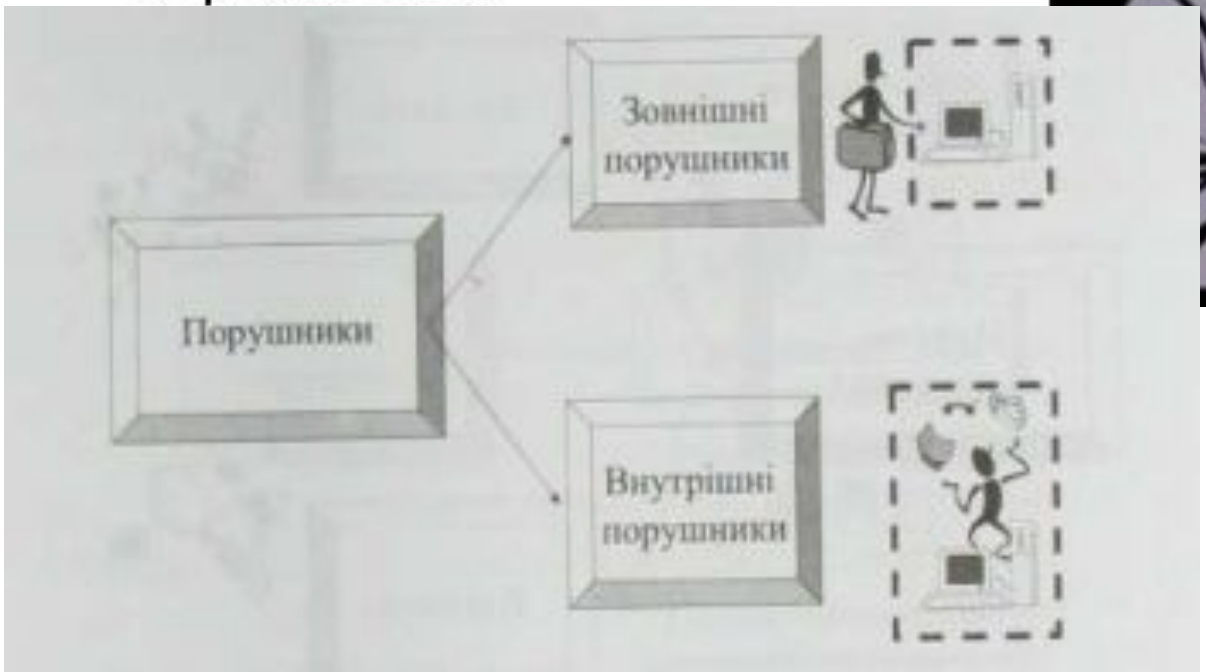
Серед комп'ютерних злочинів, що використовують комп'ютери як необхідні технічні пристрої, можна виділити злочини, що сплановані за допомогою комп'ютерних моделей, приміром, у сфері бухгалтерського обліку.

***Порушник** - особа, яка здійснила спробу виконання забороненої операції (дії) за помилкою, незнанням або свідомо зі злими намірами.*

***Зловмисник** – це порушник, який навмисно йде на порушення.*

Зловмисником може бути:

- розробник комп'ютерних систем;
- співробітник з числа обслуговуючого персоналу;
- користувач;
- стороння особа.



Внутрішнім порушником може бути особа з таких категорій персоналу:

- ***користувачі (оператори) системи***;
- ***персонал***, що обслуговує технічні засоби (інженери, техніки);
- ***працівники відділів розроблення та супроводження ПЗ*** (прикладні та системні програмісти);
- ***технічний персонал***, що обслуговує приміщення (прибиральники, електрики тощо, які мають доступ до приміщень);
- ***працівники служби безпеки;***
- ***керівники різних рівнів посадової ієрархи.***

Зовнішніми порушниками можуть бути :

- ***клієнти*** (представники організацій, громадяни);
- ***відвідувачі*** (запрошені з якого-небудь приводу);
- ***представники інших організацій***, що взаємодіють з питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання тощо);
- ***представники конкуруючих організацій або особи, що діють за їх завданням;***
- ***особи, що випадково або навмисно порушили пропускний режим*** (без мети порушити безпеку);
- ***будь-які особи*** за межами контрольованої зони.

