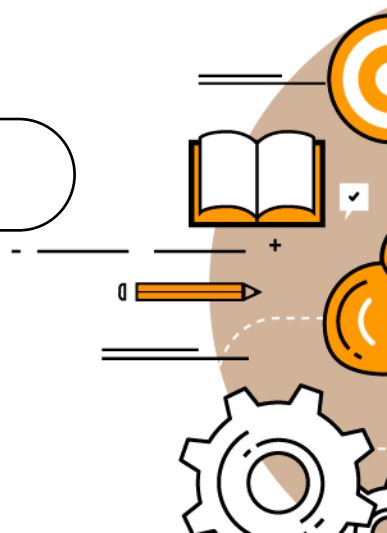
Основи інформаційної та кібербезпеки

Лекція 1.
Основні поняття інформаційної безпеки та кібербезпеки

1. **Поняття інформації та інформаційного простору**
2. **Інформаційні системи**
3. **Інформаційна безпека**
4. **Загрози безпеці інформації**
5. **Модель захисту та модель порушника в ІС**



1 Поняття інформації

Слово «**інформація**» походить від лат. *informatio*, яке має декілька значень:

- роз'яснення; виклад фактів, подій; витлумачення;
- представлення, поняття;
- ознайомлення, просвіта.

Саме слово «informatio» складається з префікса «in-» («в-, на-, при-») і дієслова «form» («надаю форму, створюю»), пов'язаного з іменником «forma» («форма»)

https://uk.wikipedia.org/wiki/Інформація

1 Поняття інформації

1. У побуті інформацією називають будь-які дані або відомості, які кого-небудь цікавлять. "Інформувати" = "повідомити щось, невідоме раніше".

2. У техніці під інформацією розуміють повідомлення, передані у формі знаків або сигналів.

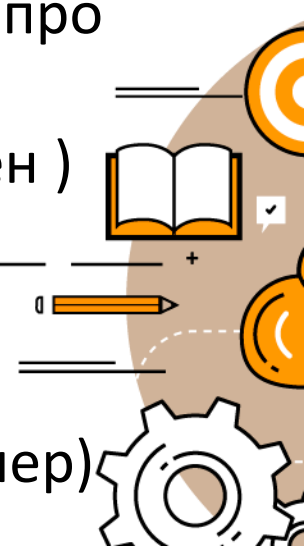
3. У кібернетиці під інформацією розуміють ту частину знань, що використовується для орієнтування, активної дії, керування, тобто з метою збереження, удосконалювання, розвитку системи (Н. Вінер).

1 Поняття інформації

- Сучасне тлумачення «**інформації**», було введено в постійне вживання в середині XX ст. Клодом Шенноном («батьком» теорії інформації).

Інформація - знята невизначеність наших знань про щось

- ***Інформація*** - відомості про об’єкти і явища навколишнього середовища, їх параметри, властивості і стан, які зменшують ступінь невизначеності і неповноти знань про них
- ***Інформація*** - це заперечення ентропії (Леон Бриллюен)
- ***Інформація*** - це міра складності структур (А. Моль).
- ***Інформація*** - це позначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього й пристосування до нього наших почуттів (Н. Вінер)



1 Поняття інформації

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

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

Закон України «Про інформацію»

1 Кількість інформації

- Ентропійний підхід (формула Шеннона)

$$I = -\sum_{i=1}^{N} p_i \log_2 p_i ,$$

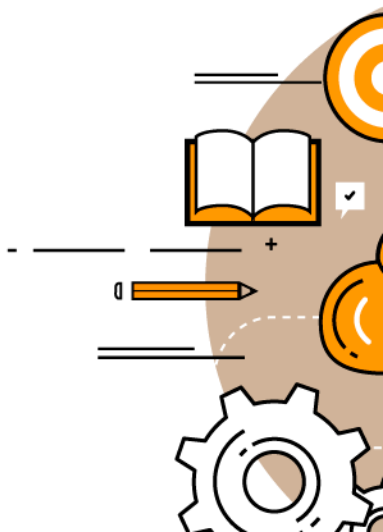
де I - кількість інформації;
N - кількість можливих подій;
p_i - імовірність *i*-ї події.

- Тезаурусний підхід (або семантична теорія інформації)

(кількість інформації, що отримується людиною з повідомлення, можна оцінити ступенем зміни його знань.)

- Прагматична міра інформації

(корисність інформації (цінність) для досягнення користувачем поставленої мети)



1 Поняття інформаційного простору

- ***Інформаційний простір*** – глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення з метою підтримання ухвалюваних рішень щодо створення оптимального задля досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах навколишньої обстановки.
- ***Інформаційний простір*** – простір, в якому створюється, переміщується і використовується інформація

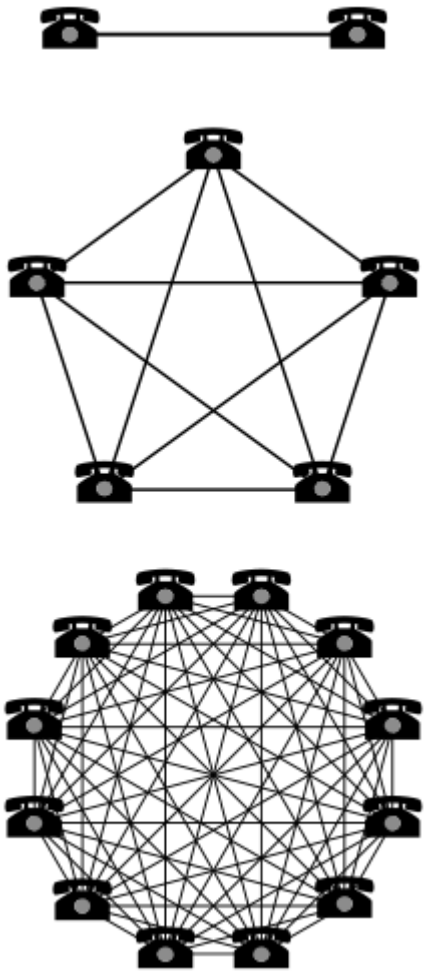
22 липня 2000 року прийнята
“Окінавська Хартія глобального інформаційного суспільства”

1 Поняття інформаційного простору

Процеси формування та розвитку сучасного **інформаційного суспільства**, базуються на синтезі двох технологій — комп’ютерної і телекомунікаційної.

Закон Мура: кількість транзисторів у процесорах збільшуватиметься вдвічі протягом кожних півтора року.

Закон Меткалфа: корисність телекомунікаційної мережі пропорційна квадрату числа підключених до неї користувачів.

