Житомирська політехніка

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»

Лекція11

ПОЛІТИКА БЕЗПЕКИ

План

11.1. Приклади кібератак та методи протидії

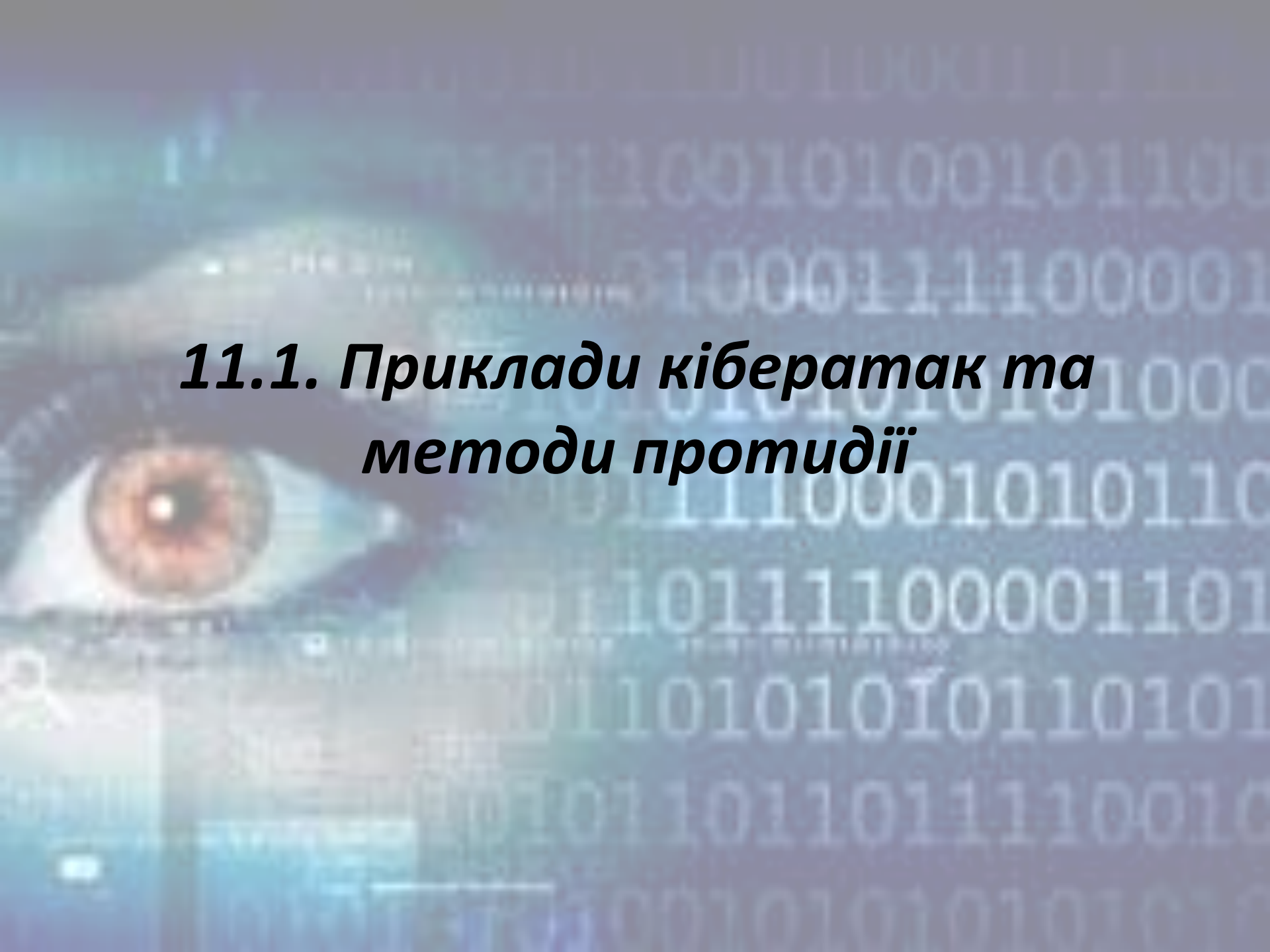
11.2.Поняття політики безпеки.

11.3. Види політик безпеки.

11.4. Організація секретного діловодства.

Література:

1. 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.— С.48-54, 75-82.
2. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – С.104-127



11.1. Приклади кібератак та методи протидії

Найпоширеніші кібератаки

№ 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

Найпоширеніші кібератаки

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

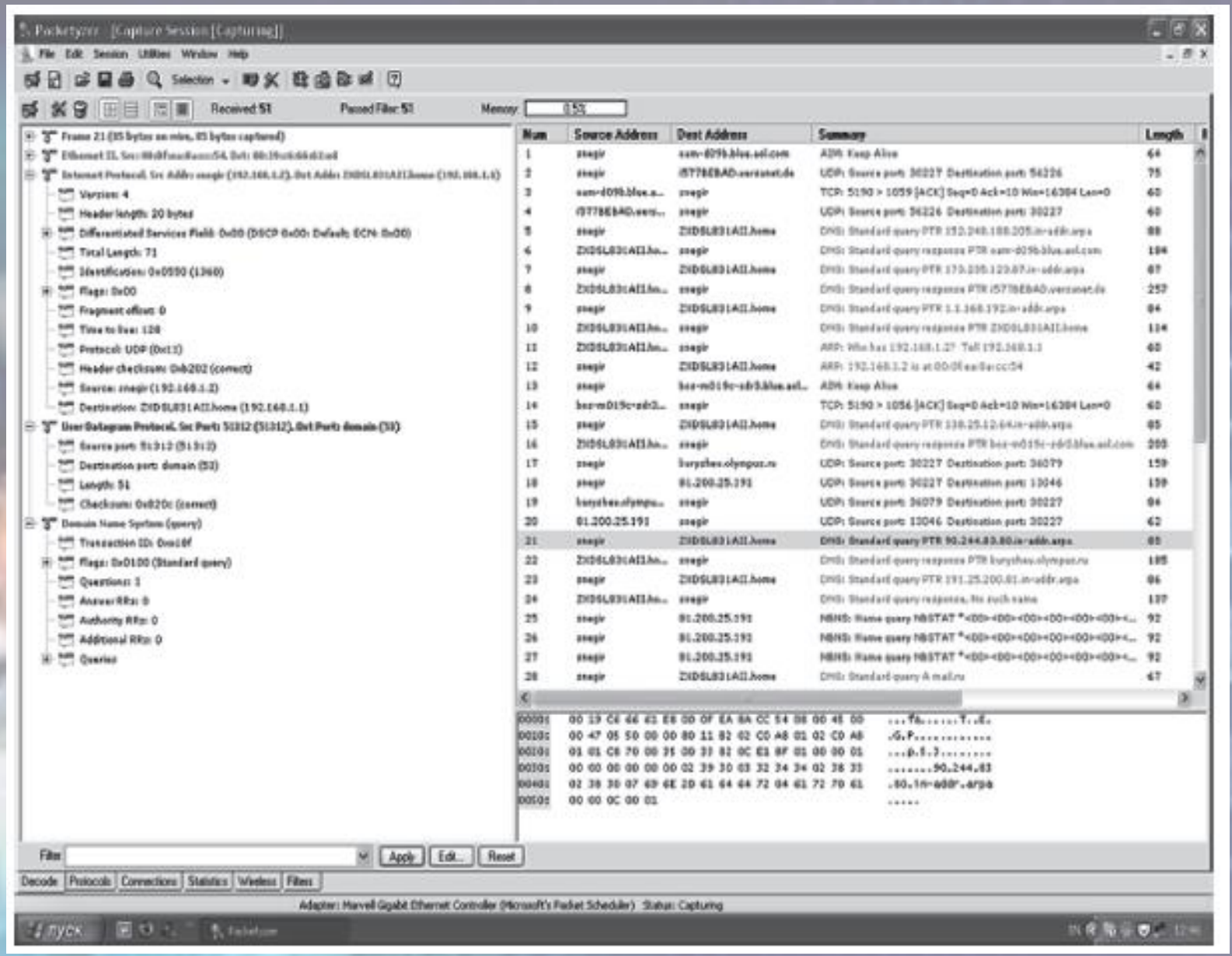


Рисунок 1 - Інтерфейс програми-сніфера Network Chemstry Packetyzer

Щоб знизити загрозу сніфінгу пакетів, доцільно:

• застосовувати такі методи автентифікації, як одноразові паролі типу One-Time Passwords (OTP) і DTP. В інших випадках, наприклад у разі перехоплення електронної пошти, зазначені методи не ефективні;

• створити комутуючу інфраструктуру (у разі використання комутуючого Ethernet-протоколу це дозволить хакерам отримати доступ лише до трафіку, що надходить на порт, до якого вони під'єднані);

• установити антисніфери або ПЗ, яке розпізнає сніфер пакетів, наявний у певній мережі (антисніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік);

• створити систему криптографічного захисту. Це найбільш ефективний спосіб боротьби зі сніфером пакетів. Якщо канал зв'язку має криптографічний захист, то хакер перехоплює не повідомлення, а зашифрований текст (тобто незрозумілу послідовність бітів).

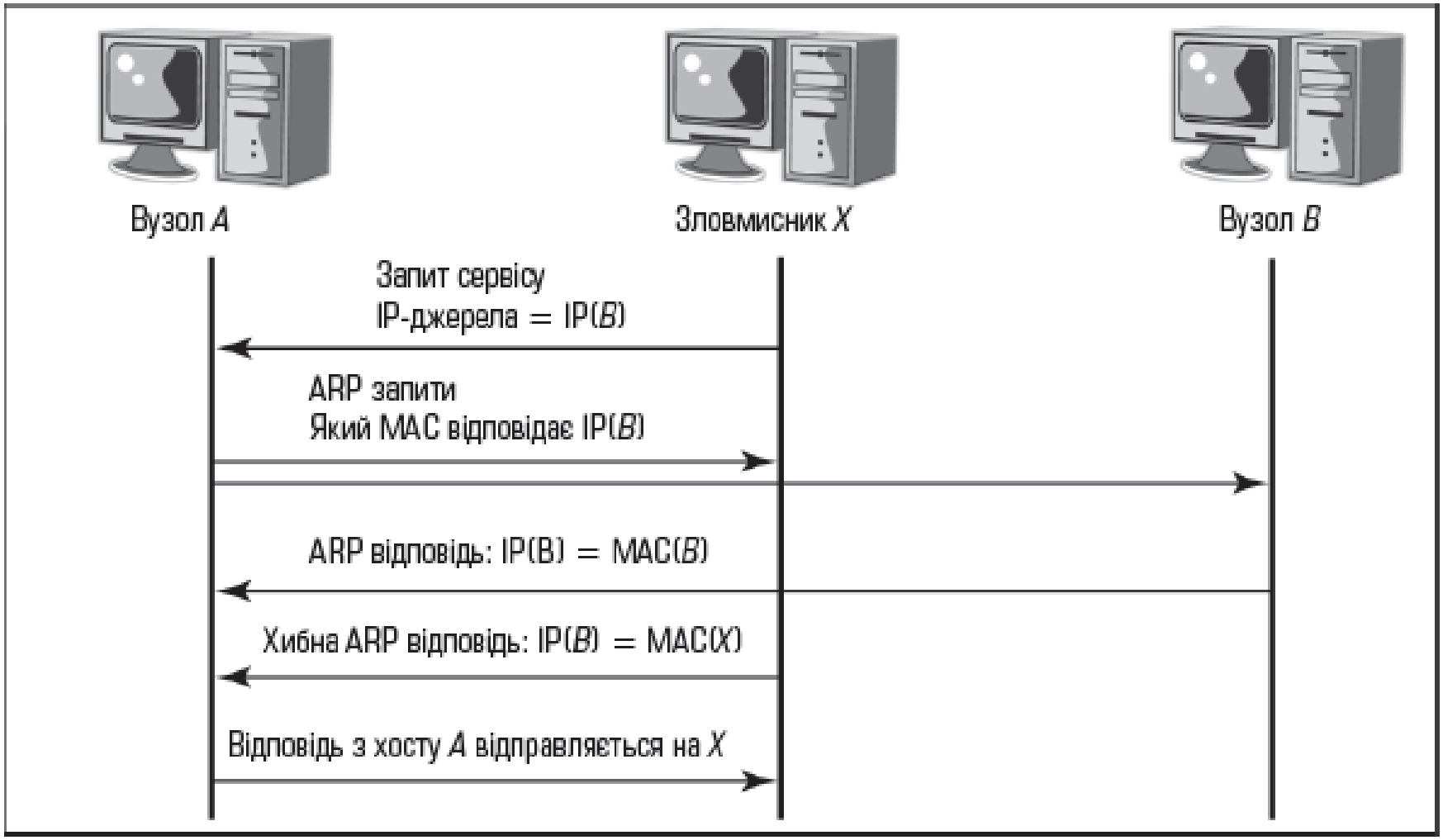


Рисунок 2 – Застосування IP-спуфінгу для отримання несанкціонованого доступу до ресурсів

Послабити загрозу IP-спуфінгу, а кібератаку перетворити на абсолютно неефективну можна завдяки:

- правильному настроюванню управління доступом (із забороною будь-якого трафіку, що надходить із зовнішньої мережі з вихідною адресою, яка має перебувати всередині власної мережі);
- застосуванню фільтрації RFC 2827 (із забороною будь-якого трафіку, вихідна адреса якого не є однією з IP-адрес певної установи);
- упровадженню додаткових заходів автентифікації, таких як створення системи криптографічного захисту.