Методи вторгнення

При активному вторгненні порушник прагне замінити інформацію, яка передається в повідомленні. Він може вибірково модифікувати, заміняти або додавати вірне чи невірне повідомлення, змінювати порядок повідомлень. Порушник може також анулювати або затримувати всі повідомлення.

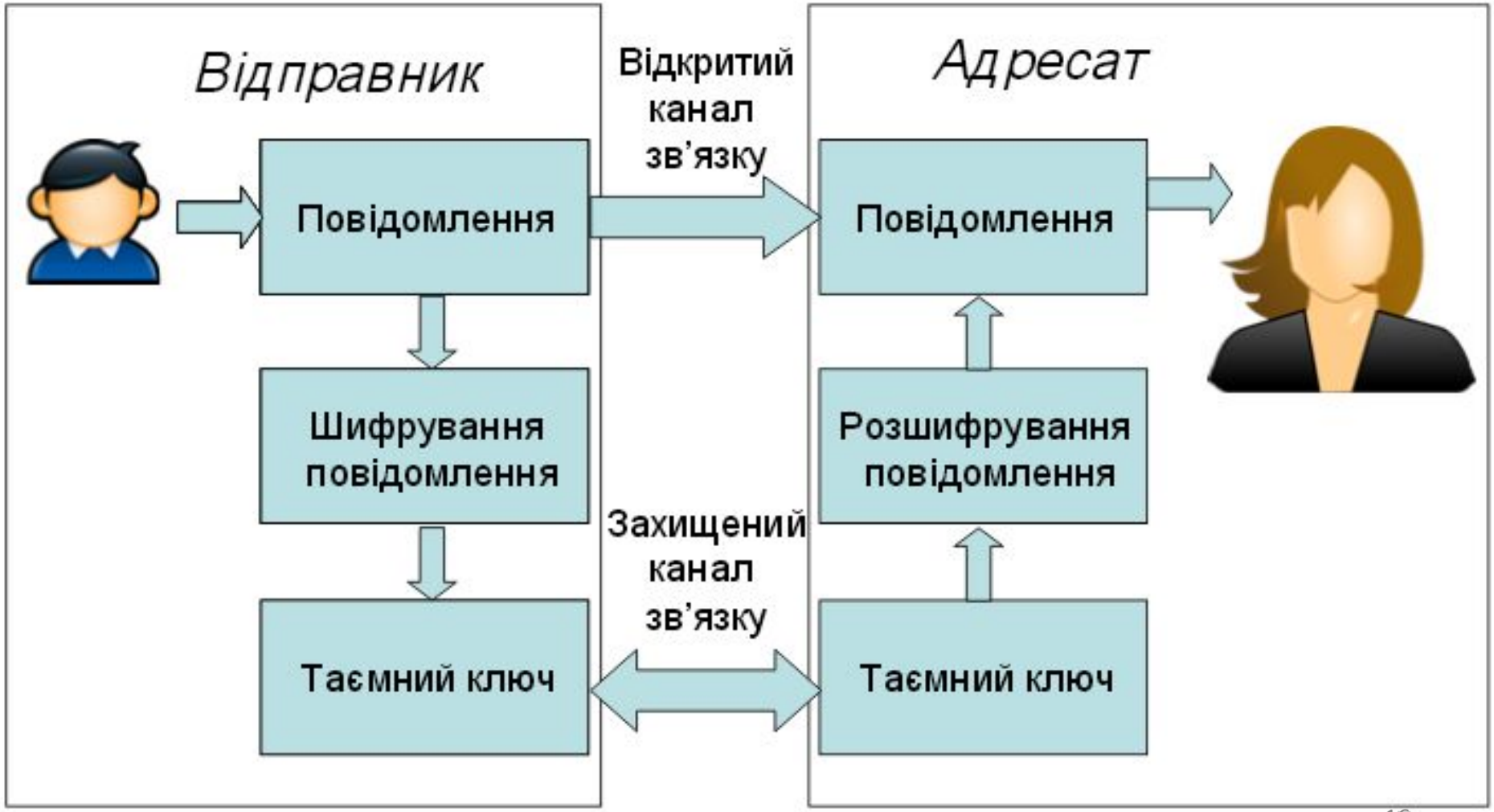
При пасивному вторгненні порушник тільки спостерігає за проходженням інформації лініями зв'язку, не вторгаючись ані в інформаційні потоки, ані в зміст інформації, що передається. Зазвичай він аналізує потік повідомлень, фіксує пункти призначення або факт проходження повідомлення, його розмір та частоту обміну, якщо зміст не підлягає розпізнанню.