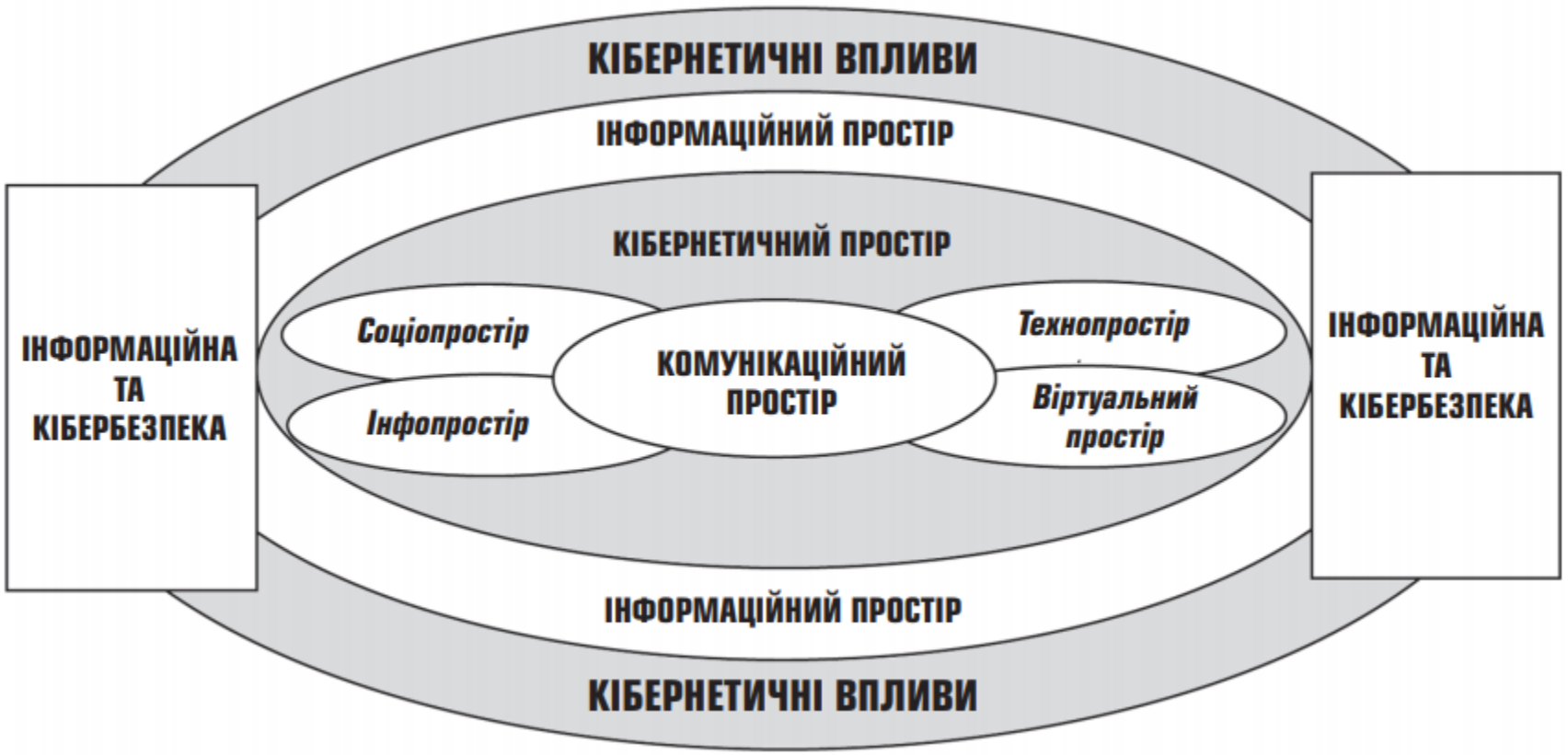


1 Поняття кіберпростору

Кіберпростір – високорозвинена модель об’єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

- подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді;
- розміщуються в пам’яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;
- перебувають у постійному русі по сукупності ІТ-систем і мереж.

1 Поняття кіберпростору



Кіберпростір –це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі

2 Інформаційні системи

- **Інформаційна система** (ІС) — сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів
- **Інформаційна система** — комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації.

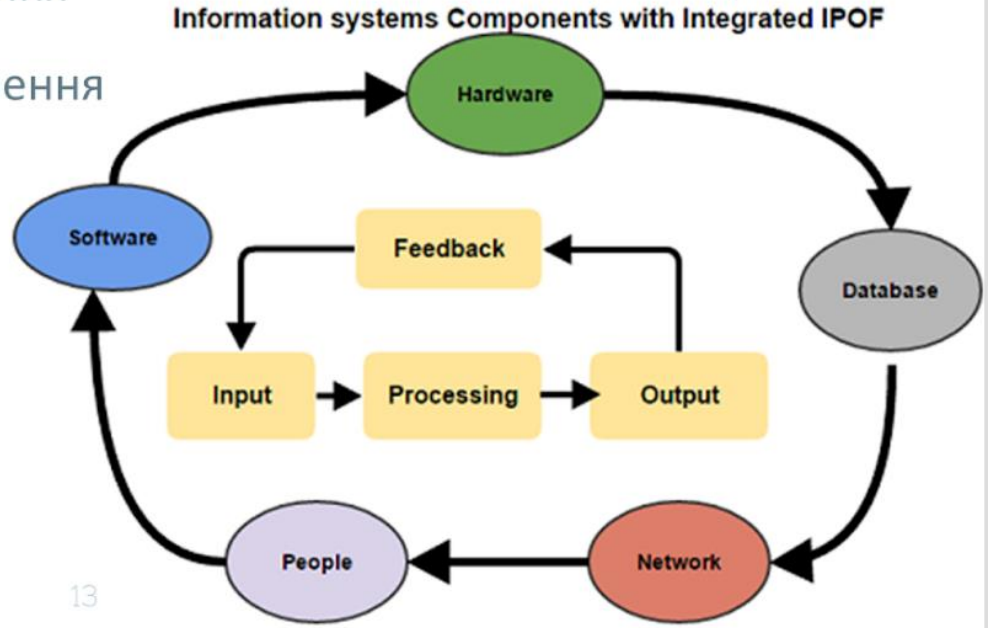
Людину чи будь-яку іншу живу істоту можна вважати біологічною інформаційною системою,

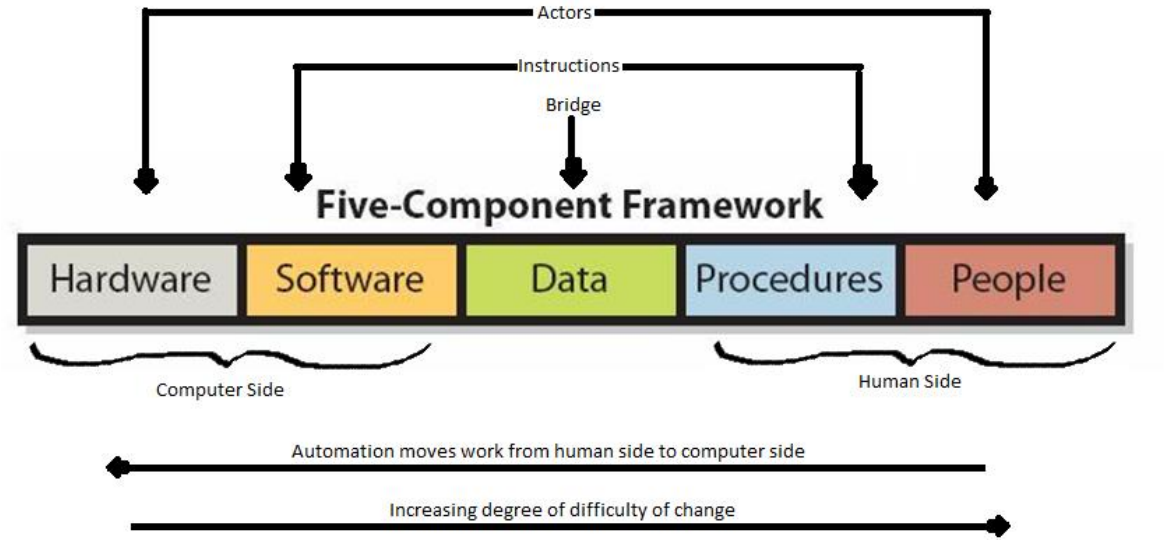
суспільство — соціальною інформаційною системою,

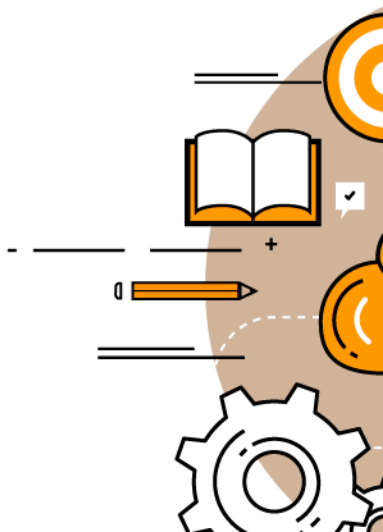
а комп’ютер — технічною.

