Кафедра комп’ютерної інженерії та програмування
Спеціальність - 123 Комп’ютерна інженерія
Освітня програма – Прикладна комп’ютерна інженерія
Рівень вищої освіти - другий (магістерський)

БЕЗПЕКА ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

лекційний курс

Розробник Главчев Максим Ігорович

Затверджено протокол засідання кафдри КІП №10 від 18.03.2024 р.

Зміст

1. Основні поняття, концепції і принципи інформаційної безпеки
2. Основні загрози інформаційної безпеки комп’ютерних систем і мереж
3. Технології автентифікації, авторизації і управління доступом
4. Криптографія ч.1. Основні поняття
5. Криптографія ч.2. Симетричні системи
6. Криптографія ч.3. Системи з відкритими ключима
7. Криптографія ч.4. Ключи та проблеми криптографії
8. Комп'ютерні атаки й технології їх виявлення
9. Виявлення вторгнень та протидія вторгенням
10. Протоколи захищених каналів
11. Міжмережеві екрани (фаєрволи, брандмауери)
12. Безпека мобільних та бездротових мереж
13. Віртуальні безпечні технології VPN
14. Безпека корпоративних мереж
15. Системи захисту інформації в комп'ютерній мережі Інтернет
16. Стеганографія

ОСНОВНІ ПОНЯТТЯ, КОНЦЕПЦІЇ І ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тріада «конфіденційність, доступність, цілісність»

Відповідно інформаційна система знаходиться в стані безпеки, якщо вона захищена від порушень конфіденційності, цілісності і доступності, де:

- конфіденційність (Confidentiality) – це стан ІС, при якому інформаційні ресурси доступні тільки тим користувачам, яким цей доступ дозволений;
- цілісність (Integrity) – це стан системи, при якому інформація, що зберігається і обробляється цією ІС, а також процедури обробки інформації не можуть бути змінені, видалені або доповнені неавторизованим чином;
- доступність (Availability) – це стан системи, при якому послуги, що надаються системою, можуть гарантовано і з прийнятною затримкою бути надані користувачам, які мають на це право.



Гексада Паркера

Однією з найбільш популярних альтернатив тріаді КЦД є так звана гексада Паркера (Parkerian Hexad), яка була запропонована Паркером в 1998 році в роботі

- «Боротьба з комп'ютерною злочинністю». В гексаді Паркера визначено шість базових видів порушень, в число яких, крім порушень конфіденційності, доступності та цілісності, входять ще три види порушень: автентичності, володіння і корисності (рис.).
- Автентичність (Authenticity) – це стан системи, при якому користувач не може видати себе за іншого, а документ завжди має достовірну інформацію про його автора. З цього визначення видно, що автентичність є аналогом неспростовності.
- Володіння (Possession) – це стан системи, при якому фізичний контроль над пристроєм або іншим середовищем зберігання інформації надається тільки тим, хто має на це право.
- Корисність (Utility) – це такий стан ІС, при якому забезпечується зручність практичного використання як власне інформації, так і пов'язаних з її обробкою і підтримкою процедур. В безпечній системі заходи, що вживаються для захисту системи, не повинні неприйнятно ускладнювати роботу співробітників, інакше вони будуть сприймати їх як перешкоду і намагатися при всякій нагоді їх обійти.



Модель STRIDE

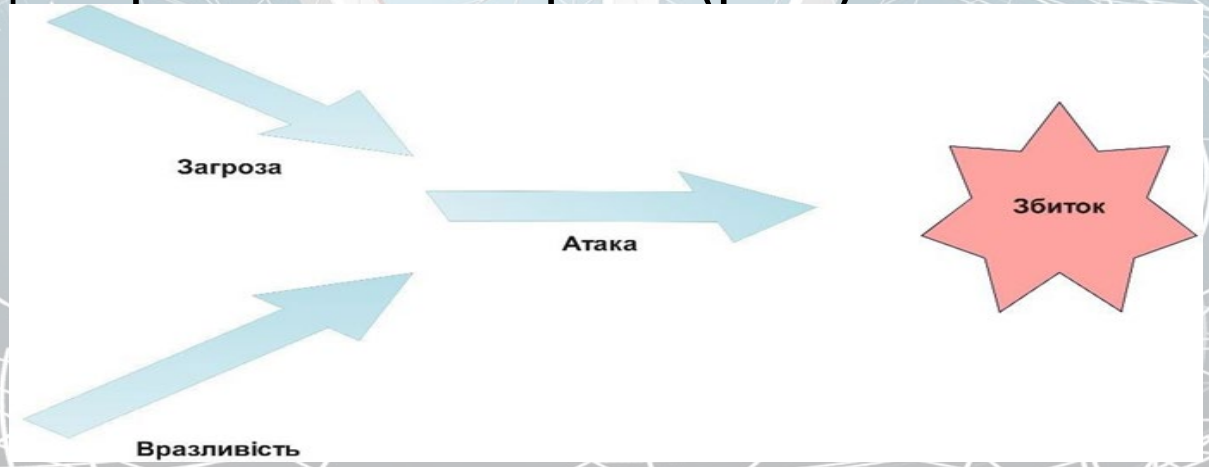
Модель STRIDE використовується компанією Microsoft при розробці безпечного програмного забезпечення. Відповідно до цієї моделі ІС знаходиться в безпеці, якщо вона захищена від наступних типів порушень: підміни даних, зміни, відмови від відповідальності, розголошення відомостей, відмови в обслуговуванні, захоплення привілеїв (рис 1.4.).

