ЛЕКЦІЯ 2

ЗАГРОЗИ ІБ В ІКС, КІБЕРАТАКИ ТА КІБЕРТЕРОРИЗМ: ПОНЯТТЯ І ВИЗНАЧЕННЯ

ЛІТЕРАТУРА:

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015. — 288 с.
2. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. — К.:Видавнича група BHV, 2009. — 608 с.:іл.
3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. - К. : ЦП «Компринт» О.В., 2021. - 444 с.

ПИТАННЯ:

1. Загрози та вразливості інформаціної безпеки(ІБ) інформаційно-комунікаційних систем(ІКС): поняття, визначення та класифікація.
2. Кібератаки: поняття, визначення та класифікація. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу.
3. Кібертероризм: поняття та визначення. Наслідки кібертероризму.

ПИТАННЯ №1

ЗАГРОЗИ ТА ВРАЗЛИВОСТІ ІНФОРМАЦІНОЇ БЕЗПЕКИ(ІБ) ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ(ІКС): ПОНЯТТЯ, ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ.

Основні поняття та визначення

Несприятливий вплив (англ. — undesired event) — вплив, що призводить до зменшення цінності інформаційних ресурсів.

Загроза (англ. - threat) — будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС. Тобто загроза — це будь-який потенційно можливий несприятливий вплив.

Уразливість системи (англ. — system vulnerability) — нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.

Вади захисту (англ. — security flaw) — сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або політики безпеки інформації. Здебільшого під вадами захисту розуміють особливості побудови програмних (а іноді й апаратних) засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам і виконувати свої функції. Тобто вади захисту є окремим випадком уразливості системи.

Загрози безпеці інформації

До можливих загроз безпеки інформації належать:

- стихійні лиха й аварії;
- збої та відмови устаткування;
- наслідки помилок проектування і розробки компонентів АС;
- помилки персоналу під час експлуатації;
- навмисні дії зловмисників і порушників.

Узагальнена класифікація загроз

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Природа виникнення	Природні загрози (загрози, які виникають через впливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини). Штучні загрози (загрози, викликані діяльністю людини)
Принцип НСД	Фізичний доступ: ✦ подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; ✦ розкрадання документів і носіїв інформації; ✦ візуальне перехоплення інформації, виведеної на екрани моніторів і принтери; ✦ підслуховування; ✦ перехоплення електромагнітних випромінювань. Логічний доступ (доступ із використанням засобів комп'ютерної системи)
Мета НСД	Порушення конфіденційності (розкриття інформації). Порушення цілісності (повне або часткове знищення інформації, її спотворення, фальсифікація, викривлення). Порушення доступності (наслідок — відмова в обслуговуванні)

Узагальнена класифікація загроз

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Причини появи вразливостей різних типів	Недоліки політики безпеки. Помилки адміністративного керування. Недоліки алгоритмів захисту. Помилки реалізації алгоритмів захисту
Об'єкт безпосередньої атаки	Політика безпеки АС. Компоненти системи захисту АС. Протоколи взаємодії. Функціональні компоненти АС
Стан кінцевого об'єкта атаки	Зберігання (об'єкт знаходиться на зовнішніх носіях). Оброблення (об'єкт знаходиться в оперативній пам'яті). Передавання (об'єкт просувається через лінію зв'язку)

Узагальнена класифікація загроз

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Спосіб впливу на об'єкт атаки	Безпосередній вплив. Вплив на систему дозволу «Маскарад». Використання наосліп
Спрямованість НСД	Безпосереднє стандартне використання: ✦ слабкостей політики безпеки; ✦ недоліків адміністративного керування. Приховане нестандартне використання: ✦ недокументованих особливостей системи; ✦ прихованих каналів
Характер впливу	Активний (внесення змін в АС). Пасивний (спостереження)
Режим НСД	За постійної участі людини (в інтерактивному режимі) можливе застосування стандартного ПЗ. Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ

Узагальнена класифікація загроз

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Умова початку здійснення впливу	У відповідь на запит від об'єкта, який атакують. Після визначеної події на об'єкті. Безумовна атака
Місцезнаходження джерела НСД	Внутрішньосегментне (джерело знаходиться в локальній мережі). У цьому випадку, як правило, ініціатор атаки — санкціонований користувач. Міжсегментне: ✦ несанкціоноване вторгнення з відкритої мережі в закриту; ✦ порушення обмежень доступу з одного сегмента закритої мережі в інший
Наявність зворотного зв'язку	Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив) Без зворотного зв'язку (атакуючий не отримує відповіді)
Рівень моделі взаємодії відкритих систем (Open Systems Interconnection, OSI)	Вплив може бути здійснено на таких рівнях: фізичному, канальному, мережному, транспортному, сеансовому, представницькому, прикладному

Перелік типових загроз ІБ

1. Природні загрози.
2. Штучні загрози:
   1) Ненавмисні загрози:
      - Ненавмисні дії, що призводять до відмови системи.
      - Неправомірне відключення устаткування чи зміна режимів роботи пристроїв і програм.
      - Ненавмисне псування носіїв інформації.
      - Запуск технологічних програм, здатних за некомпетентного використання викликати втрату працездатності системи чи незворотні зміни в ній.
      - Нелегальне впровадження і використання неврахованих програм.
      - Ненавмисне зараження вірусом.
      - Необережні дії, що призводять до розголошення конфіденційної інформації.
      - Розголошення, втрата атрибутів розмежування доступу.
      - Проектування архітектури системи з можливостями, що становлять небезпеку для самої системи.
      - Ігнорування організаційних обмежень.
      - Входження у систему в обхід засобів захисту.
      - Некомпетентне використання, настроювання і неправомірне відключення засобів захисту.
      - Пересилання даних за адресою абонента, яка є хибною.
      - Введення помилкових даних.
      - Ненавмисне ушкодження каналів зв’язку.