2 Інформаційні системи

- Апаратне забезпечення
- Програмне забезпечення
- Телекомунікації
- Бази даних
- Люди та процедури







2 Інформаційні системи

Типова схема технічної інформаційної системи

3 Інформаційна безпека

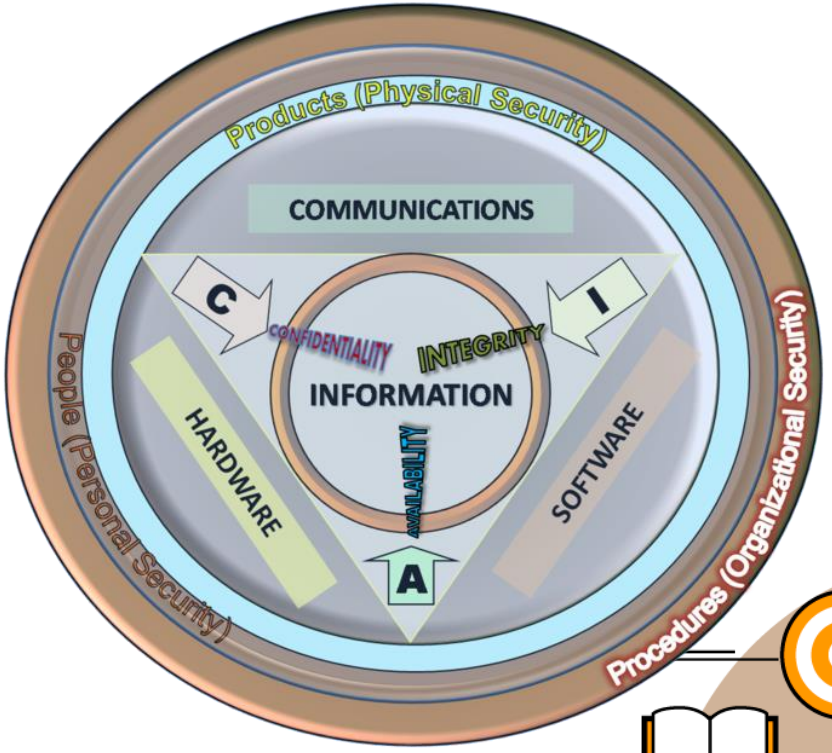
Інформаційна безпека (ІБ) – захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, здатних завдати збитків власникам або користувачам інформації.

Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

3 Інформаційна безпека

Основні задачі інформаційної безпеки:

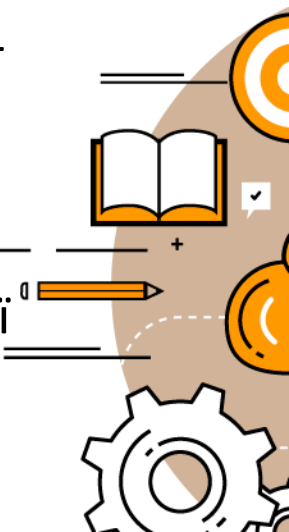
- забезпечення доступності інформації;
- забезпечення цілісності інформації;
- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;
- забезпечення невідстежуваності дій користувача.



3 Інформаційна безпека

Об’єктно-орієнтований підхід до ІБ

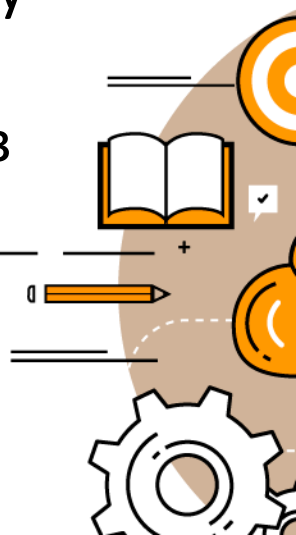
- Об’єктно-орієнтований підхід є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем.
- Об’єктно-орієнтований підхід використовує об’єктну декомпозицію, тобто, поведінка системи описується в термінах взаємодії об’єктів.
- Поняття *рівня деталізації* важливе не тільки для візуалізації об’єктів, але і для систематичного розгляду складних систем, представлених в ієрархічному вигляді. Якщо черговий рівень ієрархії розглядається з рівнем деталізації $n>0$, то наступний – з рівнем $(n-1)$. Об’єкт з рівнем деталізації 0 вважається атомарним.
- Об’єкти реального світу володіють, як правило, декількома відносно незалежними характеристиками. Стосовно об’єктної моделі такі характеристики називаються *гранями*. Основні гранями ІБ – доступність, цілісність і конфіденційність.



3 Інформаційна безпека

Об’єктно-орієнтований підхід до ІБ

- Об’єктно-орієнтований підхід є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем.
- Об’єктно-орієнтований підхід використовує об’єктну декомпозицію, тобто, поведінка системи описується в термінах взаємодії об’єктів.
- Поняття *рівня деталізації* важливе не тільки для візуалізації об’єктів, але і для систематичного розгляду складних систем, представлених в ієрархічному вигляді. Якщо черговий рівень ієрархії розглядається з рівнем деталізації $n>0$, то наступний – з рівнем $(n-1)$. Об’єкт з рівнем деталізації 0 вважається атомарним.



3 Інформаційна безпека

Об’єктно-орієнтований підхід до ІБ

- Об’єкти реального світу володіють, як правило, декількома відносно незалежними характеристиками. Стосовно об’єктної моделі такі характеристики називаються *гранями*. Основні грані ІБ – доступність, цілісність і конфіденційність.

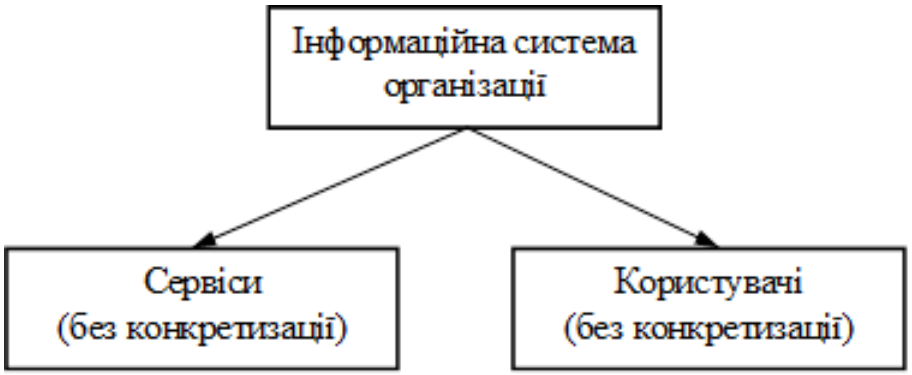
- Структура засобів досягнення мети ІБ:
  - ✓ законодавчі заходи забезпечення інформаційної безпеки;
  - ✓ адміністративні заходи (накази та інші дії керівництва організацій, пов’язаних з інформаційними системами, що захищаються);
  - ✓ організаційні (процедурні) заходи (заходи безпеки, орієнтовані на людей);
  - ✓ інженерно-технічні заходи.