5.3. Сервіси безпеки

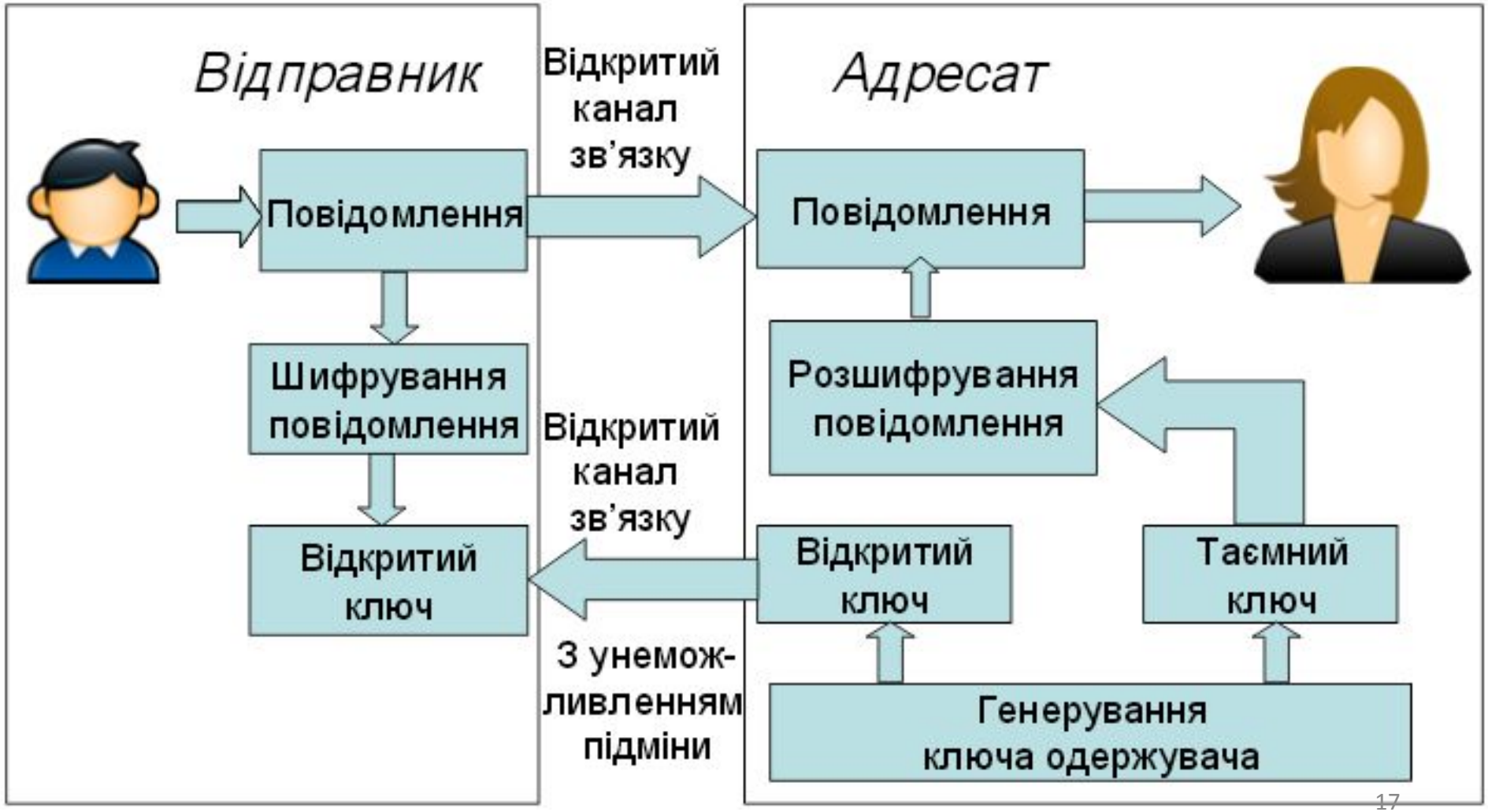
Сервіс безпеки - це сукупність заходів для зменшення ризиків порушення безпеки даних.