Перелік типових загроз ІБ

1) Навмисні загрози:
   - Фізичне руйнування системи.
   - Вимкнення чи виведення з ладу підсистем забезпечення функціонування.
   - Дії з дезорганізації функціонування системи.
   - Вторгнення агентів у оточення персоналу системи.
   - Вербування персоналу чи окремих користувачів, що мають визначені повноваження.
   - Застосування пристроїв, що підслуховують, дистанційних фото- та відеозйомок.
   - Перехоплення побічних електромагнітних, акустичних та інших випромінювань і наведень від пристроїв і каналів зв’язку.
   - Перехоплення даних, переданих по каналах зв’язку.
   - Розкрадання носіїв інформації.
   - Несанкціоноване копіювання носіїв інформації.
   - Розкрадання і вивчення виробничих відходів.
   - Зчитування залишкової інформації з оперативної пам’яті та зовнішніх запам’ятовуючих пристроїв.
   - Незаконне заволодіння паролями.
   - Несанкціоноване використання терміналів користувачів.
   - Розкриття шифрів криптографічно захищеної інформації.
   - Впровадження програмно-апаратних закладок і вірусів.
   - Незаконне підключення до ліній зв’язку з метою роботи «між рядків».
   - Незаконне підключення до ліній зв’язку з метою прямої підміни законного користувача шляхом його повного відключення.

Методика класифікації загроз STRIDE

Методика **STRIDE** розроблена, обґрунтована та активно пропагується фахівцями з корпорації Майкрософт. Фактично, це ще один варіант класифікації загроз за їхніми наслідками. Методику використовують для побудови моделі загроз під час розроблення ПЗ. Назву методики утворено з перших літер назв категорій загроз.

- ***Підміна об'єктів*** (англ. — spoofing identity). Крім згаданих вище загроз, які виникають через недоліки мережних протоколів, до цього класу належить також загроза, викликана підміною особи користувача. Її здійснюють, скориставшись слабкістю системи автентифікації або здобувши автентифікаційні дані шляхом крадіжки чи шахрайства (так звана соціальна інженерія).
- ***Модифікація даних*** (англ. — tampering with data). До цього класу належать загрози впливів (атак), мета яких — навмисне пошкодження даних. Атаки можуть бути спрямовані на інформаційні об'єкти, що перебувають у стані зберігання (файли, бази даних), і такі, що передаються мережею.
- ***Відмова від авторства*** (англ. — repudiation of origin). Загрози цього класу дають змогу порушнику відмовитися від здійснених ним дій (або бездіяльності). Причиною існування такої загрози є відсутність або слабкість механізмів реєстрації подій і слабкі механізми автентифікації.

Методика класифікації загроз STRIDE

- ***Розголошення інформації*** (англ. — information disclosure). Загрози цього класу не потребують коментарів.
- ***Відмова в обслуговуванні*** (англ. — denial of service). Атаки, що спричиняють відмову в обслуговуванні, порівняно легко здійснити в розподілених системах і дуже важко їм протидіяти. Особливо небезпечними є атаки розподіленої відмови в обслуговуванні (англ. — distributed denial of service), які здійснюють на один об'єкт одразу з кількох вузлів мережі.
- ***Підвищення привілеїв*** (англ. — elevation of privilege). До цього класу належать загрози, які дають можливість порушнику підвищити свої привілеї у системі. Наприклад, звичайний користувач отримує повноваження адміністратора, або порушник, що підключився без автентифікації до будь-якого мережного сервісу, виконує дії як авторизований користувач.