3 Інформаційна безпека

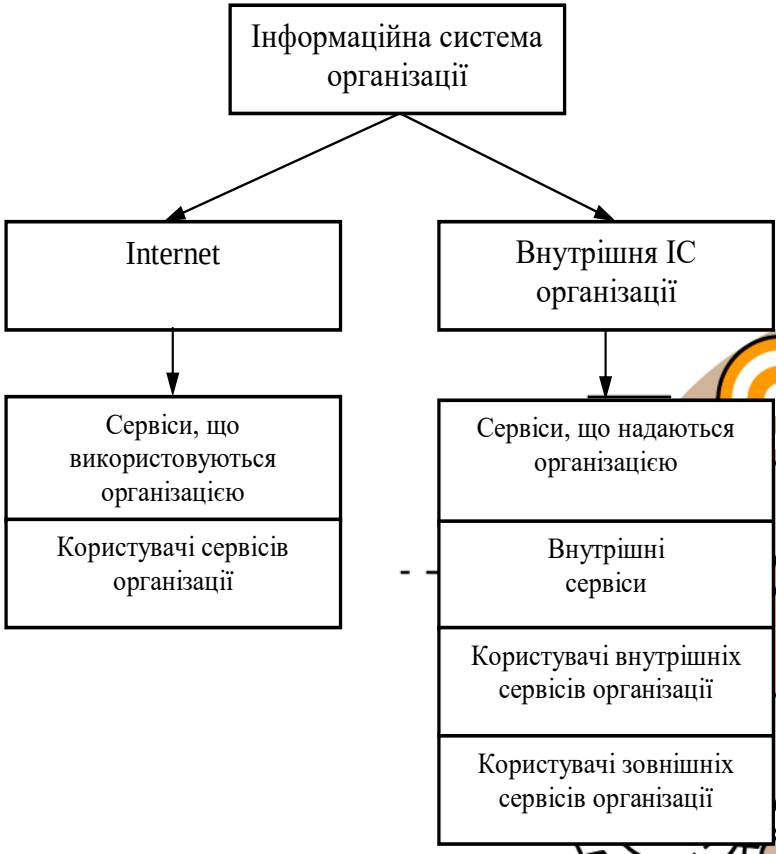
Об’єктно-орієнтований підхід до ІБ

Нульовому рівню деталізації відповідає інформаційна система в цілому.

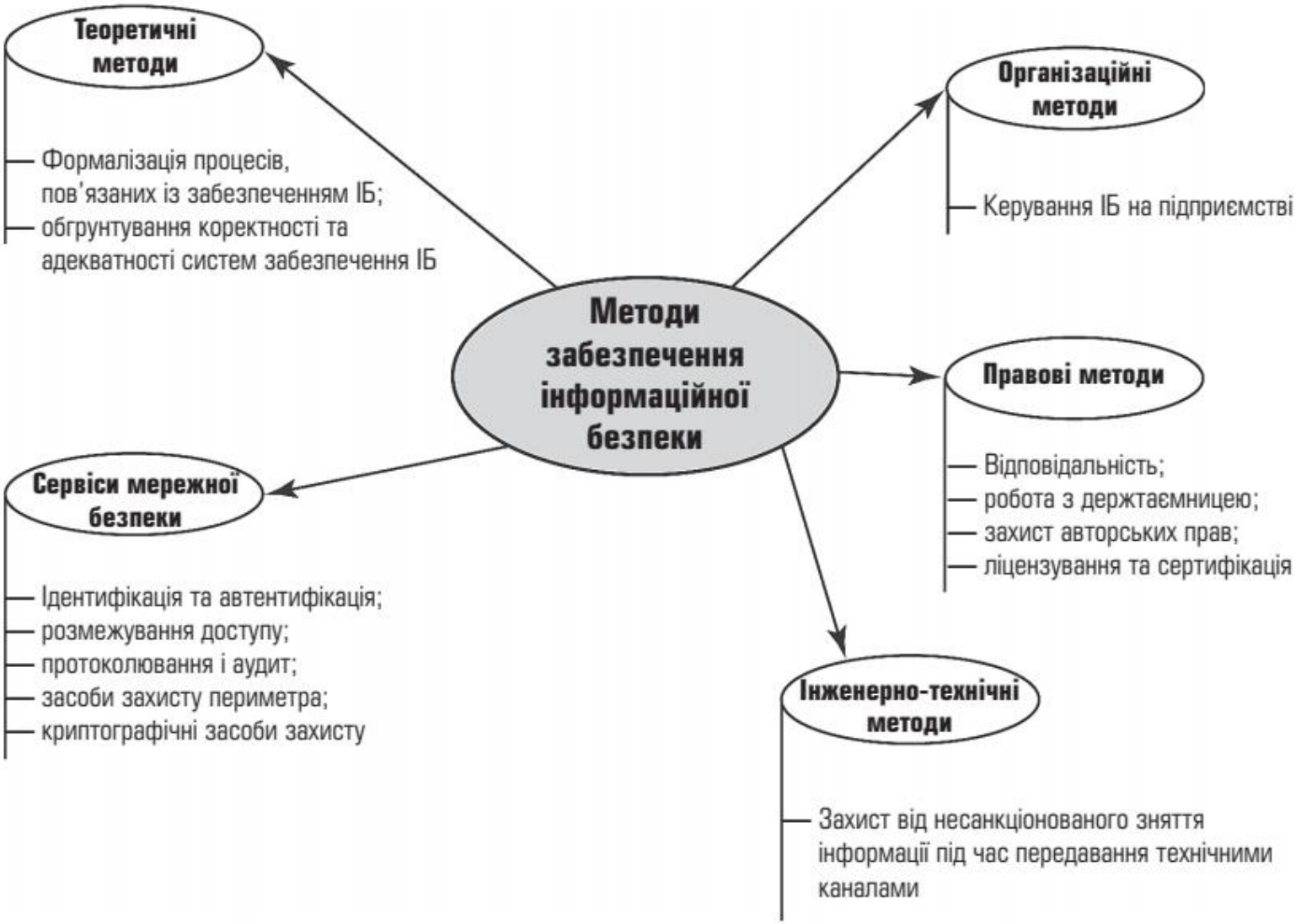
На **першому рівні** деталізації визначаються сервіси і користувачі, або, інакше кажучи, здійснюється поділ на клієнтську і серверну частину



На **другому рівні** деталізації ще не описується внутрішня структура ІС організації і деталі Internet.