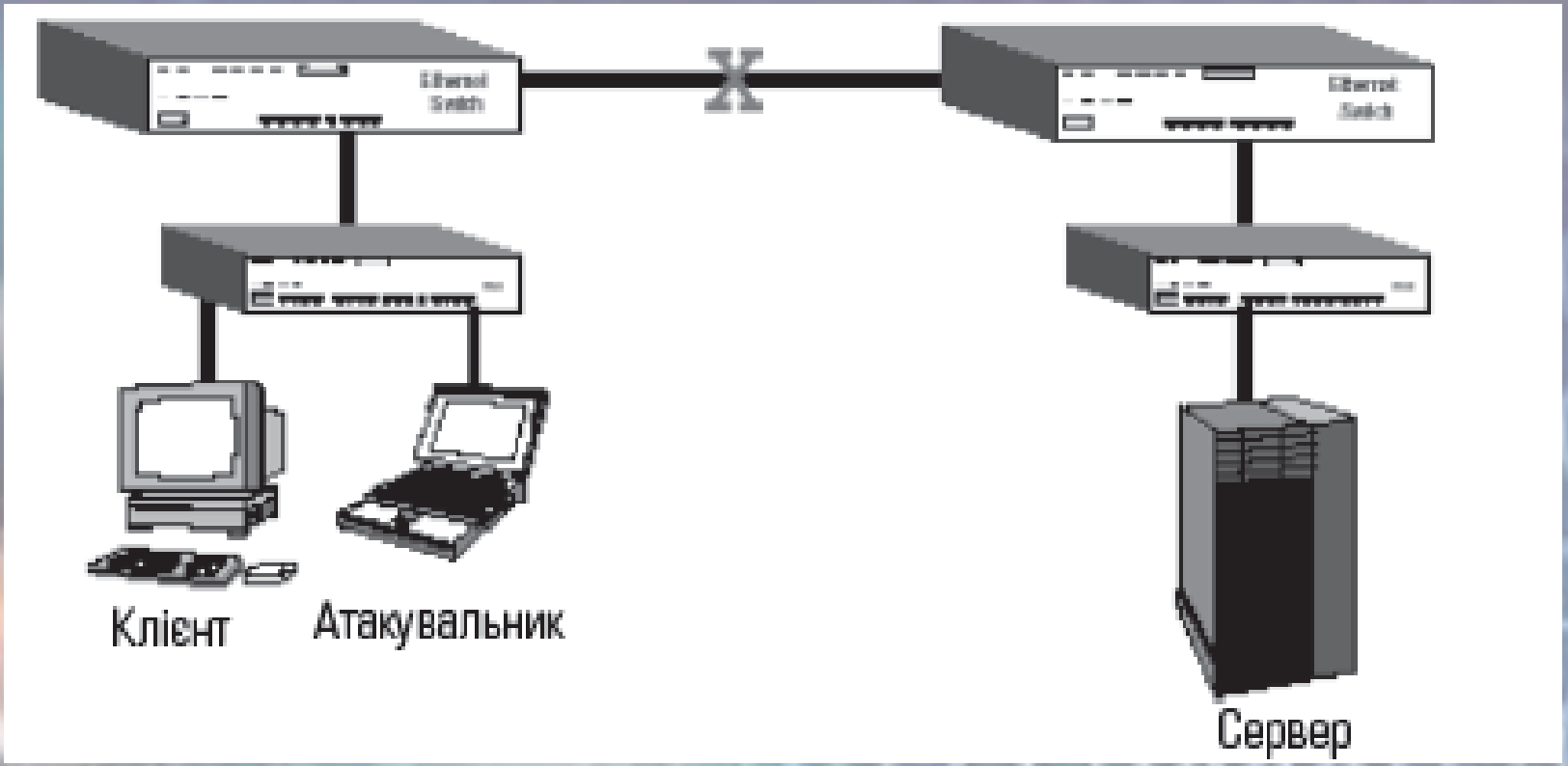


Рисунок 3 - Схема DoS атаки

До найвідоміших різновидів DoS атак належать такі: *Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco,Stacheldracht, Trinity.*

Загрозу DoS атак можна послабити за допомогою:

• правильної конфігурації на маршрутизаторах і міжмережних екранах функцій антиспуфінгу (упровадження фільтрації RFC 2827) та функцій, спрямованих проти DoS;
• обмеження обсягу некритичного трафіку (***non-critical traffic*** - визначає ймовірність того, що мережа зв'язку відповідає заданому та узгодженому трафіку), який проходить мережею. Типовим прикладом є обмеження обсягів трафіку ICMP, що використовується тільки з діагностичною метою.