ПИТАННЯ №2

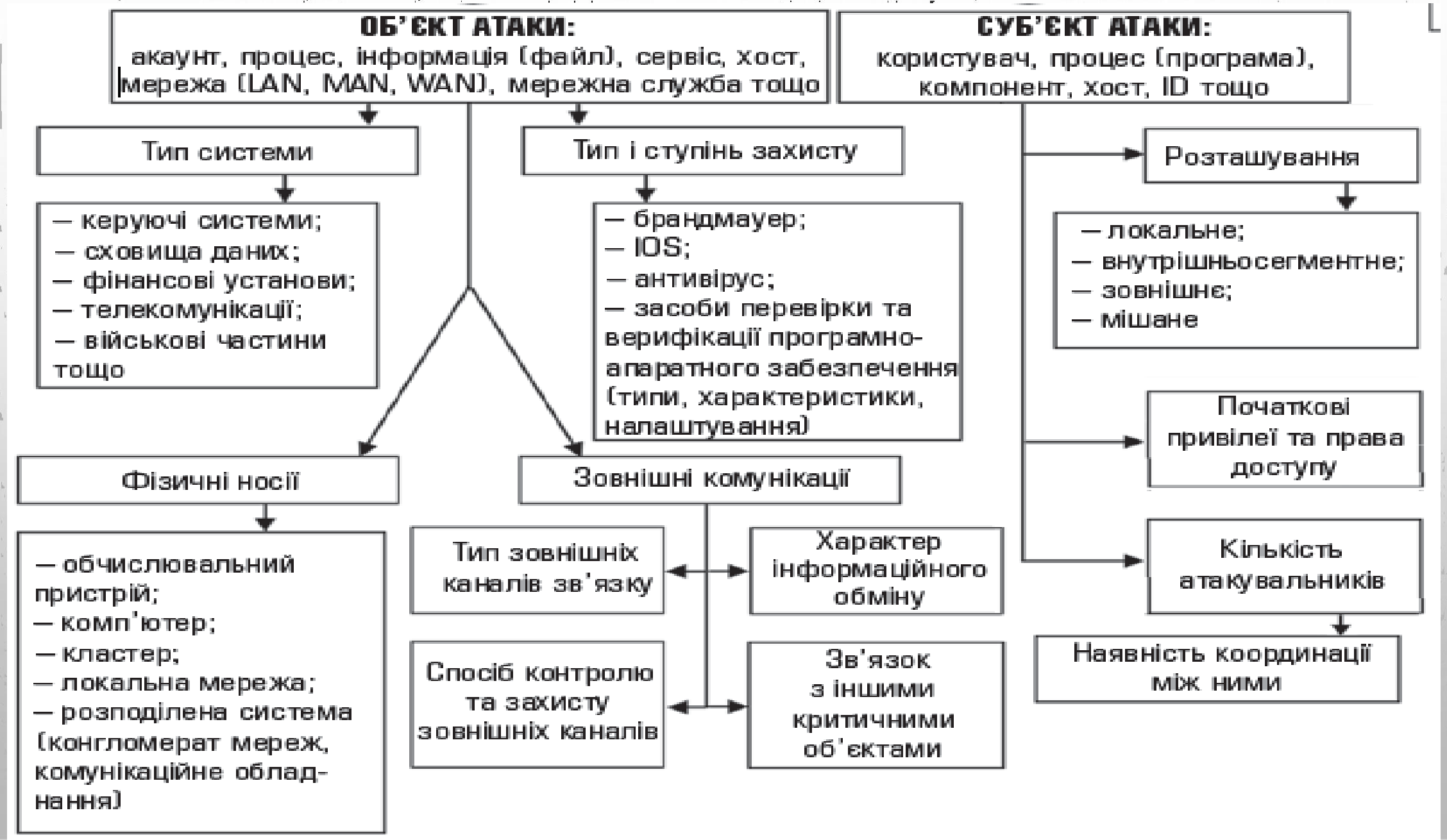
КІБЕРАТАКИ: ПОНЯТТЯ, ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ АТАК І ЗАХОДИ З ПОСЛАБЛЕННЯ ЇХНЬОГО ДЕСТРУКТИВНОГО ВПЛИВУ

Визначення поняття «кібератака»

Кібератака — сукупність узгоджених щодо мети, змісту та часу дій або заходів — так званих кіберакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності і/або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи іт-систем і мереж зазначеного об’єкта.

Загальна структура кібернетичної атаки

Загальна структура кібернетичної атаки



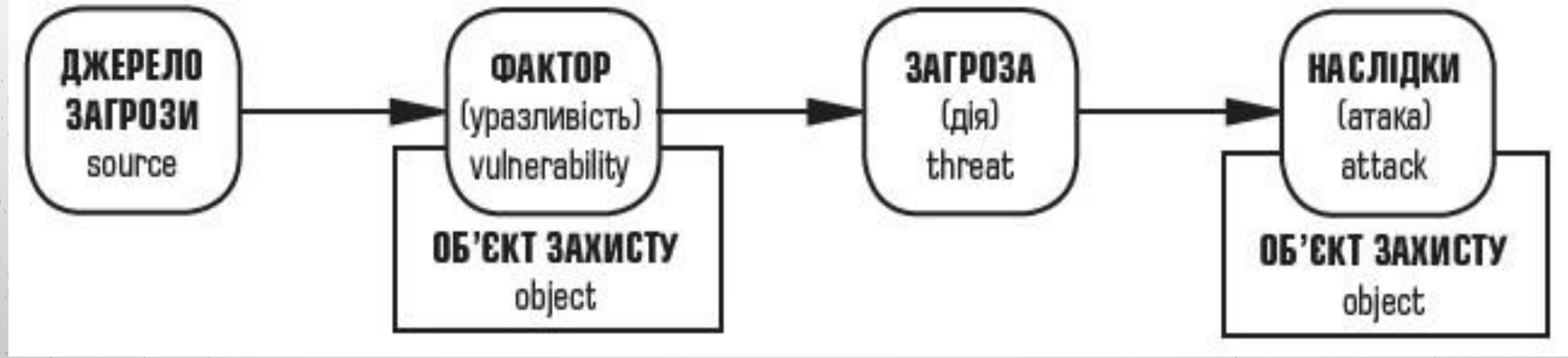
Класифікація кібератак

1. ***За метою впливу на об'єкт атаки***(порушення цілісності (integrity) або конфіденційності (confidentiality) інформації, її захищеності від несанкціонованого доступу (authentication), а також на порушення живучості (survivability) системи та надійності (availability) її функціонування);
2. ***За принципом впливу на об'єкт атаки***(використання прихованих каналів; застосування прав суб'єкта системи до об'єкта);
3. ***За характером впливу на об'єкт атаки***(активні та пасивні);
4. ***За способом впливу на об'єкт атаки***, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв.

Класифікація кібератак

5. ***За засобами впливу на об'єкт атаки***(використання або стандартного ПЗ, або спеціально розроблених програм);
6. ***За об'єктом атаки***(на систему в цілому; на дані і програми, що містяться на зовнішніх або внутрішніх пристроях системи, а також у каналах передавання даних; на процеси і підпроцеси системи за участю користувачів);
7. ***За станом об'єкта***(безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися);
8. ***За використовуваною системою захисту***; ***за кількістю атакувальників***; ***за джерелами атак***; ***за розміщенням атакуючого об'єкта відносно атакованого***; ***за наявністю зв'язку з атакованим об'єктом***; ***за рівнем еталонної моделі OSI об'єкта, на який здійснюється вплив***.