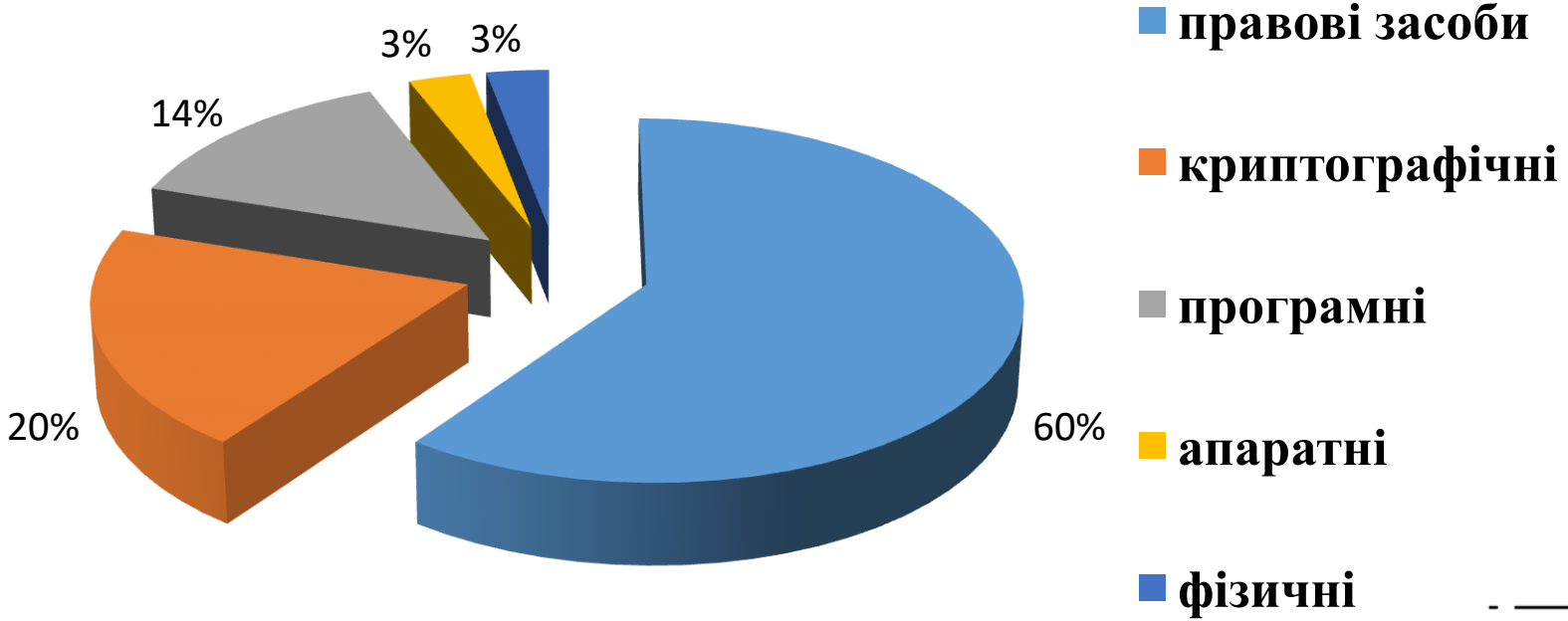


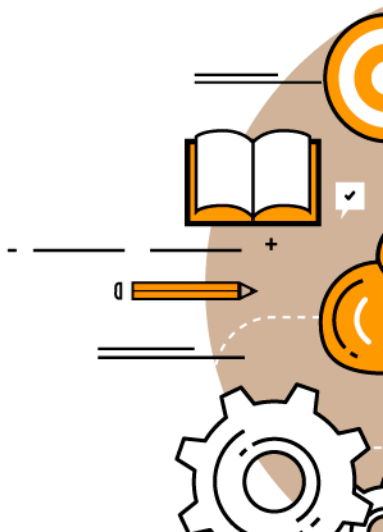
3 Інформаційна безпека



3 Інформаційна безпека

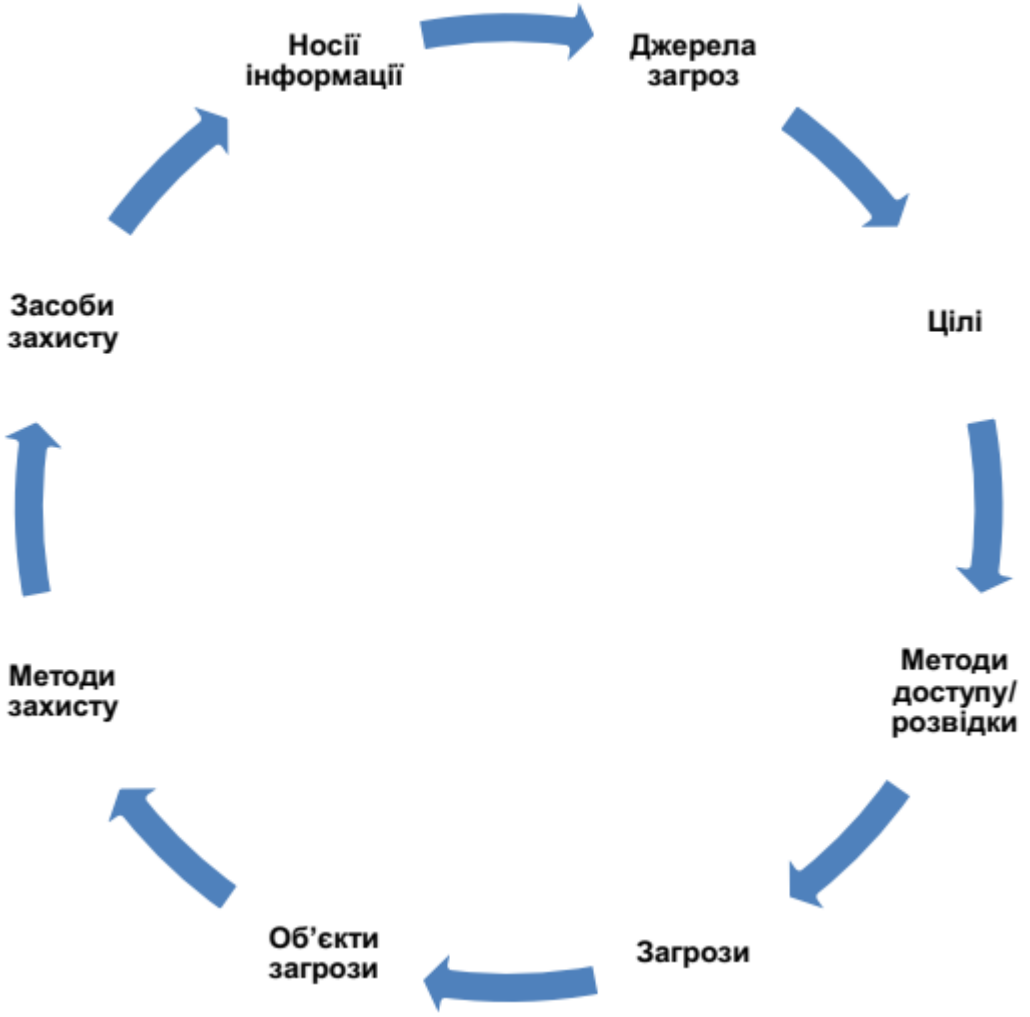
Питома вага форм захисту інформації

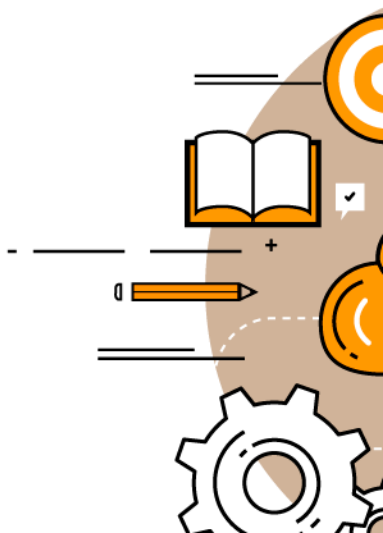




3 Інформаційна безпека

Циклічна модель забезпечення ІБ





4 Загрози безпеці інформації

Під ***загрозою безпеці*** будемо розуміти потенційно можливу подію, процес або явище, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформації.

- **випадкові** або ненавмисні (за статистичним даними – до 80% збитків від усіх можливих загроз);
- **навмисні**:
  - традиційне шпигунство;
  - тероризм і диверсії;
  - несанкціонований доступ до інформації в комп’ютерних системах;
  - технічна розвідка, що включає візуальну, акустичну та радіоелектронну розвідки;
  - кібернетичні атаки на комп’ютерні системи.