- ***Сервіс аутентифікації.*** Аутентифікація – процедура перевірки, чи є користувач ІС тим, за кого себе видає, яка відбувається в два етапи – введення імені користувача (**ідентифікація**) та паролю (**верифікація**). Для аутентифікації можуть використовуватися біометричні методи розпізнавання відбитків пальців, сітківки ока та ін.
- ***Сервіс конфіденційності***. Здебільшого полягає у шифруванні даних, яке, як і зворотна процедура (дешифрування) здійснюється з використанням **криптографічного** ключа. Якщо відправник і одержувач користуються одним і тим самим ключем, то шифрування називається симетричним, якщо різними ключами - асиметричним
- ***Сервіс цілісності***. Відповідає за захист електронних даних від зміни чи вилучення.
- ***Сервіс дотримання зобов'язань***. Гарантує, що учасники інформаційного процесу не зможуть заперечити факт своєї участі в ньому. Реалізується за допомогою **цифрових підписів**. Цифровий підпис дає змогу встановити особу, яка підписала документ та перевірити інформацію на цілісність.

Симетричне шифрування (на таємному ключі)



Асиметричне шифрування (на відкритому ключі)



Порівняння симетричного та асиметричного шифрування

Симетричне шифрування	
Переваги	**Недоліки**
▪ швидкість (на 3 порядки) ▪ простота реалізації ▪ менша довжина ключа для визначення стійкості	▪ складність управління ключами ▪ складність обміну ключами

Асиметричне шифрування	
Переваги	**Недоліки**
▪ відсутність необхідності захищеного каналу ▪ наявність тільки одного секретного ключа ▪ число ключів в мережі менше і не росте в квадратичній залежності	▪ складність проведення зміни алгоритму ▪ неможливість шифрування ID відправника та адресата ▪ велика довжина ключа, порівняно із симетричним шифруванням

5.2. Стандарти захисту інформації

Комп'ютерна система безпечна, якщо вона забезпечує контроль за доступом до інформації так, що тільки уповноважені особи або процеси, що функціонують від їхнього імені, мають право читати, писати, створювати або знищувати інформацію.

Класи захисту обчислювальних систем

- ***Клас D:*** Мінімальний захист.
- ***Клас C1:*** *Захист, заснований на розмежуванні доступу* (ОАС).
- ***Клас C2***: *Захист, заснований на керованому контролі доступом.*
- ***Клас B1:*** *Мандатний захист*
- ***Клас B2:*** *Структурований захист.*
- ***Клас B3:*** *Домени безпеки.*
- ***Клас A1:*** *Верифіковоний проект.*