- Підміна даних (Spoofing) – це таке порушення, при якому користувач або інший суб'єкт ІС шляхом підміни даних, наприклад IP-адреси відправника, успішно видає себе за іншого, отримуючи таким чином можливість нанесення шкоди системі.
- Зміна даних (фальсифікації) (Tampering) означає порушення цілісності.
- Відмова від відповідальності (Repudiation) являє собою негативну форму вже розглянутої властивості неможливість відмови від авторства (non-repudiation).
- Розголошення інформації (Information Disclosure) – це порушення конфіденційності.
- Відмова в обслуговуванні (Denial of Service) стосується порушення доступності.
- Захоплення привілеїв (Elevation of Privilege) полягає в тому, що користувач або інший суб'єкт ІС несанкціонованим чином підвищує свої повноваження в системі, зокрема незаконне привласнення зловмисником прав мережевого адміністратора

Spoofing	Підміна даних
Tampering	Зміна даних (фальсифікації)
Repudiation	Відмова від відповідальності
Information Disclosure	Розголошення інформації
Denial of Service	Відмова в обслуговуванні
Elevation of Privilege	Захоплення привілеїв

Вразливість, загроза, атака

- Вразливість (Vulnerability) – це слабка ланка інформаційної системи, яка, ставши відомою зловмисникові, може дозволити йому порушити її безпеку.
- Загроза (Threat) – набір обставин і дій, які потенційно можуть призвести до порушення безпеки системи (тобто до порушення її конфіденційності, цілісності і доступності, якщо користуватися моделлю КЦД).
- Атака (Attack) – це реалізована загроза. Атака може відбутися тільки тоді, коли одночасно існують вразливість і спрямована на використання цієї вразливості загроза (рис.).



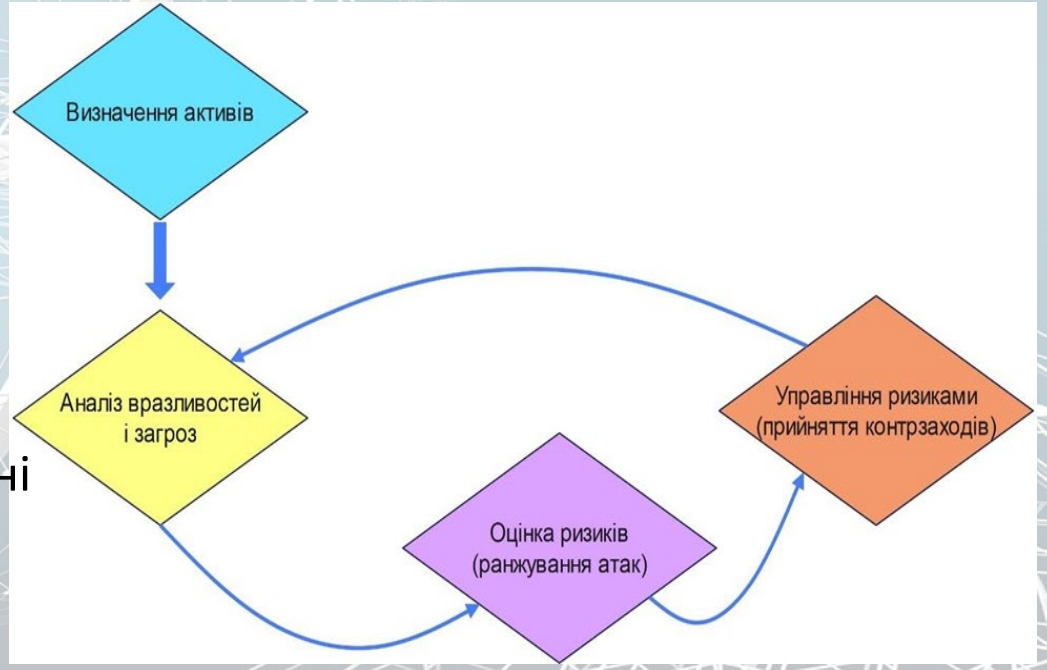
Збиток та ризик. Управління ризиками

Збиток (Loss, Impact) – це негативний вплив на систему, який чиниться проведеною атакою.