4 Загрози безпеці інформації

Шпигунство:
- розкрадання документів і машинних носіїв інформації, програм і атрибутів системи захисту;
- підкуп і шантаж співробітників;
- збір і аналіз відходів машинних носіїв інформації;
- підслуховування;
- візуальне спостереження;

Терор та диверсії реалізуються не тільки шляхом підпалів, вибухів, захоплення заручників, транспортних засобів та високотехнологічних виробництв, а й завдяки застосуванню методів спрямованого надпотужного електромагнітного випромінювання.

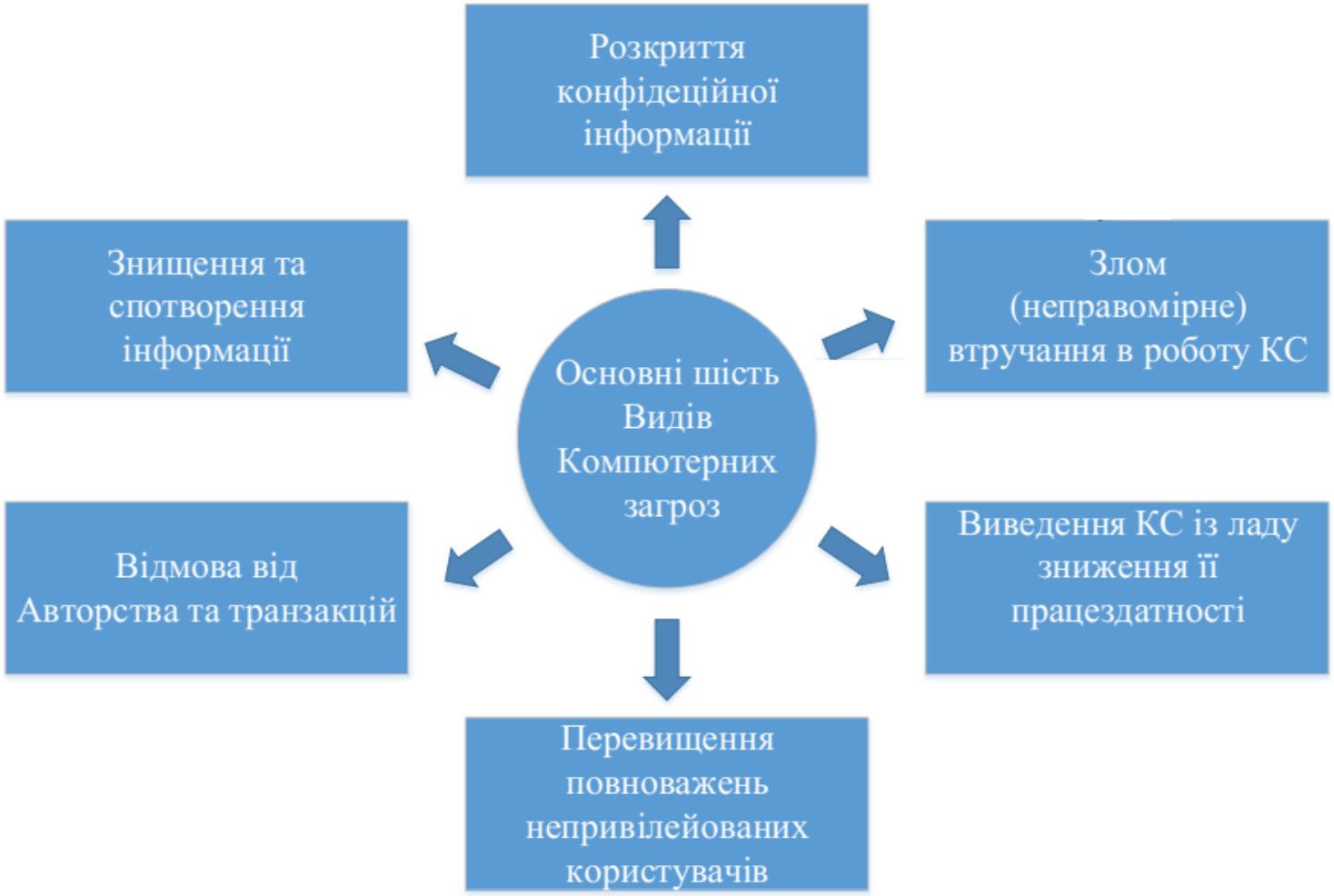
4 Загрози безпеці інформації

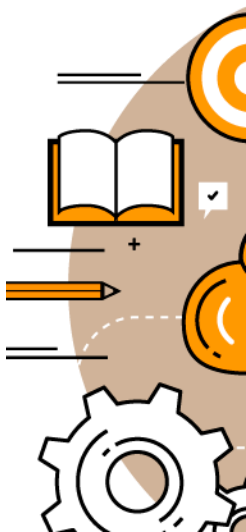
Виконання встановлених правил розмежування доступу в ІС реалізується за рахунок створення системи розмежування доступу (СРД).

Несанкціонований доступ до інформації з використанням штатних апаратних і програмних засобів відбувається в наступних випадках:

- відсутність системи розмежування доступу, помилки в її елементах зроблені під час розробки, збій або відмова в її функціонуванні;
- помилки користувачів автоматизованих систем або адміністраторів безпеки;
- фальсифікація повноважень або навмисне блокування роботи СРД.

4 Загрози безпеці інформації





4 Загрози безпеці інформації

Класифікація джерел інцидентів Інтерполом

1)QA — несанкціонований доступ або перехоплення:

QAH — комп’ютерний абордаж;

QAI — перехоплення;

QA1 — крадіжка часу;

QAZ — інші види несанкціонованого доступу й перехоплення;

2) QD — зміна комп’ютерних даних:

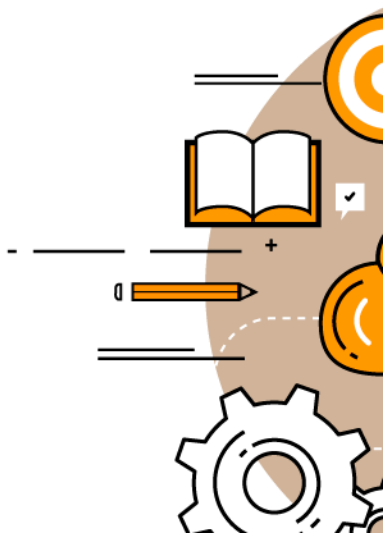
QDL — логічна бомба;

QDT— троянський кінь;

QDV— комп’ютерний вірус;

QDW— комп’ютерний хробак;

QDZ— інші види зміни даних;



4 Загрози безпеці інформації

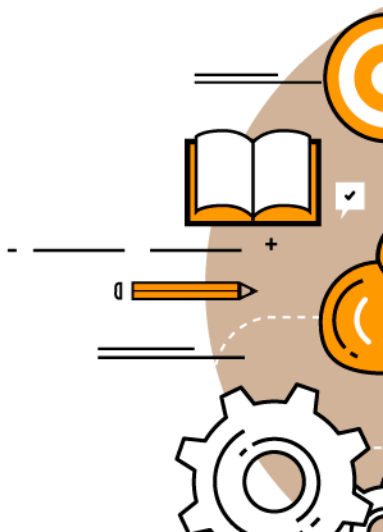
Класифікація джерел інцидентів Інтерполом

3) QF — комп’ютерне шахрайство (computer fraud):

QFC— шахрайство з банкоматами;
QFF— комп’ютерна підробка;
QFG— шахрайство з ігровими автоматами;
QFM— маніпуляції з програмами вводу/виводу;
QFP — шахрайство з платіжними засобами;
QFT— телефонне шахрайство;
QFZ— інші види комп’ютерного шахрайства;

4) QR — незаконне копіювання («піратство»):

QRG — комп’ютерні ігри;
QRS — інше програмне забезпечення;
QRT — топографія напівпровідникових виробів;
QRZ — інше незаконне копіювання;



4 Загрози безпеці інформації

Класифікація джерел інцидентів Інтерполом

5) QS — комп’ютерний саботаж:

QSH — з апаратним забезпеченням;

QSS — із програмним забезпеченням;

QSZ — інші види саботажу;

6) QZ — інші комп’ютерні злочини:

QZB — із використанням комп’ютерних дощок оголошень;

QZE — розкрадання інформації, що становить комерційну таємницю;

QZS — передавання інформації конфіденційного характеру;

QZZ — інші комп’ютерні злочини.