Механізм формування кібератаки



Джерела несанкціонованих дій

Основні типи кібератак згідно класифікацією П. Ноймана

Тип атак	Спосіб здійснення	Результат
Зовнішні	Візуальне спостереження	Спостереження за клавіатурою або монітором
	Омана	Уведення в оману операторів або користувачів
	Вилучення сміття	Вилучення інформації зі сміттєвих корзин
Апаратні	Логічне відновлення	Вилучення інформації з викрадених носіїв
	Прослуховування	Перехоплення даних
	Втручання	—
	Фізична атака	Руйнування або ушкодження обладнання, джерел живлення
	Фізичне видалення	Вилучення обладнання або сховищ даних
Маскувальні	Імітування	Використання хибних ідентифікаторів
	Узурпація ліній зв'язку або хостів	—
	Атака з підміною параметрів	—
	Заплутування мереж	Маскування фізичного місця розташування або маршруту

Основні типи кібератак згідно класифікацією П. Ноймана

Злоякісні програмні коди		Троянські коні	Впровадження злоякісного коду
		Логічні бомби	Різновид троянських коней
		Черв'яки	Заволодіння розподіленими ресурсами
		Віруси	Прикріплення до програм та розповсюдження
		Обхід	Обхід механізмів безпеки
		Експлуатація уразливостей	—
		Зламування паролів	—
Зловживання	активне	Інкрементальні атаки	Поступова ескалація привілеїв, повільне просування до мети
		Відмова в обслуговуванні	Здійснення масованих атак
	пасивне	Огляд	Випадковий або вибірковий пошук
		Збір та виведення даних	Використання баз даних та аналіз трафіку
		Приховані канали	Використання прихованих каналів або інших способів витоку інформації
	інертне	—	—
	побічне	—	—

Особливості найпоширеніших кібератак

№ з/п	Тип атаки	Опис впливу
1	Denial of service	Атака з поодинокого джерела. Блокує авторизованим користувачам доступ до того чи іншого комп'ютера-жертви через «переповнення» легального трафіку зовнішніми повідомленнями
2	Distributed denial of service	Скоординована атака відразу з багатьох комп'ютерів. Для її організації комп'ютери, що беруть у ній участь, часто попередньо заражаються спеціальними програмами — черв'яками
3	Exploit tools	Привселюдно доступні засоби проникнення в системи різного рівня складності з метою пошуку в тій чи інший кіберсистемі уразливих місць і одержання доступу до комп'ютера-жертви
4	Logic bombs	Форма саботажу, коли програміст уводить спеціально сконструйований код, що викликає деструктивну роботу виконуваної програми, зокрема її повне припинення
5	Phishing	Створення та подальше використання спеціальних електронних повідомлень і web-сайтів, подібних до легальних і добре відомих користувачам. Має на меті дезорієнтувати користувачів, спонукати їх до розкриття своїх персональних даних
6	Sniffer	Програма, що перехоплює та фільтрує інформаційний трафік, вишукуючи в ньому спеціальну інформацію про користувача, наприклад передані паролі
7	Trojan horse	Комп'ютерна програма, що містить неявні шкідливі коди. Трояни, як правило, маскуються під звичайні програми, якими користувач зазвичай послуговується

Особливості найпоширеніших кібератак

8	Virus	Програма, що інфікує комп'ютерні файли включенням до них спеціальних команд. Ці команди виконуються, як правило, при завантаженні інфікованого файла в оперативну пам'ять комп'ютера. На відміну від комп'ютерних черв'яків, розмноження вірусів вимагає втручання (хоча найчастіше й неусвідомленого) людини-користувача
9	Vishing	Різновид фішингу, який використовує дешеві інтернет-технології для передавання звукових (у тому числі голосових) файлів. Дає змогу шахраям створювати власні телефонні «кол-центри» і звідти (від імені легальних користувачів) надсилати потенційним жертвам голосові або електронні повідомлення з проханням виконати певні деструктивні дії
10	War driving	Метод отримання несанкціонованого доступу до комп'ютерних мереж, що використовують ноутбуки. Для проникнення в мережу Інтернет застосовує антени та безпроводові мережні адаптери, що містять контрольовані локатори
11	Worm	Незалежні комп'ютерні програми, поширювані в мережі Інтернет за допомогою копіювання самих себе з одного комп'ютера в інший. На відміну від комп'ютерних вірусів, черв'яки не вимагають для свого розмноження втручання людини
12	Zero-day exploit	Спосіб запобігання кіберзахисту. Загроза реалізується того самого дня, коли громадськість дізнається про наявність у системі безпеки уразливих місць

Сніфер пакетів

Сніфер пакетів — програма, яка використовує мережний інтерфейс, функціонуючи в так званому нерозбірливому (promiscuous mode) режимі. Вона перехоплює мережний трафік, призначений для інших вузлів, та здійснює його подальший аналіз.

Щоб знизити загрозу сніфінгу пакетів, доцільно:

1) Застосовувати такі методи автентифікації, як одноразові паролі типу one-time passwords (OTP) і DTP;
2) Створити комутуючу інфраструктуру;
3) Установити антисніфери або ПЗ, яке розпізнає сніфер пакетів, наявний у певній мережі;
4) Створити систему криптографічного захисту.