Управління ризиками – це системний аналіз загроз, прогнозування та оцінка їх наслідків для підприємства, ранжування загроз за ступенем їх ймовірного здійснення і небезпеки наслідків і, нарешті, вибір на пріоритетній основі контрзаходів, спрямованих на пом'якшення або виключення можливого негативного впливу цих порушень на діяльність підприємства.

Аналіз вразливостей – об'єктивне обстеження реально існуючих комп'ютерної мережі, адміністративних процедур і персоналу. Загрози визначаються по відношенню до активів підприємства, тобто ресурсів підприємства, які представляють для нього цінність і є об'єктом захисту (обладнання, нерухомість, транспортні засоби, обчислювальні пристрої, ПЗ, документація та ін.).

Оцінка ризиків – ранжування можливих атак за ступенем небезпеки. Для цього обчислюються відповідні ризики – ймовірнісні оцінки збитку, який може бути нанесений підприємству кожної з атак протягом деякого періоду часу. Ризик атаки тим вищий, чим більше шкоди від неї і чим вище її ймовірність.



Ієрархія засобів захисту від інформаційних загроз



Багаторівнева модель засобів захисту від інформаційних загроз Інформаційні технології пронизують наше життя, тому цілком природно,

- Загальновизнаним є представлення різних засобів захисту у вигляді чотирьох ієрархічно організованих рівнів, засоби кожного з яких можуть бути використані на різних етапах життєвого циклу системи забезпечення інформаційної безпеки
- До цього рівня засобів безпеки відносяться правове регулювання, стандартизація, ліцензування та морально-етичні норми, прийняті в суспільстві. Законодавство може прямо впливати на концепцію побудови захисту.
- Законодавство включає заходи обмежувально-репресивного характеру, спрямовані на запобігання порушень, в тому числі шляхом застосування покарань (наприклад, кримінальний кодекс), і заходи творчого характеру, спрямовані на координацію робіт у сфері ІБ, навчання і допомогу в створенні і використанні засобів забезпечення інформаційної безпеки (наприклад, стандарти).

Приклад стандартизації критеріїв безпеки

До числа найвідоміших сертифікаційних стандартів відносять Помаранчеву книгу (формальна назва цього стандарту: «Міністерство оборони США. Критерії оцінки довірених комп'ютерних систем»). , ця розробка стала класичною і загальноприйнятою в усьому світі для класифікації ступеня захищеності системи, згідно наступних рівнів:

- D - рівень мінімального захисту (Minimal Protection). Зарезервовано для систем, які одержали попередню оцінку, однак для класифікації за іншими рівнями не гарантують потрібного рівня безпеки;
- C1 - рівень вибіркового захисту (Discretionary Protection). Дає змогу користувачам застосовувати обмеження доступу для захисту приватної інформації;
- C2 - рівень керованого доступу (Controlled Access Protection). Містить вимоги рівня C1, а також захист процесу реєстрації у системі, облік подій захисту, ізоляцію ресурсів різних процесів;
- B1 — рівень захисту за категоріями (Labeled Protection). До вимог рівня C2 додається можливість захисту окремих файлів, записів у файлах, інших об'єктів системи. Вважають, що подолати такий захист може добре підготовлений хакер, а звичайний користувач - ні;
- B2 - рівень структурованого захисту (Structured Protection). До вимог рівня B1 додається повний захист усіх ресурсів системи прямо чи посередньо доступних користувачу. Вважають, що хакери не зможуть проникнути у систему з таким захистом;
- B3 - рівень доменів безпеки (Security Domains). До вимог рівня B2 додається явна специфікація користувачів, яким заборонено доступ до певних ресурсів, повніша реєстрація потенційно небезпечних подій. Вважають, що навіть досвідчені програмісти не в стані подолати систему з таким рівнем безпеки;
- A1 - рівень верифікованої (випробуваної) розробки (Verified Design). Повний захист інформації. Специфіковані та верифіковані механізми захисту. Вважають, що у систему з таким рівнем захисту без дозволу не може проникнути ніхто (навіть спеціалісти спецслужб).

Адміністративний рівень. Політика безпеки

- Основу адміністративного рівня засобів безпеки становить політика безпеки, яка визначає стратегічні напрями інформаційної захисту підприємства, а саме окреслює коло критично важливих інформаційних ресурсів підприємства, захист яких представляє найвищий пріоритет, пропонує можливі заходи усунення або зменшення пов’язаних з цими ресурсами ризиків. На основі знайденої стратегії розробляється програма забезпечення безпеки ІС, планується сукупний бюджет, необхідний для виконання програми, призначаються керівники і обмежується зона їх відповідальності.
- Політика безпеки – це сукупність документованих правил, процедур, практичних прийомів або керівних принципів в області безпеки інформації, якими керується організація у своїй діяльності.