5 Модель захисту від загроз

В рамках нормативних документів системи технічного захисту інформації автоматизована система (АС) розглядається як організаційно-технічна система, що об’єднує програмне забезпечення (включаючи, операційну систему - ОС, прикладні програми), фізичне середовище, персонал і оброблювану інформацію.

- клас «1» - один комп’ютер + один користувач;
- клас «2» - локальна обчислювальна мережа;
- клас «3» - розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

(істотною відміною цього класу від класу «2» є необхідність передачі інформації через незахищені канали або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Прикладом цього класу є глобальна мережа.)

5 Побудова моделі загроз (приклад)

Варіант опису штучних навмисних загроз і їх класифікацію для КС другого класу:

початкові дані:

- технологія мережі - Ethernet, що працює на швидкості 100 Мбіт/с, з середовищем передачі інформації 10BASE-T (вита пара), 10BASE-FL та Radio Ethernet;
- топологія - типу «пасивне дерево»;
- комутаційні вузли і устаткування, що забезпечує передачу:

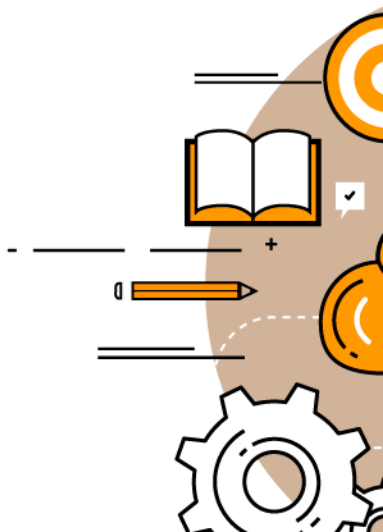
o кабелі для передачі інформації; o роз'єми для приєднання кабелів;
o мереживі адаптери; o конвертори-трансівери;
o концентратори; o комутатори;
o маршрутизатори; o шлюзи;

- мережа функціонує на основі декількох серверів:

o Web; o FTP; o поштовий;

- використовується два стеки протоколів IBM/Microsoft і TCP/IP;
- операційні системи на серверах і робочих станціях КС:

o різні версії Windows;
o різні версії Linux.



5 Побудова моделі загроз (приклад)

Знакомісце	Загрози
+.*.*.*.0	**ЗШ** - зовнішні, **ВТ** – внутрішні.
.+..*.0	**П** – пасивні, **А** – активні.
..+.*.0	**К** – порушення конфіденційності, **Ц** – порушення цілісності, **Д** – порушення доступності.
..*.+.0	**КВІ** – по каналах витоку інформації, **КСВ** – по каналах спеціального впливу, **НСД** – шляхом несанкціонованого доступу в КС.

Ідентифікатор					Опис загрози
ВТ	А	Д	НСД	1	Порушення фізичної цілісності ліній зв'язку
ВТ	А	Д	НСД	2	Порушення фізичної цілісності комутаційних вузлів
ВТ	А	Д	НСД	3	Фізичний вивід з ладу серверів ЛОМ
ВТ	А	Д	КСВ	1	Формування спеціальних сигналів в лініях зв'язку і комутаційних вузлах з метою порушення працездатності мережі
ЗШ	А	Д	КСВ	2	Формування спеціальних радіосигналів для блокування виходу ЛОМ по радіоканалу в глобальну мережу
ВТ	А	К	КВІ	1	Індукційне зняття інформації в електричних лініях зв'язку
ВТ	А	К	КВІ	2	Контактне підключення до ліній зв'язку з метою перехоплення інформації
ЗШ	П	К	КВІ	3	Перехоплення даних в радіоканалі
ЗШ	П	К	КВІ	4	Перехоплення ПЕМВН при функціонуванні комп'ютерів і комунікаційних вузлів ЛОМ

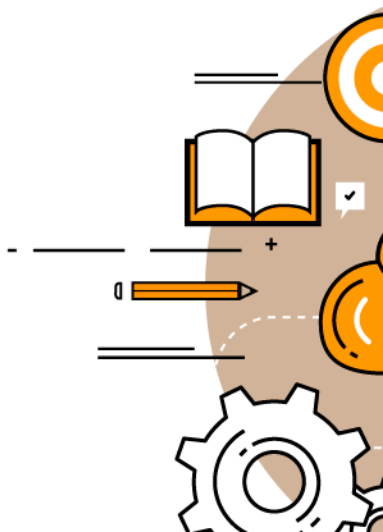
5 Побудова моделі загроз (приклад)

Ідентифікатор	Джерела загроз інформаційної безпеки
[1.0.0]	*АНТРОПОГЕННІ ДЖЕРЕЛА*
[1.A.0]	***Зовнішні антропогенні джерела***
[1.A.1]	кримінальні структури
[1.A.2]	потенційні злочинці і хакери
[1.A.3]	недобросовісні партнери
[1.A.4]	технічний персонал постачальників телематичних послуг
[1.A.5]	представники наглядових організацій і аварійних служб
[1.A.6]	представники силових структур
[1.B.0]	***Внутрішні антропогенні джерела****
[1.B.1]	основний персонал (користувачі, програмісти, розробники)
[1.B.2]	представники служби захисту інформації (адміністратори)
[1.B.3]	допоміжний персонал (прибиральники, охорона)
[1.B.4]	технічний персонал (життєзабезпечення, експлуатація)
[2.0.0]	*ТЕХНОГЕННІ ДЖЕРЕЛА*
[2.A.0]	***Зовнішні техногенні джерела загроз***
[2.A.1]	засоби зв'язку
[2.A.2]	мережі інженерних комунікацій (водопостачання, каналізації)
[2.A.3]	транспорт
[2.B.0]	***Внутрішні техногенні джерела загроз***
[2.B.1]	неякісні технічні засоби обробки інформації
[2.B.2]	неякісні програмні засоби обробки інформації
[2.B.3]	допоміжні засоби (охорона, сигналізації, телефонії)
[2.B.4]	інші технічні засоби, вживані в установі

5 Побудова моделі загроз (приклад)

[3.0.0]	*СТИХІЙНІ ДЖЕРЕЛА ЗАГРОЗ*
[3.A.0]	***Зовнішні стихійні джерела***
[3.A.1]	пожежі
[3.A.2]	землетруси
[3.A.3]	повені
[3.A.4]	урагани
[3.A.5]	магнітні бурі
[3.A.6]	радіоактивне випромінювання
[3.A.7]	різні непередбачені обставини
[3.A.8]	нез'ясовні явища
[3.A.9]	інші форс-мажорні обставини**

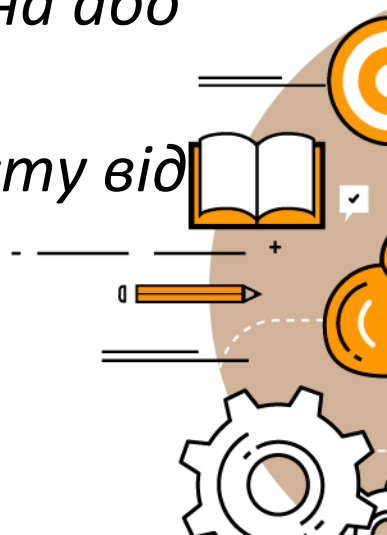
При виборі методу *ранжирування джерел загроз* можна використовувати методологію, викладену в міжнародних стандартах, а також практичний досвід експертів в сфері інформаційної безпеки.