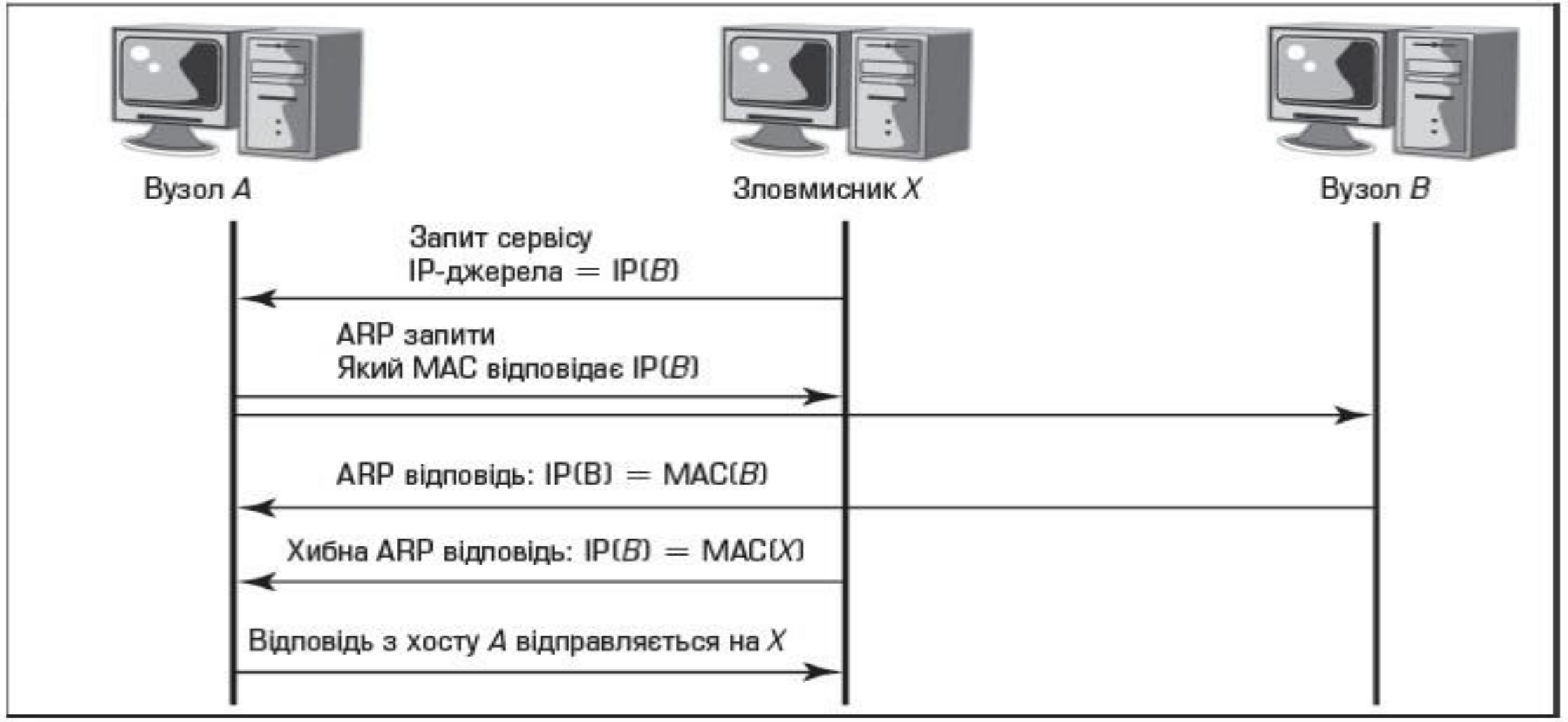
IP-спуфінг

IP-спуфінг (spoof — обман, містифікація, підроблення) — вид хакерської атаки, що передбачає використання чужої IP-адреси, тобто введення в оману системи безпеки (зловмисник, який перебуває всередині корпорації/установи або поза нею, видає себе за санкціонованого користувача).

Щоб знизити загрозу IP-спуфінгу, доцільно:

1) Правильному настроюванню управління доступом;
2) Застосуванню фільтрації;
3) Упровадженню додаткових заходів автентифікації, таких як створення системи криптографічного захисту.

IP-спуфінг


Вузол A
Зловмисник X
Вузол B
Запит сервісу
IP-джерела = IP(B)
ARP запити
Який MAC відповідає IP(B)
ARP відповідь: IP(B) = MAC(B)
Хибна ARP відповідь: IP(B) = MAC(X)
Відповідь з хосту A відправляється на X