Засоби безпеки процедурного рівня

Засоби безпеки процедурного рівня вирішують завдання, поставлені адміністративним рівнем, з використанням технічних засобів, що надаються технічним рівнем. В якості основного засобу процедурного рівня виступає людина, яка виконує взаємопов’язану послідовність дій, спрямовану на вирішення певної задачі забезпечення безпеки.

При управлінні персоналом слід дотримуватися кількох загальновизнаних принципів.

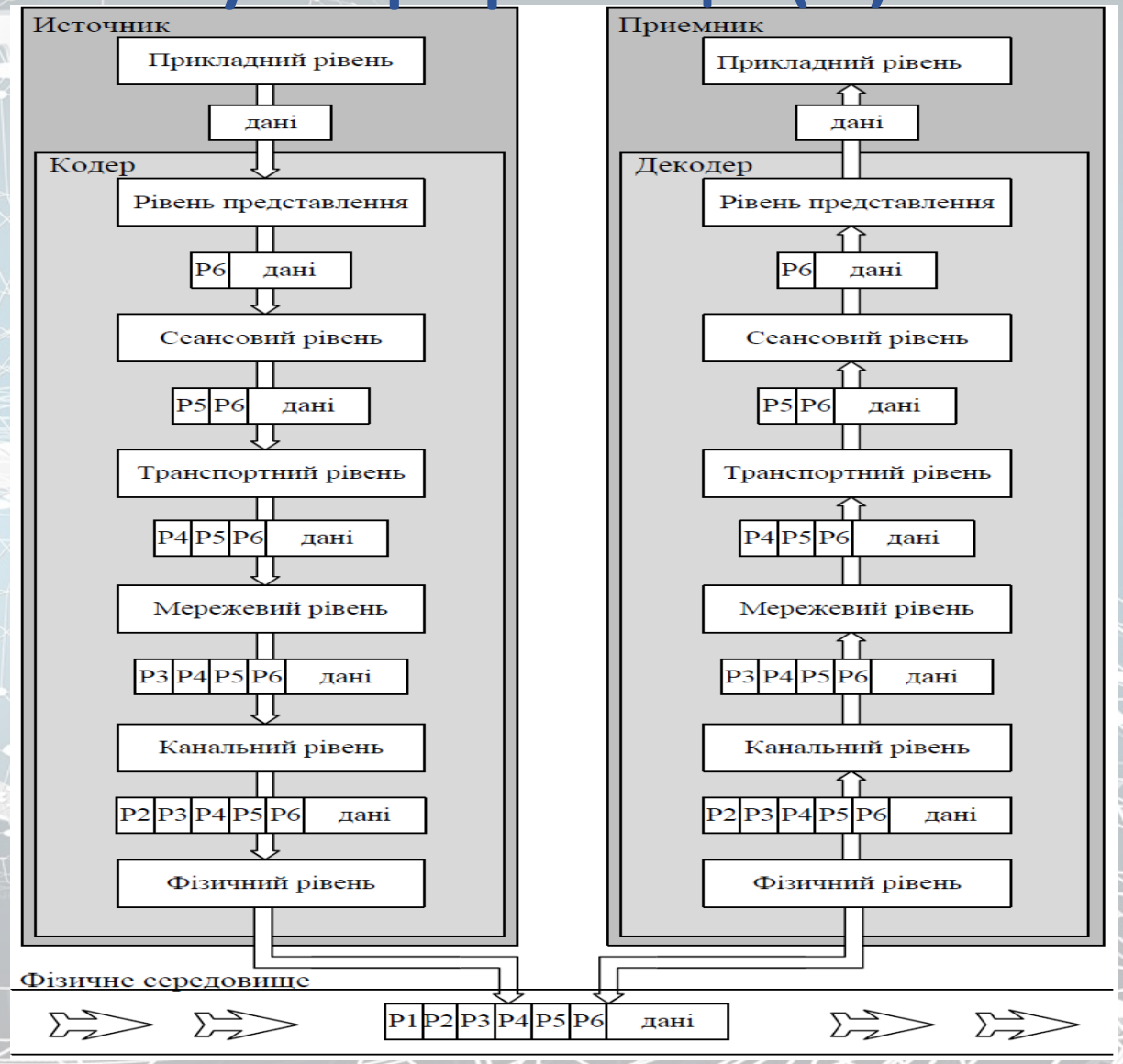
- Розмежування обов’язків переслідує кілька цілей: по-перше, це сприяє підвищенню продуктивності за рахунок спеціалізації, по-друге, усуває непотрібне дублювання, а по-третє (що важливо для безпеки), не дає концентрувати занадто багато повноважень в одних руках. У деяких, особливо критичних випадках, таке розмежування вводиться для того, щоб якась дія могла бути виконана лише за участю двох (або більше) осіб.
- Принцип мінімально необхідного рівня привілеїв означає, що кожен співробітник повинен мати тільки той тип доступу і тільки до тих ресурсів, які йому необхідні для виконання його службових обов’язків.
- Принцип безперервного навчання правилам безпеки. Ознайомлення з політикою безпеки підприємства при поступленні на роботу повинно доповнюватися регулярними роз’ясненнями всіх внесених до неї змін; необхідно донести до співробітників важливість забезпечення безпеки і пояснити, що в зв’язку з цим очікується від них.