5 Модель порушника в ІС

Модель порушника - абстрактний формалізований або неформалізований опис зловмисника, який прагне реалізувати атаку.

Неформальна модель порушника відображає його практичні і теоретичні можливості, апріорні знання, час і місце дії і т.п. Для досягнення своєї мети порушник повинен докласти зусилля, витратити певні ресурси. *Дослідивши причини порушень, можна або вплинути на ці причини (якщо можливо), або точніше визначити вимоги до системи захисту від даного виду порушень або злочинів.*

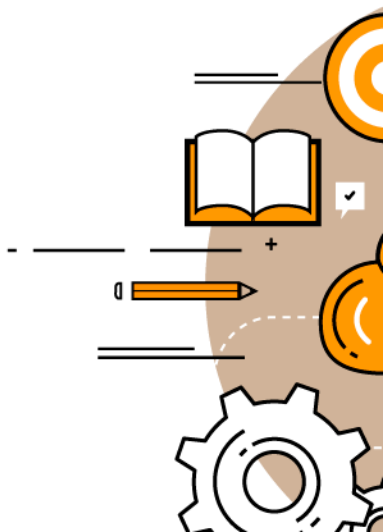


5 Модель порушника в ІС

При розробці моделі порушника можуть враховуватися наступні можливі відомості

- категорії осіб, з числа яких може бути порушник;
- мотиви (цілі) порушника;
- ступінь знань про ІС;
- використовувані технічні засоби;
- місце дії;
- час дії;
- і таке інше.

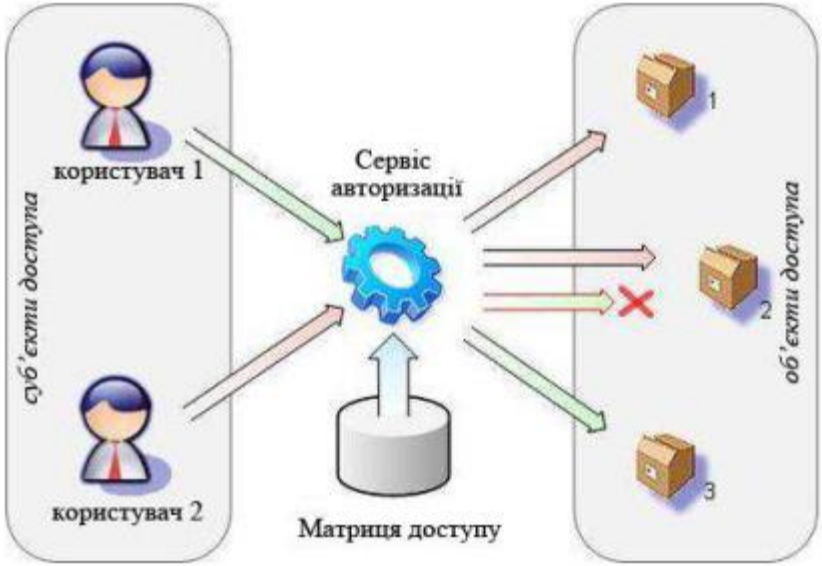
Можна виділити три основні мотиви порушень: недбалість (безвідповідальність), самоствердження (помста) і корисливий інтерес.

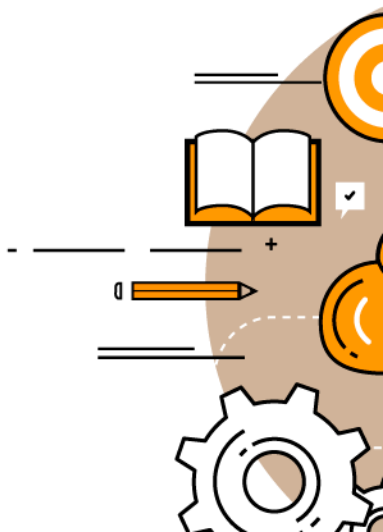


5 Моделі захисту інформації

Більшість моделей захисту інформації базується на одному з двох базових методів розмежування доступу суб'єктів інформаційних систем до об'єктів ***дискреційному*** або ***мандатному***.

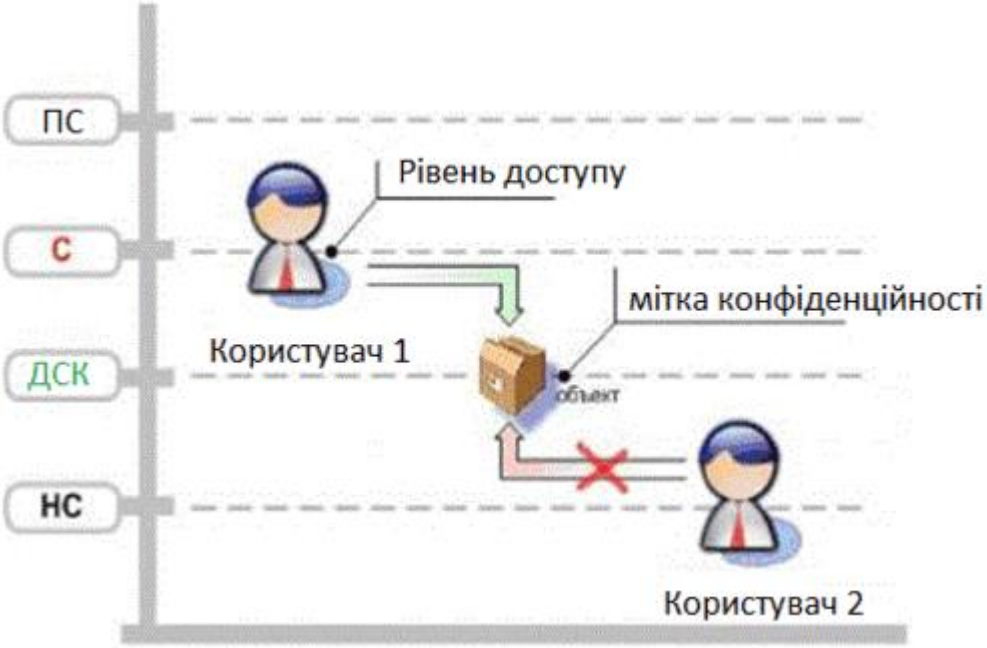
Дискреційне або матричне (вибіркове) управління доступом





5 Моделі захисту інформації

Мандатне управління доступом (англ. Mandatory access control, MAC) - вид розмежування доступу суб'єктів до об'єктів, що заснований на призначенні позначки конфіденційності для інформації, що міститься в об'єктах, та видачі спеціального дозволу суб'єктам для поводження з інформацією такого рівня конфіденційності.



ПС — повністю секретно;
С — секретно;
ДСК — для службового користування;
НС — не секретно.

5 Політика безпеки

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

Етап 1. Реєстрація ресурсів, які підлягають захисту.
Етап 2. Визначення потенційних загроз для кожного ресурсу.
Етап 3. Оцінка ймовірності появи кожної загрози та можливі втрати від неї.
Етап 4. Прийняття рішень щодо захисту ІС.