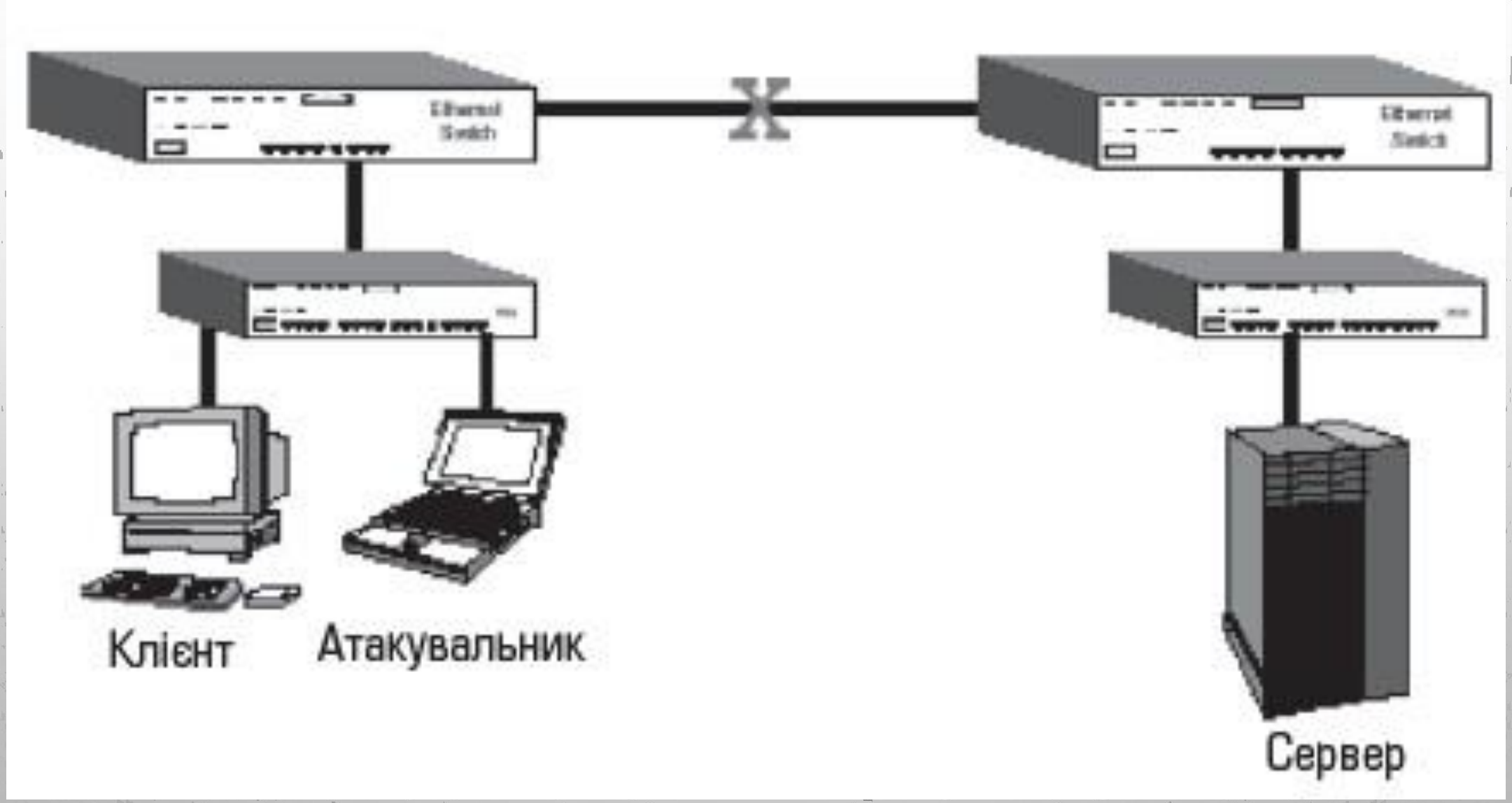
DoS-атака

Відмова в обслуговуванні (denial of service – DOS) — атака на комп'ютерну систему, що має на меті зробити комп'ютерні ресурси/мережу недоступними для користувачів через перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесора та зменшення пропускної здатності каналу зв'язку.

Щоб знизити загрозу DOS-атаки, доцільно:

1) Правильної конфігурації на маршрутизаторах і міжмережних екранах функцій та функцій, спрямованих проти dos;
2) Обмеження обсягу некритичного трафіку, який проходить мережею.

Схема DoS-атаки



DDoS-атака

Розподілена DDOS атака (distributed denial of service) — це підтип DOS атаки, здійснюваної одночасно з великої кількості IP-адрес (комп'ютерів) на систему об'єкта атаки, аби зробити мережу недоступною для звичайного використання.

Протидія DDOS атакам передбачає:

1) Профілактику причин, що спонукають тих чи інших осіб організовувати DDOS атаки;
2) Розосередження або побудову розподілених і резервних систем, які не припинять обслуговувати користувачів, навіть якщо деякі їхні елементи стануть недоступні;
3) Фільтрацію трафіку на маршрутизаторах.