Засоби безпеки технічного рівня

Технічні засоби і методи можна розділити на програмні, апаратні та програмно-апаратні. Програмні засоби включають захисні інструменти операційних систем (підсистеми автентифікації та авторизації користувачів, засоби управління доступом, аудит та ін.) і прикладні програми, призначені для вирішення завдань безпеки (системи виявлення та запобігання вторгнень, антивірусні засоби, проксі-сервери). Прикладом апаратних засобів, що спеціалізуються на інформаційному захисті, є джерела безперебійного живлення, генератори напруги, засоби контролю доступу в приміщення і ін. До апаратно-програмних засобів відносяться, наприклад, деякі аналізатори мережевого трафіку і міжмережеві екрани. І хоча даний рівень засобів називається технічним, до нього також відносять математичні методи (методи криптографії), алгоритми (евристичний алгоритм розрахунку часу обороту в протоколі TCP), абстрактні моделі (моделі контролю доступу) і т. п.

Послуги і механізми захисту інформації (1)

Еталонну модель OSI (англ. Open Systems Interconnection) було розроблену інститутом стандартизації ISO з метою розмежування функцій різних протоколів у процесі передачі інформації від одного абонента іншому. Подібних класів функцій було виділено 7. Вони одержали назву рівнів. Кожен рівень виконує певні завдання в процесі передачі блоку інформації
В цілому проходження блоку даних від відправника до одержувача показане на рис. Кожен рівень додає до пакета невеликий обсяг своєї службової інформації – префікс (на рисунку вони зображені як P1...P7). Деякі рівні в конкретній реалізації цілком можуть бути відсутніми. Дана модель дозволяє провести класифікацію мережевих атак відповідно до рівня їх дії.



Послуги і механізми захисту інформації (2)

- Фізичний рівень відповідає за перетворення електронних сигналів у сигнали середовища передачі інформації (імпульси напруги, радіохвилі, інфрачервоні сигнали). На цьому рівні основним класом атак є "відмова в сервісі".
- Канальний рівень керує синхронізацією двох і більшої кількості мережевих адаптерів, підключених до єдиного середовища передачі даних.
- Мережевий рівень відповідає за систему унікальних імен і доставку пакетів за цим іменем, тобто за маршрутизацію пакетів. Відповідно й атаки на цьому рівні найчастіше спрямовані на конфіденційність і цілісність службової інформації, пов'язаної з адресацією і наявністю унікальних імен.
- Транспортний рівень відповідає за доставку великих повідомлень по лініях з комутацією пакетів. Оскільки в подібних лініях розмір пакета є зазвичай невеликим числом (від 500 байт до 5 кілобайт), то для передачі великих обсягів інформації їх необхідно розбивати на передавальній стороні й збирати на приймальній
- Сеансовий рівень відповідає за процедуру встановлення початку сеансу і підтвердження (квитування) приходу кожного пакета від відправника одержувачу.
- Представницький рівень визначає формат, використаний для обміну даними між мережевими комп'ютерами і відповідає за перетворення протоколів, трансляцію даних, їх шифрування, зміну або перетворення вжитого набору символів (кодової таблиці) і розширення графічних команд.
- Прикладний рівень – найвищій рівень моделі OSI. Він є вікном для доступу прикладних процесів до мережевих послуг. Цей рівень забезпечує послуги, що безпосередньо підтримують додатки користувача, такі, як програмне забезпечення для передачі файлів, доступу до баз даних, електронна пошта.

Послуги і механізми захисту інформації (3)

Методологічною основою розробки системи захисту інформації є стандарт ISO/IEC 15408, згідно з яким основними нормативними документами, що характеризують інформаційну систему з точки зору безпеки, є профіль захисту (protection profile) і проект забезпечення безпеки (security target).