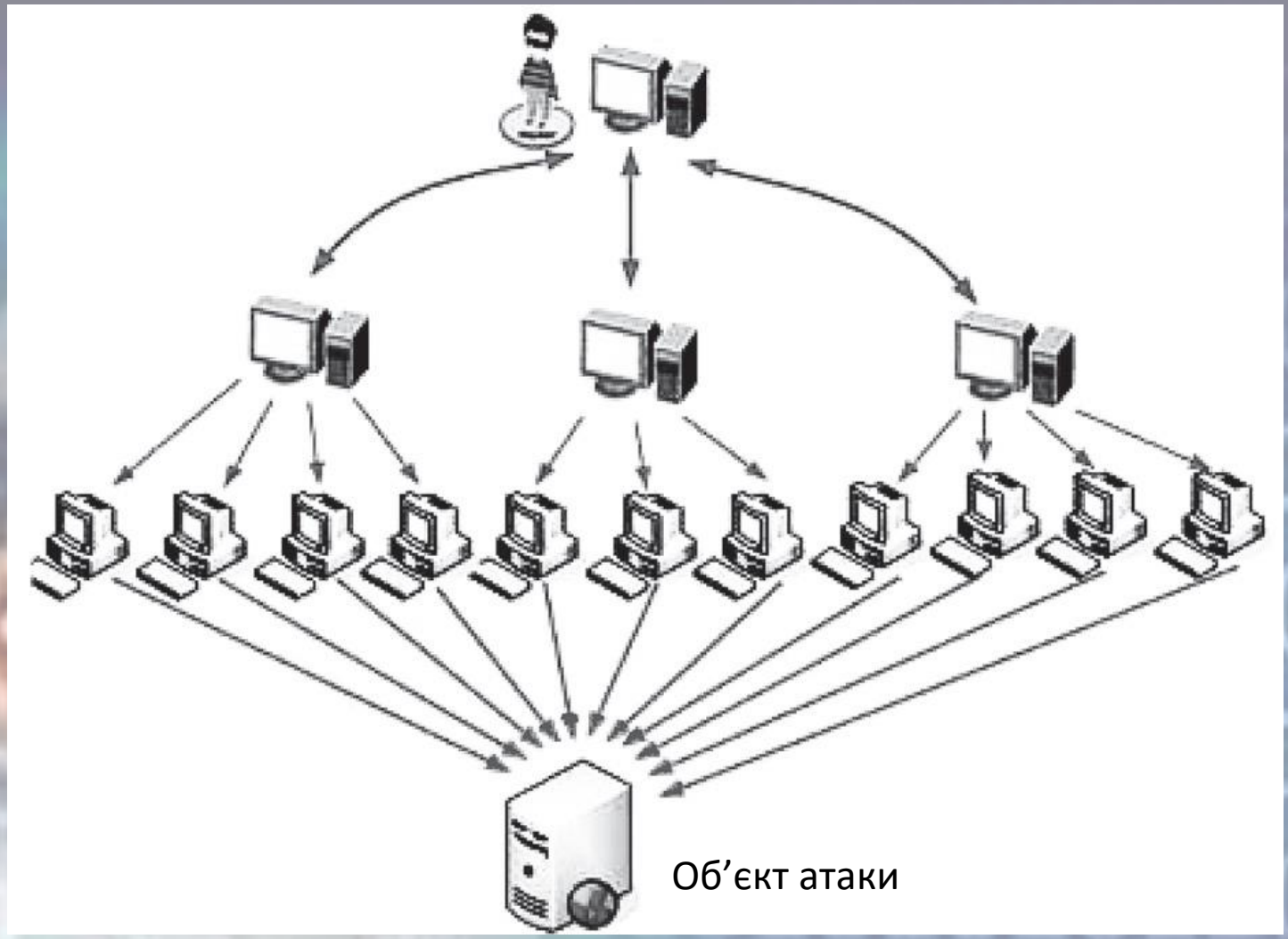


Рисунок 4 - Схема DDoS атаки

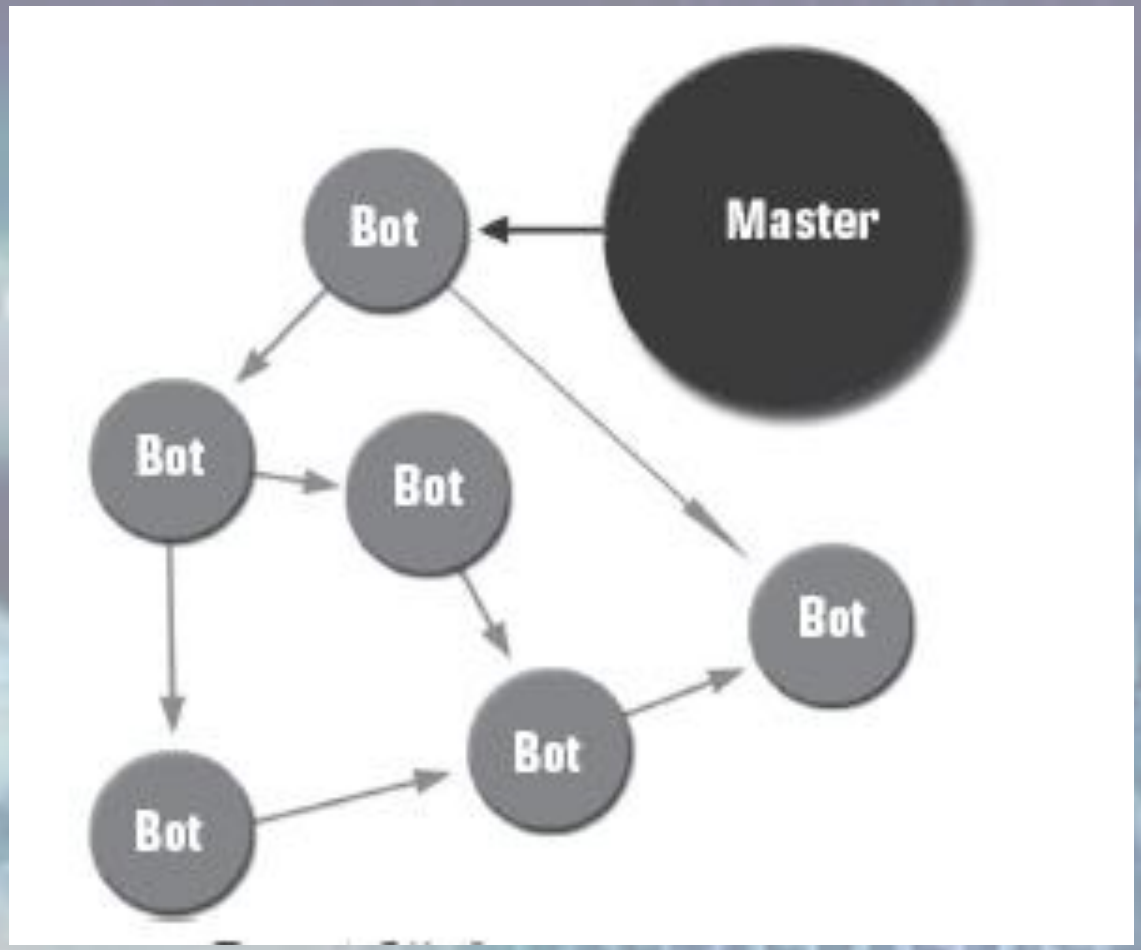


Рисунок 5 - Загальна схема організації бот-мережі

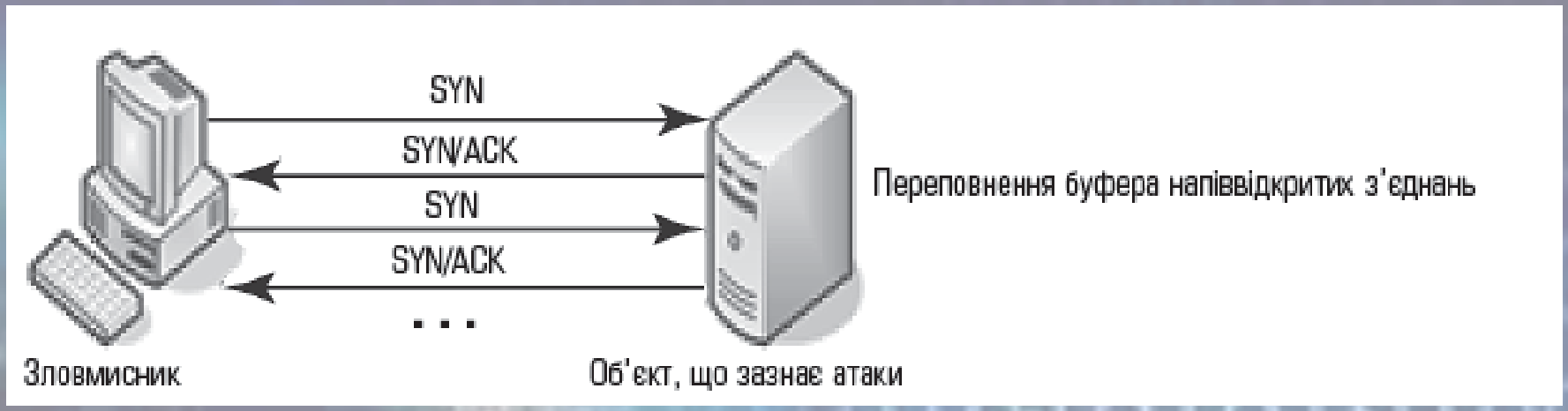


Рисунок 6 -TCP SYN flood атаки

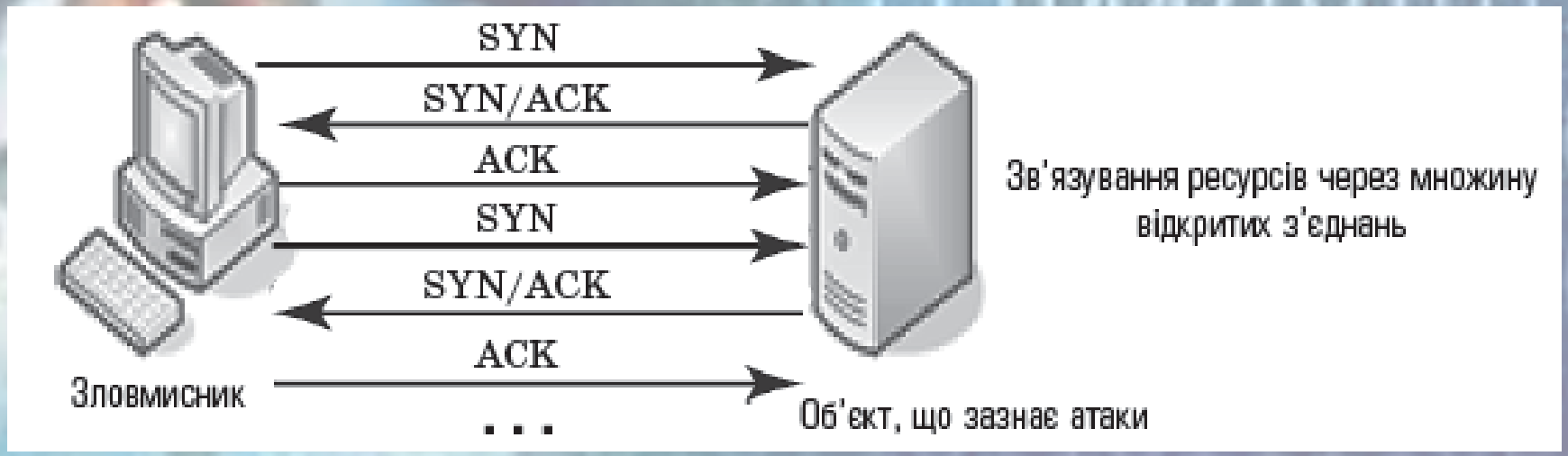


Рисунок 7 -TCP flood атака

Протидія DDoS атакам передбачає:

• профілактику причин, що спонукають тих чи інших осіб організовувати DDoS атаки. Дуже часто атаки здійснюються внаслідок особистої образи або політичних, релігійних розбіжностей;

• розосередження або побудову розподілених і резервних систем, які не припинять обслуговувати користувачів, навіть якщо деякі їхні елементи стануть недоступні;

• фільтрацію трафіку на маршрутизаторах (міжмережні екрани та спеціалізовані antiflood засоби фільтрації - найбільш ефективний, але й найбільш дорогий метод. Їх установлюють якнайближче до джерела flood. Наприклад, програмний засіб ADoS, який є динамічним фільтром TCP-пакетів, здатний блокувати в реальному часі доступ до web-сервера з IP-адрес, що генерують інтенсивний потік HTTP-запитів);

• розміщення (розташування) безпосередньої цілі атаки - доменного імені або IP-адреси подалі від інших ресурсів, які часто зазначають впливу разом із безпосередньою ціллю;

• нарощування ресурсів системи (якщо flood спрямований на вичерпання ресурсів, то найпримітивнішим способом протидії цьому є нарощування власних ресурсів, щоб протиборча сторона не змогла їх вичерпати).