Схема DDoS-атаки

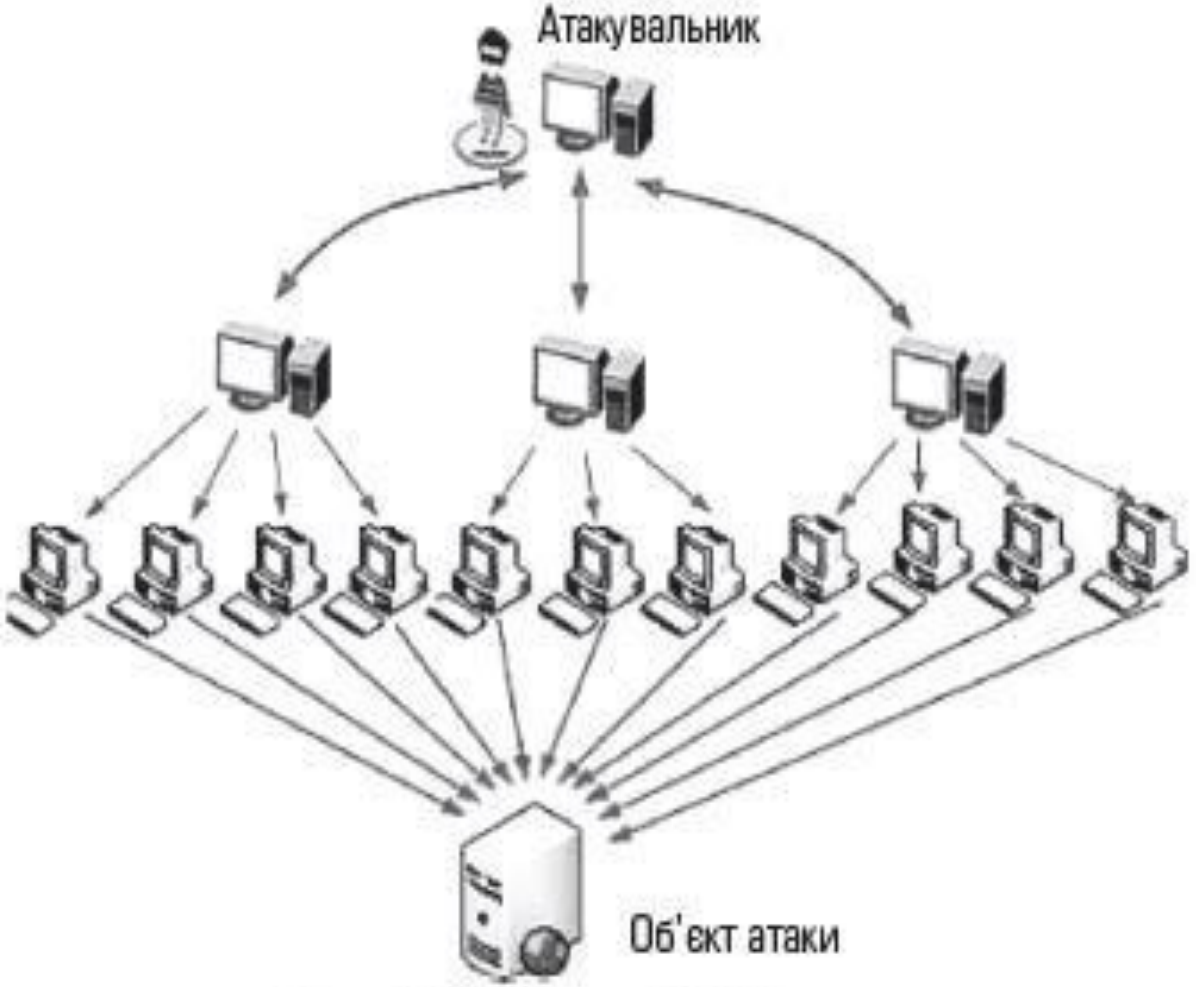


Рис. 1.24. Схема DDoS атаки

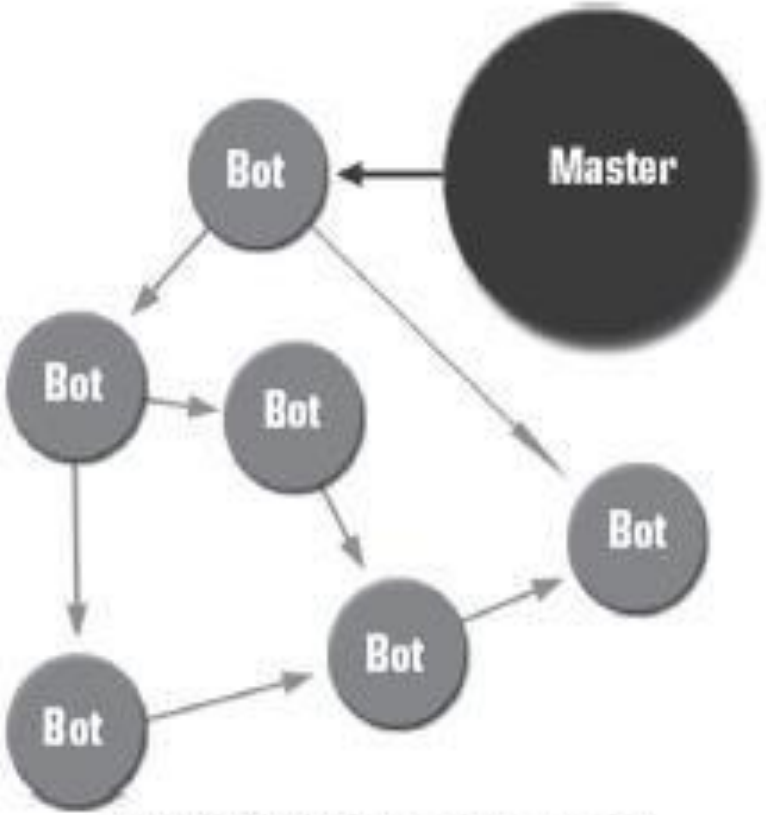
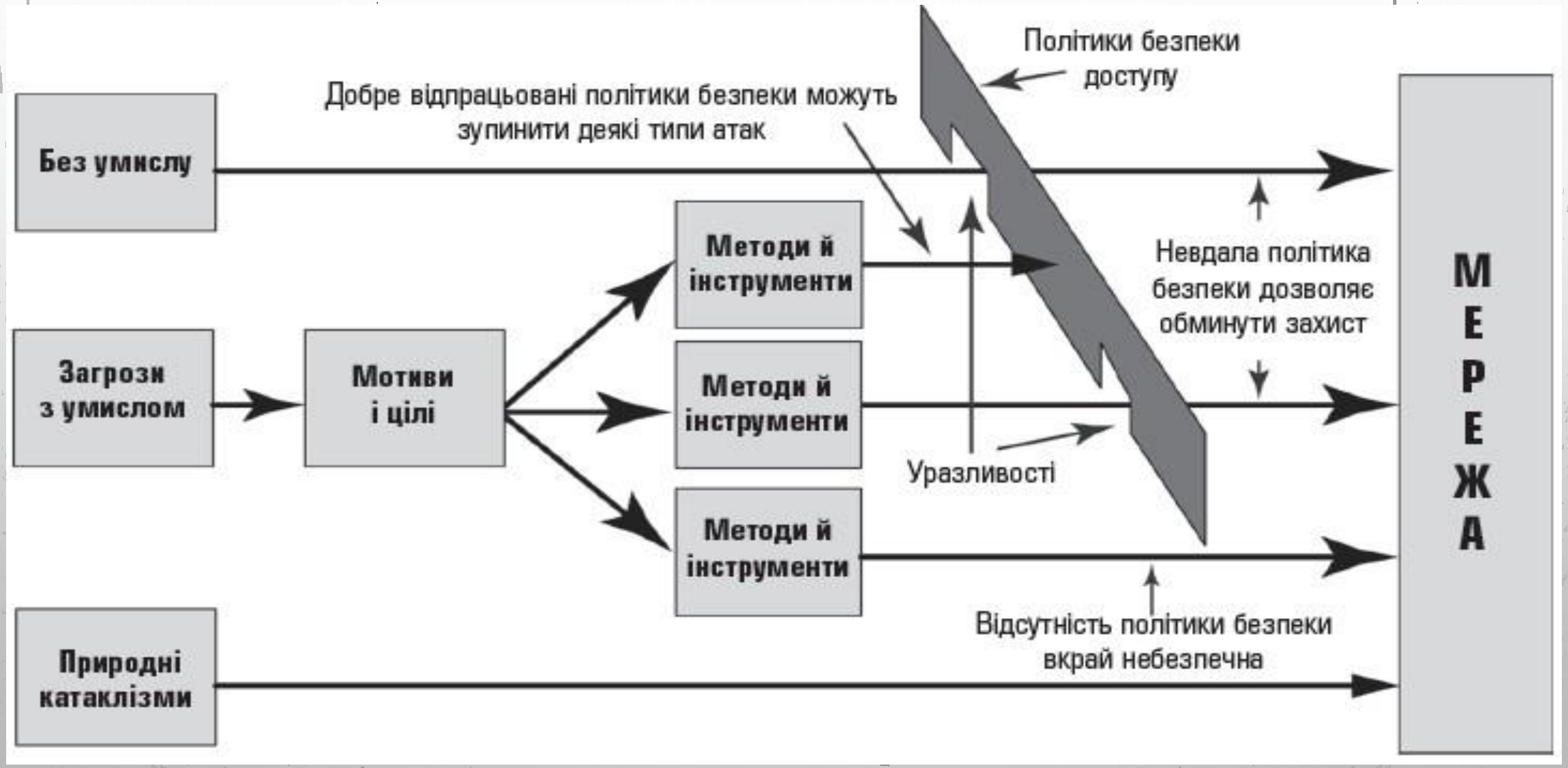