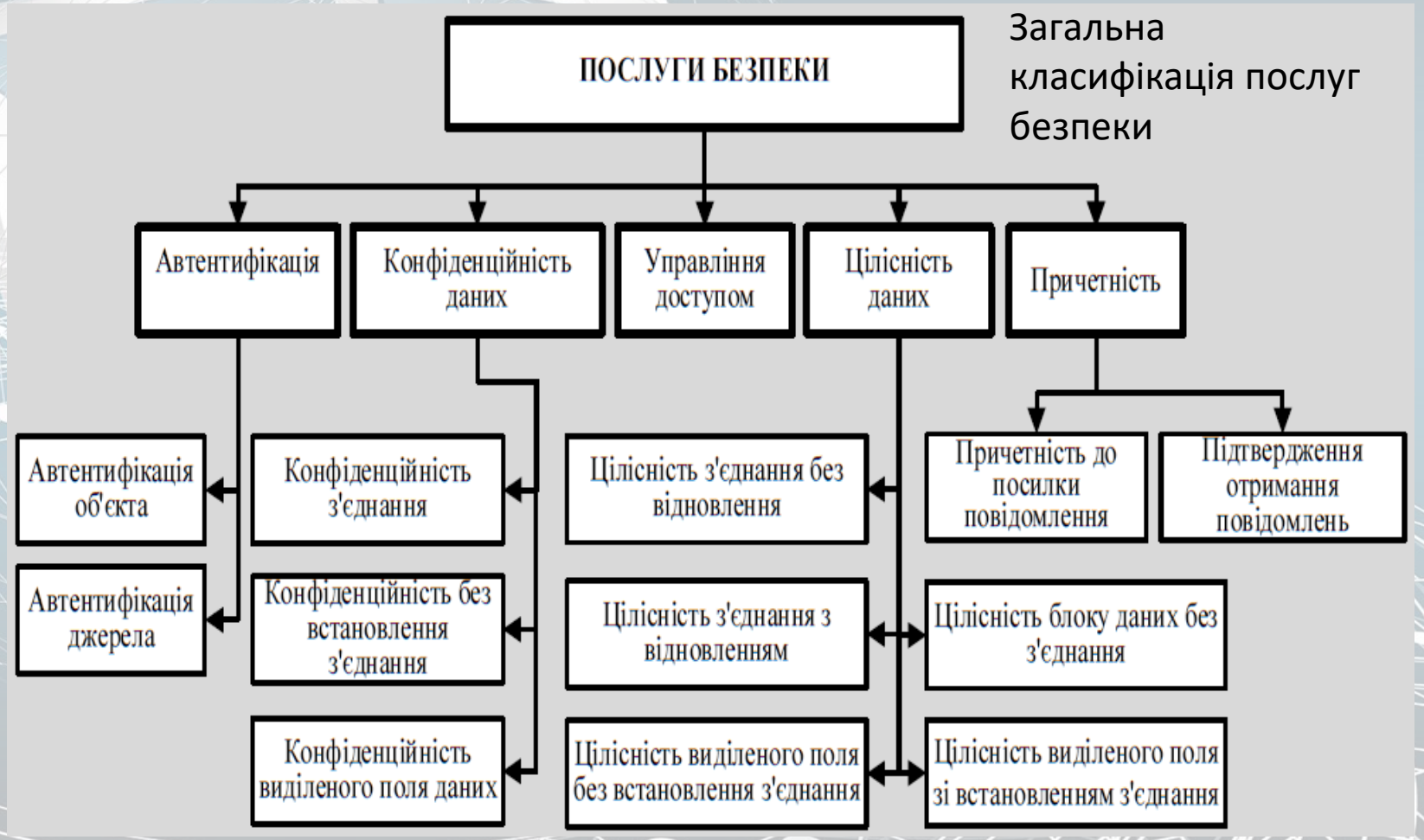
Відповідно до основних положень міжнародних стандартів життєвий цикл системи захисту інформації складається з п'яти етапів:

1. Визначення політики безпеки, яка містить абстрактний ряд вимог до безпеки системи.
2. Аналіз вимог безпеки, включаючи аналіз ризиків, аналіз урядових, правових і стандартних вимог.
3. Визначення послуг безпеки, необхідних для задоволення поставлених вимог.
4. Побудова і впровадження системи безпеки, включаючи вибір механіз- мів безпеки, що забезпечують конкретні вибрані послуги безпеки.
5. Безперервне управління безпекою.

Послуги і механізми захисту інформації (4)

Стандарти ISO 7498, ISO/IEC 10181 визначають п'ять базових загальноприйнятих послуг безпеки (рис.):