Рисунок 9 - Фактори, що впливають на інформаційну безпеку

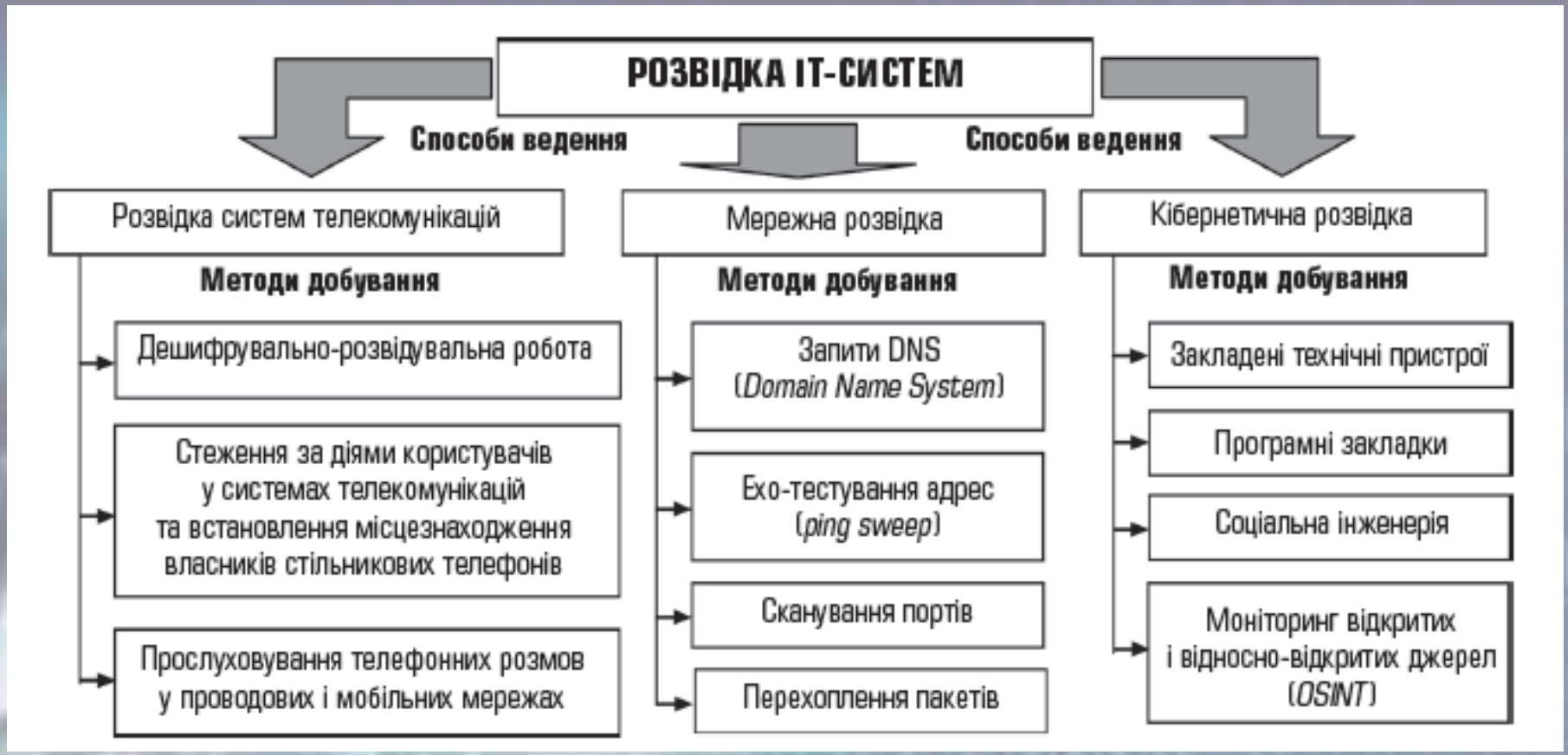


Рисунок 10 -Способи та методи ведення розвідки ІТ-систем

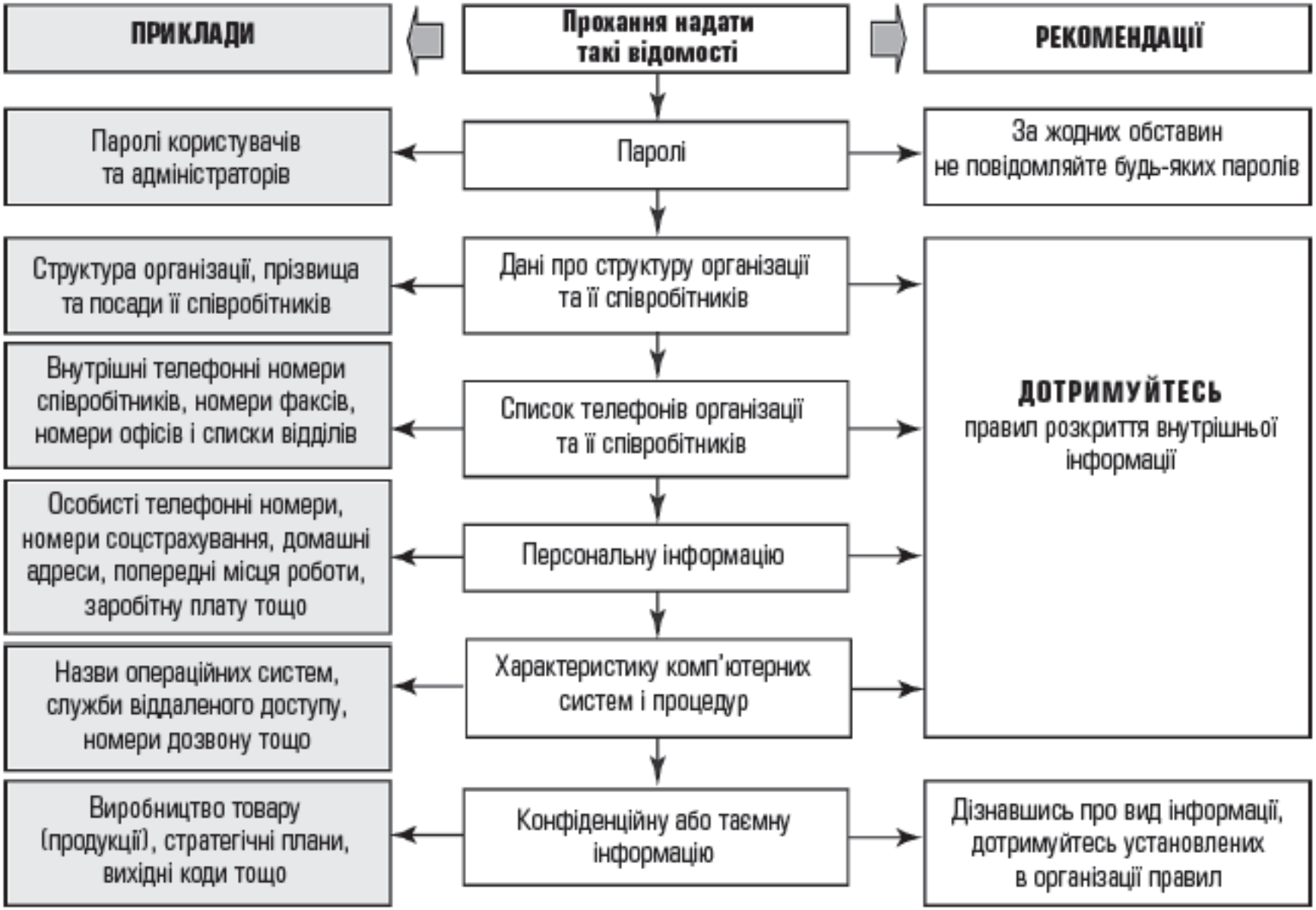


Рисунок 11 - Рекомендація щодо розкриття атаки, спрямованої на отримання інформації

Основні методи і засоби несанкціонованого отримання інформації та її захисту

Типова ситуація	Канал витоку інформації	Методи і засоби	
		отримання інформації	захисту інформації
Розмова в приміщенні та на вулиці	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
	Віброакустичний	Стетоскоп, вібродатчик	
	Акустоелектронний	Спеціальні радіоприймачі	
Розмова по телефону:	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
– проводовому	Сигнал у лінії	Паралельний телефон, пряме підімкнення, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
– радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка

Основні методи і засоби несанкціонованого отримання інформації та її захисту

Дії з документом на паперовому носії:	Безпосередньо сам документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
	Продавлення стрічки або паперу	Крадіжка, прочитування	Оргтехзаходи
– виготовлення	Акустичний шум принтера	Апаратура акустичного контролю	Пристрої шумозаглушування
	Паразитні сигнали, наведення	Спеціальні радіотехнічні засоби	Екранування
– поштове відправлення	Безпосередньо сам документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії:	Носій	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
– виготовлення	Відображення на дисплеї	Візуальний, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричні та оптичні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
– передавання документа по каналах зв'язку	Електричні та оптичні сигнали	Несанкціоноване підімкнення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

11.2. Поняття політики безпеки

Фундаментальним поняттям захисту інформації є політика безпеки (ПБ), або політика захисту.