Рис. 1.25. Загальна схема організації бот-мережі

Алгоритм реалізації кібератаки



Фактори, що впливають на інформаційну безпеку

ПИТАННЯ №3

КІБЕРТЕРОРИЗМ: ПОНЯТТЯ ТА ВИЗНАЧЕННЯ. НАСЛІДКИ КІБЕРТЕРОРИЗМУ

Визначення поняття «кібертероризм»

Кібертероризм — це суспільно небезпечна діяльність, що свідомо здійснюється в кіберпросторі (або з використанням його технічних можливостей) окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на ІТС з використанням високих технологій.

Головні особливості кібертероризму

- висока ефективність кібератак;
- просторово-часова невизначеність джерела кібератаки та його віддаленість від об’єкта атаки;
- часова невідповідність між власне кібератакою та процесом її підготовки;
- можливість організації складних кібератак одночасно на різні ітс із різних напрямів тощо.

Індустрія сучасного кібертероризму

Прийоми кібертерористів

- завдання збитків окремим елементам інформаційного та кібернетичного простору;
- руйнування апаратних засобів, мереж електроживлення та елементної бази ІТС, а також наведення завад за допомогою спеціальних програм, біологічних і хімічних засобів;
- крадіжку або знищення суспільно значущих інформаційних, програмних і технічних ресурсів інформаційного та кіберпростору через подолання їхніх систем захисту, упровадження вірусів та різного роду закладок;
- вплив на програмне забезпечення та інформацію з метою спотворення або модифікації;
- розкриття із загрозою опублікування (або власне саме опублікування) закритої інформації про функціонування інформаційної інфраструктури держави, про суспільно значущі військові інформаційні системи, коди шифрування та принципи роботи шифрувальних систем;
- захоплення каналів ЗМІ з метою поширення дезінформації, чуток, демонстрації сили терористичної організації та оголошення нею своїх вимог;
- знищення або активне пригнічення ліній зв’язку, штучне перевантаження вузлів комутації;
- проведення інформаційних і психологічних операцій.

Наслідки кібертероризму

Згідно з конвенцією Ради Європи 2001 року щодо кіберзлочинів, засобами кібертероризму можуть виступати комп'ютерна система, комп'ютерні дані, послуги ТКС, а також дані трафіку.

Збиток від застосування таких засобів може знаходити таке вираження:

1) людські жертви або матеріальні втрати, викликані деструктивним використанням елементів мережної інфраструктури;

2) втрати (у тому числі й загибель людей) від несанкціонованого використання інформації з високим рівнем таємності або мережної інфраетруктури керування в життєво важливих (критичних) для держави сферах діяльності;

3) витратами на відновлення керованості мережі, спричинені діями щодо її руйнування або ушкодження;

4) моральний збиток, якого зазнав сам власник мережної інфраструктури та його інформаційний ресурс;

5) усілякі втрати від несанкціонованого використання інформації з високим рівнем таємності.

Чинники, що заважають поліпшити ситуацію в боротьбі з кіберзлочинністю

- складність організації захисту міжмережної взаємодії;
- наявність помилок у загальному та спеціальному пз, ос та утилітах, що відкрито розповсюджуються мережею;
- неправильне чи помилкове адміністрування систем;
- відсутність адекватного захисту даних у більшості із сучасних мережних протоколів;
- наявність помилок у конфігурації систем і засобів забезпечення безпеки, а іноді й повне ігнорування необхідності їх упровадження.

ДЯКУЮ ЗА УВАГУ!!!