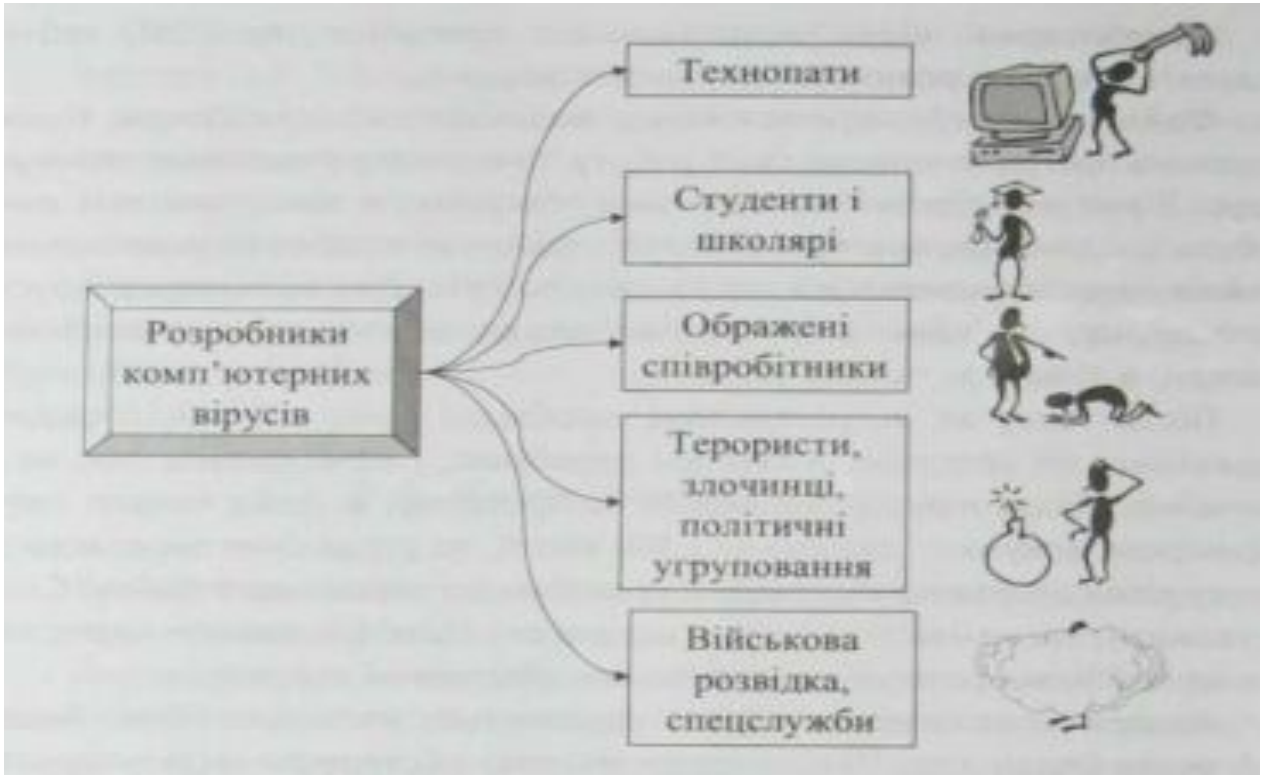
6.4. Комп'ютерні віруси

Офіційно вважається, що термін «комп'ютерний вірус» вперше вжив **Ф.Коен у 1984 р.** (Лехайський університет, США*):* ***комп'ютерний вірус - програма, що може заражати інші програми, модифікуючи їх додаванням своєї, можливо, зміненої, копії.***

- Ключовим поняттям у визначенні вірусу є його **спроможність до розмноження**, оскільки це - єдиний критерій, що дозволяє відрізнити віруси від інших програм.
- ***Комп'ютермий вірус*** - це невелика програма, яка може самостійно розмножуватись, переноситись на інші носії інформації чи передаватися мережею та порушувати нормальну роботу ПЗ.
- ***Комп'ютерний вірус*** - це звичайна програма для ЕОМ, тобто результат творчої розумової діяльності людини.

Найпоширеніші ознаки присутності вірусів:

- зміна розмірів файлів;
- помітне зменшення швидкодії комп'ютера;
- поява пошкоджених секторів на диску;
- поява на екрані непередбачених повідомлень;
- зависання деяких програм;
- зменшення вільного місця на диску.