З ПБ пов’язується поняття оптимальності рішень з організації та підтримки системи захисту.

Система захисту не самоціль, а має лише підпорядковане значення і має виконувати підпорядковану функцію порівняно з головною метою обчислювального процесу

Приклад 1.

Нехай два відділи в деякій організації ведуть розробки двох проблем. Кожний з відділів користується своїми базами даних, у тому числі і для збору інформації про вирішення проблем. Припустимо, що серед множин задач першого і другого відділів виявилися однакові задачі. На жаль, звичайний офіцер служби безпеки, що дозволяє чи забороняє доступ до баз, не в змозі встановити, що в двох базах накопичується інформація з вирішення одного і того ж завдання. Розглянемо різні рішення офіцера щодо забезпечення безпеки інформації.

1. Якщо він дозволить доступ відділів до баз один одного, то співробітники одного з них, взявши інформацію з іншої бази чи зі своєї, анонімно, і тому безкарно, зможуть продати інформацію, тому що немає персональної відповідальності (неможливо встановити, хто саме продав інформацію з даної бази). При цьому безкарність іноді може навіть стимулювати злочин.

2. Якщо він не дозволить доступ відділів до баз один одного, то виникає небезпека збитків через недоступність інформації (одні вирішили завдання, а інші – ні; тоді завдання іншого відділу виявиться невирішеним, через що можливі великі збитки для фірми, тому що відповідну проблему могли вирішити конкуренти).

Очевидно, що в обох випадках досягається зменшення однієї небезпеки за рахунок зростання іншої.

Приклад 2.

Нехай у БД збирається інформація про здоров’я приватних осіб, яка у більшості країн вважається конфіденційною. БД потрібна, тому що ця інформація дозволяє ефективно робити діагностику. Якщо доступ до цієї бази з точки зору захисту інформації сильно обмежений, то в такій БД не буде користі для лікарів, які ставлять діагнози, і не буде користі від самої бази. Якщо доступ відкрити, то можливий витік конфіденційної інформації, за який через суд може бути поданий позов. Яким має бути оптимальне рішення?

Рішення

- Результатом рішення в наведених прикладах та інших аналогічних задачах є вибір правил розподілу і збереження інформації, а також поводження з інформацією, що й називається політикою безпеки.

Під поняттям *ПБ інформації* розуміється організована сукупність документованих керівних рішень, спрямованих на захист інформації й асоційованих з нею ресурсів системи. ПБ викладає систему поглядів, основних принципів, практичних рекомендацій і вимог, що закладаються в основу реалізованого в системі комплексу заходів із захисту інформації.

Дотримання ПБ має забезпечити виконання того компромісу між альтернативами, який вибрали власники цінної інформації для її захисту. Вочевидь, будучи результатом компромісу, ПБ ніколи не задовольнить усі сторони, що беруть участь у взаємодії з інформацією, що захищається. У той же час вибір ПБ це кінцеве вирішення проблеми: що добре і що погано при роботі з цінною інформацією. Після прийняття такого рішення можна будувати захист, тобто систему підтримки виконання правил ПБ. Таким чином, побудована система захисту інформації добра, якщо вона надійно підтримує виконання правил ПБ. Навпаки, система захисту інформації погана, якщо вона ненадійно підтримує ПБ.

Приклад 3.

Сформулюємо просту політику безпеки в деякій установі. Ціль, що стоїть перед захистом – забезпечення таємності інформації. ПБ полягає в наступному: кожен користувач користується своїми і тільки своїми даними, не обмінюючись з іншими користувачами. Легко побудувати систему, що підтримує цю політику. Кожен користувач має свій персональний комп’ютер у персональній кімнаті, куди не допускаються сторонні особи. Легко бачити, що сформульована вище політика реалізується в цій системі. Будемо називати таку політику тривіальною розмежувальною (дискреційною) політикою.

ПБ визначається неоднозначно і, звичайно, завжди пов’язана з практичною реалізацією системи і механізмів захисту. Наприклад, ПБ у прикладі 3 може цілком змінитися, якщо в організації немає достатнього числа комп’ютерів і приміщень для підтримки цієї політики. Побудова ПБ звичайно відповідає таким крокам:

- 1 крок. В інформацію вноситься структура цінностей і проводиться аналіз ризику.
- 2 крок. Визначаються правила для будь-якого процесу користування даним видом доступу до елементів інформації, що має дану оцінку цінностей.

Однак реалізація цих кроків є складним завданням. Результатом помилкового чи бездумного визначення правил ПБ, як правило, є руйнування цінності інформації без порушення політики. Таким чином, навіть добра система захисту може бути «прозорою» для зловмисника при поганій ПБ.

Приклад 4.

Нехай банківські рахунки зберігаються в зашифрованому вигляді у файлах ПК. Для шифрування, природно, використовується блокова система шифру, що для надійності реалізована поза комп'ютером і оперується за допомогою довіреної особи. Провівши аналітику механізмів захисту, служба безпеки банку переконана адміністрацію, що якщо шифр стійкий, то зазначеним способом інформація добре захищена. Справді, прочитати її при надійному шифрі неможливо, але службовець банку, що знає стандарти заповнення рахунків і має доступ до комп'ютера, може замінити частину шифротексту у своєму рахунку на шифротекст у рахунку багатого клієнта.

Якщо формати збіглися, то рахунок такого службовця з великою ймовірністю зросте. У цьому прикладі акцентується увага на те, що в такій ситуації небезпека для цілісності інформації є значно вищою від небезпеки для порушення таємності, а обрана ПБ добре захищає від порушень таємності, але не орієнтована на небезпеку для цілісності.

Приклад 5.

Якщо невдало вибрати ПБ, то можна показати, як користувач, що не має доступу до секретної інформації, реалізує канал витоку секретних даних про те, де в пустелі знаходиться колодязь з водою (нехай, для простоти, у розглянутій місцевості є тільки один колодязь). Отже, інформація про карту будь-якої ділянки пустелі є загальновідомою, але координати колодязя є секретною інформацією. Для одержання секретної інформації користувач робить послідовність запитів у базу даних, причому кожен наступний запит (можна говорити про кроки алгоритму користувача) визначається відповіддю на попередній.

- І крок. Розбивається район (для зручності – прямокутник) на вертикальні смути і робиться запит на ці ділянки в базу даних. Відповідно до вибраної ПБ відповідь подається у двох формах:
  - відмова від показу карти, якщо вона секретна, оскільки користувачеві, що не має допуску до секретної інформації, база даних, природно, не повинна її показувати;
  - представлення карти на екрані, якщо ділянка не містить колодязя. Якщо є відмова в доступі, то висновок – в даній смузі є колодязь.

2 крок. Смуга, де є колодязь (тобто де є відмова в доступі), розбивається на окремі ділянки по горизонталі, і знову робиться запит у базу даних. Відмова знову означає, що в даній ділянці є колодязь.