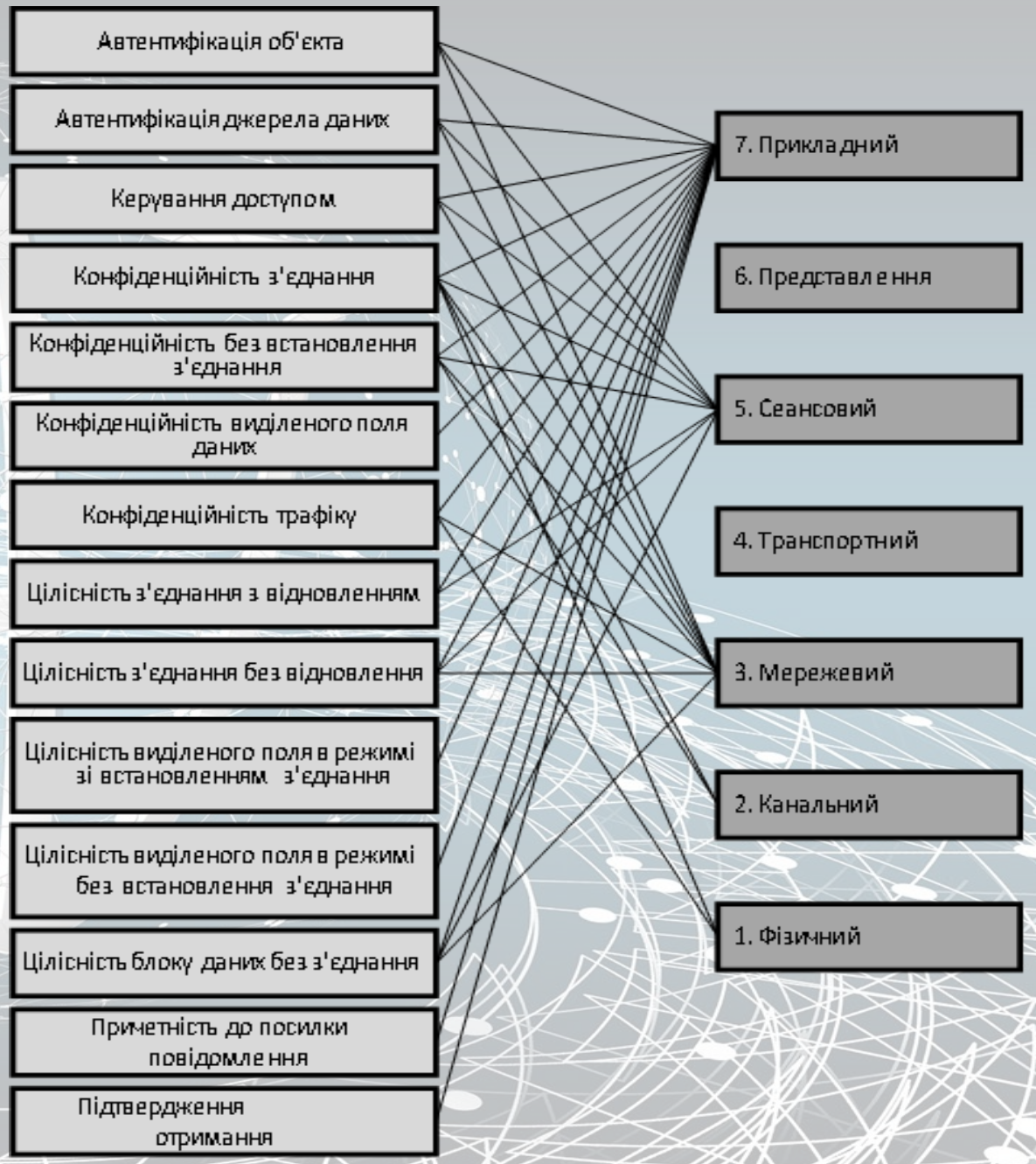
- автентифікація (authentication);
- керування доступом (access control);
- конфіденційність даних (data confidentiality);
- цілісність даних (data integrity);
- невідмова (причетність) (non-repudiation).