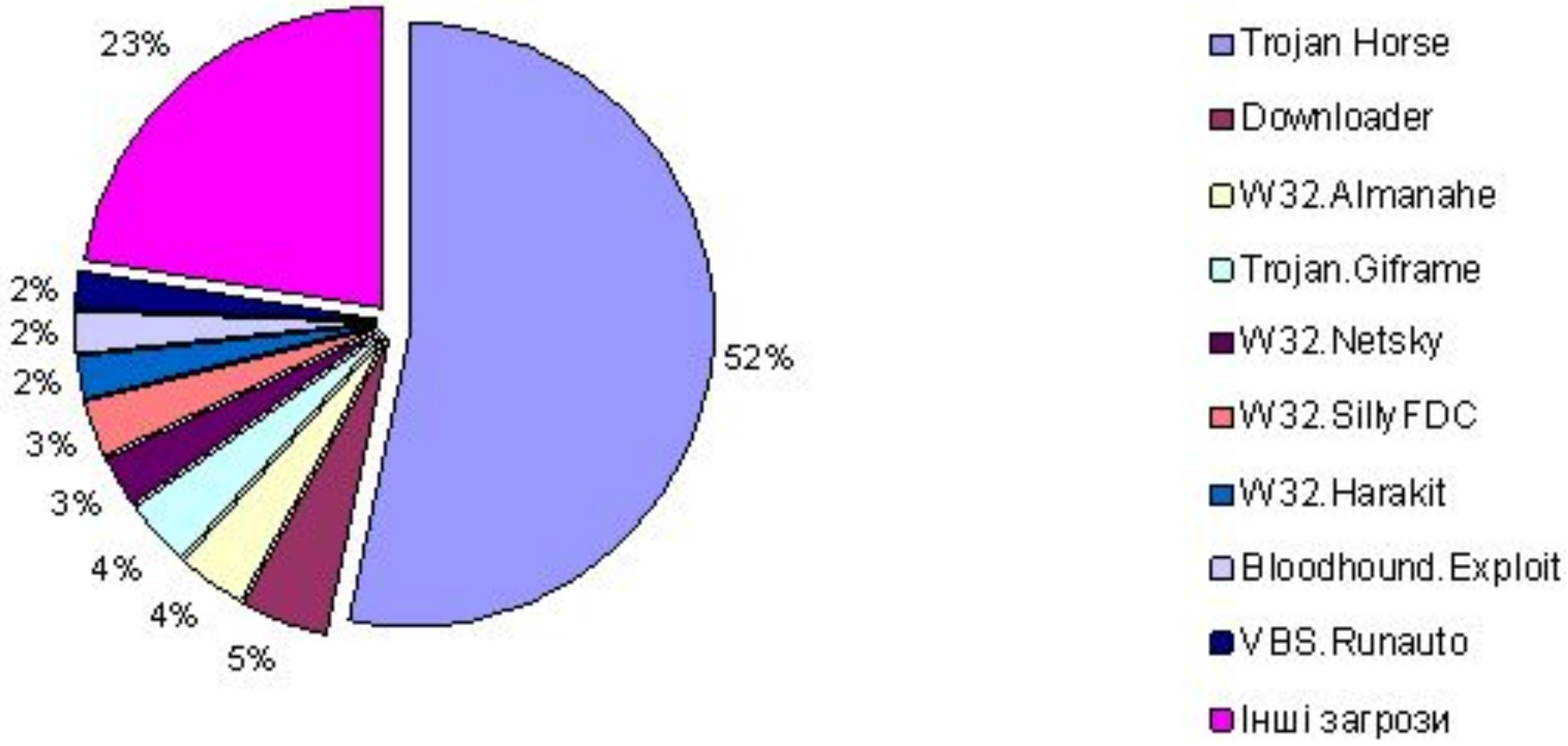
Класифікація комп'ютерних вірусів

- ***Нешкідливі віруси*** ніяким чином не впливають на роботу комп'ютера, крім зменшення вільного місця в результаті свого поширення.
- ***Безпечні віруси*** обмежують свій вплив на роботу комп'ютера зменшенням вільного місця на диску та графічними і звуковими ефектами.
- ***Небезпечні віруси*** можуть призводити до серйозних збійних ситуацій у роботі комп'ютера (приміром, до зависання потрібних користувачеві програм).
- ***Дуже небезпечні*** віруси можуть призвести до втрати інформації (як програм, так і даних), перезаписувати системні розділи пам'яті і навіть спричиняти прискорений знос апаратної частини.

Найпоширеніші види загроз безпеці ІС:

- несанкціонований доступ;
- незаконне використання привілеїв;
- атаки «салямі»;
- використання прихованих каналів;
- «маскарад»;
- «збір сміття»;
- шкідливі програми;
- зламування системи;
- «люки»;
- «троянський кінь»;
- віруси;
- «черв'як»;
- «жадібні» програми;
- захоплювачі паролів.

Діаграма вірусної активності за типами вірусів



Антивірусний захист

Загальні рекомендації щодо інформаційної безпеки

1. Необхідний комплексний підхід до інформаційної безпеки.

Інформаційну безпеку слід розглядати як складову частину загальної безпеки, причому як важливу і невід'ємну її частину.

2. Необхідна участь співробітників керівництва безпеки на етапі вибору-придбання-розроблення автоматизованої системи.

Цю участь не слід зводити до перевірки надійності постачальника та його продукції. Керівництво безпеки має контролювати наявність належних засобів розмежування доступу до інформації, що одержує система.

ДЯКУЮ ЗА УВАГУ