У результаті обчислюються координати колодязя, причому це можна зробити з будь-якою заданою точністю (залежно від рівня дискретизації ділянок пустелі). Таким чином, ПБ дотримана, однак відбувся витік секретної інформації.

Зрозуміло, що ПБ можна відкоригувати таким чином: нехай будь-який користувач одержує карту за запитом, але користувач з допуском до секретної інформації одержує карту з нанесеним колодязем, а користувач без такого доступу – без колодязя. У цьому випадку канал, побудований вище, не працює і ПБ надійно захищає інформацію.

Під *ПБ інформації* слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін «політика безпеки» може бути застосований щодо організації, ІС, АСУ, ОС, послуги, що реалізується системою (набору функцій) тощо. Чим дрібніший об’єкт, до якого застосовується даний термін, тим конкретнішими і формальнішими стають правила. Далі для скорочення замість словосполучення «політика безпеки інформації» може використовуватись словосполучення «політика безпеки», а замість словосполучення «політика безпеки інформації, що реалізується послугою» – «політика послуги» тощо.

Для визначення і формалізації процесу розробки ПБ в деякій організації звичайно необхідно розробляти два комплекти документів:

1. Узагальнена політика (program-level).
2. Проблемно-орієнтована (окрема) політика (issue-specific).

Основна функція *узагальненої ПБ* є визначення програми ЗІ, призначення відповідальних за її виконання осіб, формулювання цілей і об'єктів захисту, а також вироблення схеми для забезпечення додержання розроблених правил і вказівок. Компонентами узагальненої ПБ вважаються призначення, сфера поширення, визначення цілей ЗІ, розподіл відповідальності за виконання і методи забезпечення додержання правил.

Проблемно-орієнтована ПБ необхідна для виділення певних проблемних сфер і визначення позицій організації щодо них.

Якщо узагальнена ПБ описує глобальні аспекти ЗІ і її схему, то окремі ПБ розробляються для деяких видів діяльності й у деяких випадках для конкретних систем (наприклад, для захисту електронної кореспонденції).

Основними етапами формального підходу до перевірки СЗІ на повноту і коректність є:

1) визначення об’єктів і цілей захисту;
2) розробка політики,
3) доведення того, що при її додержанні інформація не компрометується
4) визначення набору функцій для підтримки політики;
5) доведення того, що набір функцій забезпечує додержання політики;
6) вибір апаратного і програмного забезпечення для реалізації функцій ЗІ.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

- неможливість минати захисні засоби;
- посилення самої слабкої ланки;
- неприпустимість переходу у відкритий стан;
- мінімізація привілеїв;
- поділ обов’язків;
- багаторівневий захист;
- розмаїтість захисних засобів;
- простота і керованість інформаційної системи;
- забезпечення загальної підтримки заходів безпеки.

11.2. Види політик безпеки

Серед ПБ найбільш відомі **дискреційна**, **мандатна і рольова**. Основою *дискреційної політики безпеки (ДПБ)* є дискреційне управління доступом, яке визначається двома властивостями:

- всі суб’єкти і об’єкти повинні бути однозначно ідентифіковані;
- права доступу суб’єкта до об’єкта системи визначаються на основі деякого зовнішнього відносно системи правила.

ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об’єктів та суб’єктів, доступних кожному суб’єкту. Існує декілька варіантів задавання матриці доступу.

1. *Листи можливостей*: для кожного суб’єкта створюється лист (файл) усіх об’єктів, до яких він має доступ;
2. *Листи контролю доступу*: для кожного об’єкта створюється список усіх суб’єктів, що мають доступи до нього.

До переваг ДПБ можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлений той факт, що більшість поширених сьогодні захищених АСУ забезпечують виконання положень ДПБ.

Вади ДПБ:

1. Один із найсуттєвіших недоліків цього класу політик тс, що вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що СЗІ, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему й інших засобів прихованої руйнівної дії.

2. Наступна проблема ДПБ – це автоматичне визначення прав. Так як об’єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб’єкта на доступ до об’єктів неможливо. Тому матриця доступу різними способами агрегується.

- Наприклад, як суб’єкти залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб’єкта, породженого користувачем, до об’єкта. Звичайно, ці функції можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання деякої події. Можливі модифікації, які залежать від інших параметрів.

3. Ще одна з найважливіших проблем при використанні ДПБ – це проблема контролю поширення прав доступу. Найчастіше буває, що власник файлу передає вміст файлу іншому користувачеві і той, таким чином, набуває права власника на цю інформацію. Отже, права можуть поширюватися, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після декількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі деякий суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АСУ. У загальному випадку при використанні ДІІЬ перед органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується деяким набором правил, стоїть задача, яку алгоритмічно розв'язати неможливо; перевірити, призведуть його дії до порушень безпеки чи ні.

Основу *мандатної (повноважної)* політики безпеки (МПБ) становить мандатне управління доступом , що передбачає:

- всі суб’єкти і об’єкти повинні бути однозначно ідентифіковані;
- задано лінійно упорядкований набір міток секретності;
- кожному об’єкту системи присвоєна мітка секретності, яка визначає цінність інформації, що міститься в ньому – його рівень секретності в АС;
- кожному суб’єкту системи присвоєна мітка секретності, яка визначає рівень довіри до нього в АСУ – максимальне значення мітки секретності об’єктів, до яких, суб’єкт має доступ; мітка секретності суб’єкта називається його рівнем доступу.

Основна мета МПБ – запобігання витоку інформації від об’єктів з високим рівнем доступу до об’єктів з низьким рівнем доступу, тобто протидія виникненню в АСУ інформаційних каналів зверху вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності (певним значенням мітки секретності) інформаційних об’єктів.

Однак досвід показує, що в будь-якій АСУ майже завжди для будь-якої пари об’єктів *X* та *Y* можна сказати, який із них більш цінний. Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція *c(X)*, яка дозволяє для будь-яких об’єктів *X* та *Y* сказати, що коли *Y* більш цінний об’єкт, ніж *X*, то $c(Y) > c(X)$. І навпаки, з огляду на однозначність, якщо $c(X) > c(Y)$, то *Y* – більш цінний об’єкт, ніж *X*. Тоді потік інформації від *X* до *Y* дозволяється, якщо $c(X) < c(Y)$, і не дозволяється, якщо $c(X) > c(Y)$.
Таким чином, МПБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені дуже простою умовою значенням наведеної функції. Інакше кажучи, управління потоками інформації здійснюється через контроль доступів.

Наведемо ряд переваг МПБ порівняно з ДПБ.

1. Для систем, де реалізовано МПБ, характерним є більш високий ступінь надійності. Це пов’язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб’єктів системи до об’єктів, а й стан самої АСУ. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника.
2. Правила МПБ більш ясні і прості для розуміння розробниками і користувачами АСУ, що також є фактором, який позитивно впливає на рівень безпеки системи.
3. МПБ стійка до атак типу «Троянський кінь».
4. МПБ допускає можливість точного математичного доведення, що дана система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади – вона складна для практичної реалізації і вимагає значних ресурсів обчислювальної системи. Це пов’язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Саме ці вади часто заважають її практичному використанню.

Рольова ПБ.

Рольову політику безпеки не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель є цілком новим типом політики, що базується на компромісі між гнучкістю керування доступом, яка є характерною для ДПБ, і жорсткістю правил контролю доступу, яка притаманна МПБ.

У РПБ класичне поняття *суб'єкт* замішується поняттями користувач і роль. *Користувач* – це людина, яка працює з системою і виконує певні службові обов'язки. *Роль* – це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ є досить поширеною, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя. Справді, користувачі, що працюють у системі, діють не від свого власного імені – вони завжди здійснюють певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю.

Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладною інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків. Наприклад, у реальній системі обробки інформації можуть працювати системний адміністратор, менеджер БД і користувач.

У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією; роль менеджера баз даних дає змогу здійснювати керування сервером БД; а права простих користувачів обмежуються мінімумом, необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів – один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватись однією і тією ж роллю, якщо вони виконують однакову роботу.

11.4. Організація секретного діловодства

При роботі з документами, що містять конфіденційну інформацію, слід дотримуватися наступних правил:

- строгий контроль (чи особисто через службу безпеки) за допуском персоналу до секретних документів;
- встановлення конкретних осіб з керівництва фірми, що організують і контролюють секретне діловодство фірми; наділення їх відповідними повноваженнями;
- розробка інструкції (пам’ятки) по роботі із секретними документами, ознайомлення з нею відповідних працівників фірми;
- контроль за прийняттям відповідними службовцями письмових зобов’язань про збереження комерційної таємниці фірми;
- уведення системи матеріального й іншого стимулювання працівникам фірми, що мають доступ до її секретів;
- впровадження в повсякденну практику механізмів і технологій захисту комерційної таємниці фірми;
- особистий контроль з боку керівника фірми служби внутрішньої безпеки і секретного діловодства.

Імовірність витоку секретної інформації з документів особливо велика в процесі їх пересилання. Очевидно, що в комерційних структур немає можливостей скористатися послугами воєнізованої кур'єрської доставки. Тому доставку секретних документів і цінностей приходиться здійснювати власними силами із залученням охоронців фірми чи звертатися в спеціальні фірми.

Фірми, відповідальні за схоронність, використання і своєчасне знищення секретних документів, повинні бути захищені від спокуси торгівлі секретами фірми простим, але радикальним способом – гарною платою за роботу.

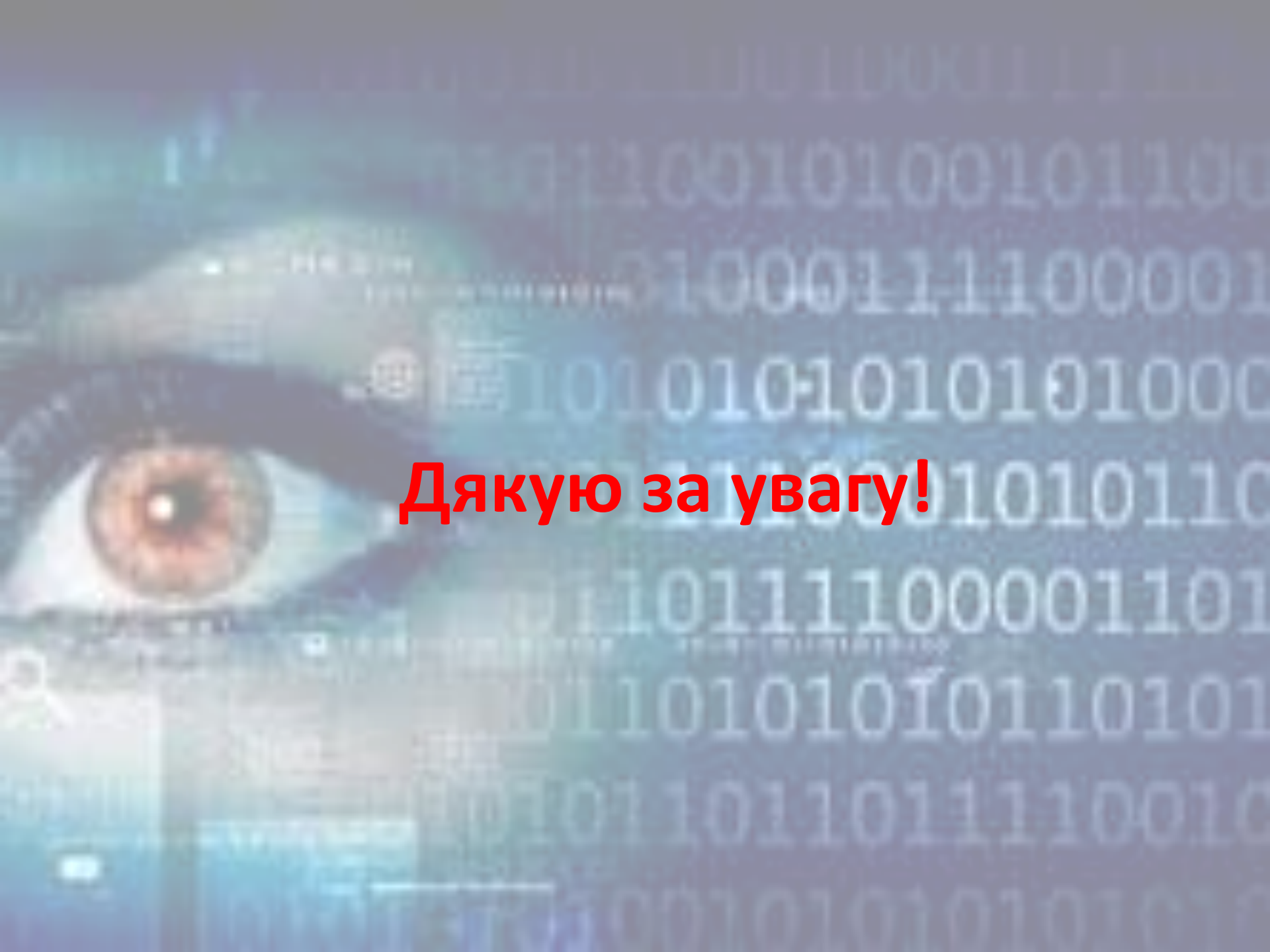
У процесі збереження і пересилання секретних документів фірми можуть бути застосовані засоби захисту і сигналізації про несанкціонований доступ до них. Одна з новинок – невидиме світлочутливе покриття, наносимо на документи, що виявляється під впливом світла, указуючи тим самим на факт несанкціонованого ознайомлення з чи документами їхнього фотографування.

Приміщення, у яких ведеться робота із секретними документами, повинні добре охоронятися, а доступ туди повинен бути закритий для сторонніх облич. Ці приміщення повинні мати міцні перекриття і стіни, посилені металеві двері, міцні віконні рами з подвійним склом і ґратами, щільні штори. Сховище повинне бути обладнане охоронною і пожежною сигналізацією і ретельно охоронятися силами внутрішньої охорони. Доступ у сховище строго обмежений. Не рекомендується розташовувати таке приміщення на першому й останньому поверхах будинку. Секретні документи зберігаються у сейфах або вогнестійких металевих шафах з надійними замками і запорами.

Різні прийоми ведення секретного діловодства спрямовані на запобігання витоку комерційних секретів. Наприклад, документи, що містять комерційну таємницю, діляться по ступеню таємності відображеної в них інформації і забезпечуються відповідним грифом таємності.

Навіть та таємниці фірми, що ретельно охороняються можуть стати надбанням конкурентів зі звичайних публікацій, якщо пустити цю справу на самоплив. Тому один зі службовців фірми обов’язково повинен бути наділений самими широкими владними повноваженнями, щоб займатися попередньою цензурою брошур, що готуються, рекламних оголошень, прес-релізів і інших матеріалів для симпозіумів, виставок, конгресів, а також виступів, наукових і інших публікацій співробітників фірми.

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:
форма 1 – для роботи з секретною інформацією, що має ступені секретності «особливої важливості», «цілком таємно» та «таємно»;
форма 2 – для роботи з секретною інформацією, що має ступені секретності «цілком таємно» та «таємно»;
форма 3 – для роботи з секретною інформацією, що має ступінь секретності «таємно».
Діють такі терміни дії допусків:
для форми 1 – 5 років;
для форми 2 – 7 років (абзац сьомий частини першої статті 22 із змінами, внесеними згідно із Законом N 2432-VI (2432-17) від 06.07.2010);
для форми 3 – 10 років (абзац восьмий частини першої статті 22 із змінами, внесеними згідно із Законом N 2432-VI (2432-17) від 06.07.2010).


Дякую за увагу!