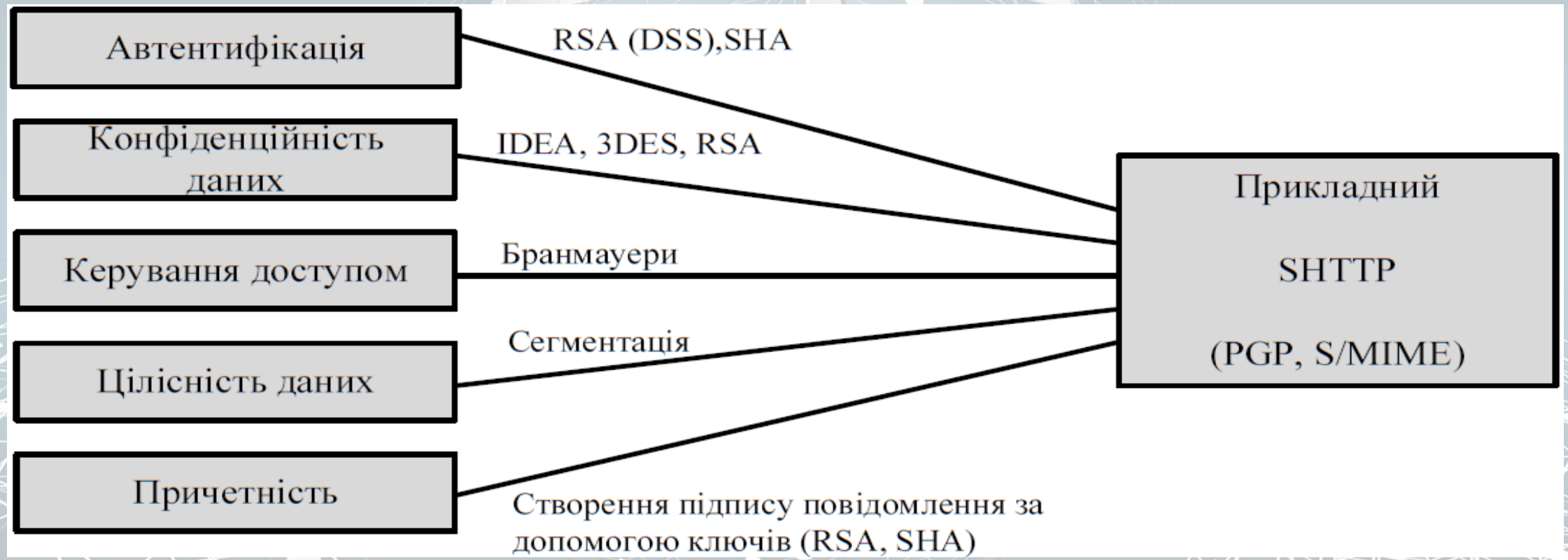
Загальна класифікація послуг безпеки

Послуги і механізми захисту інформації (5)

- На рис. подано розподіл послуг безпеки по рівнях моделі взаємодії відкритих систем (ВВС). Як видно з наведеного рисунка, велика частина послуг безпеки доводиться на верхні рівні моделі ВВС, переважно, на рівень прикладного процесу. Розглянемо основні системи забезпечують захист інформації на різних рівнях моделі ВВС.

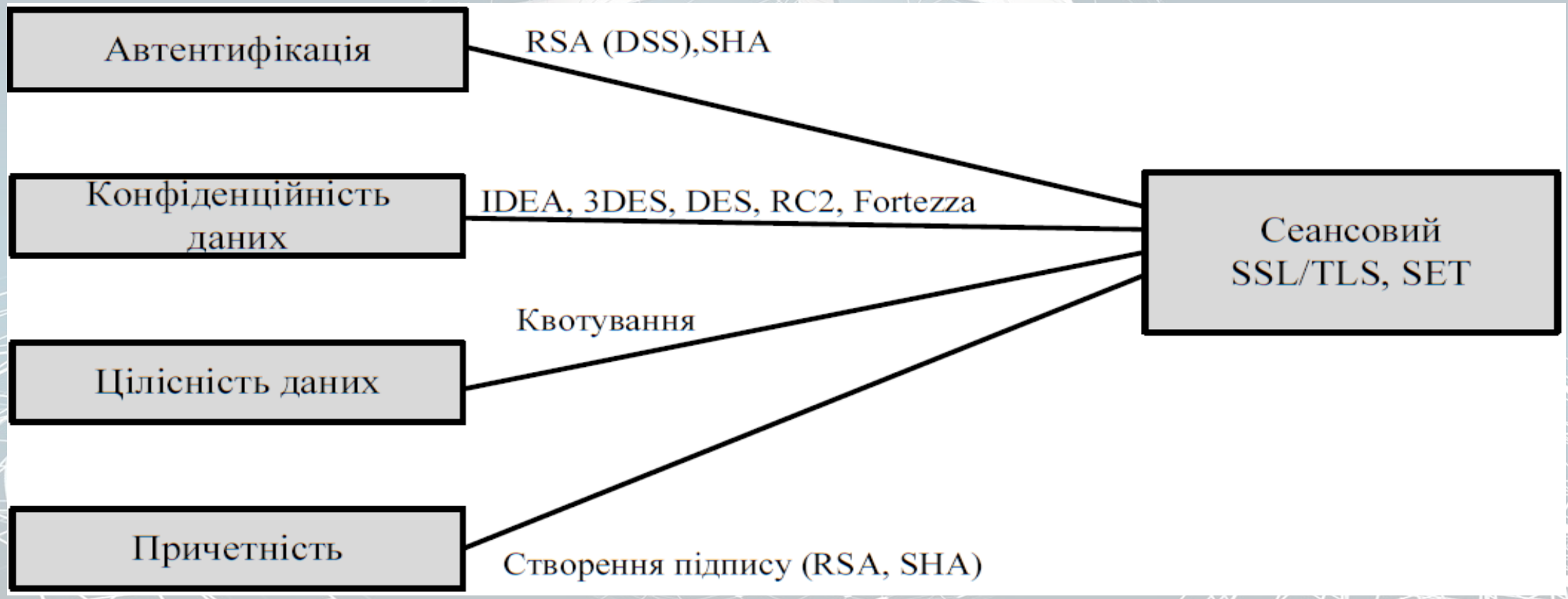


Послуги і механізми захисту інформації (6)



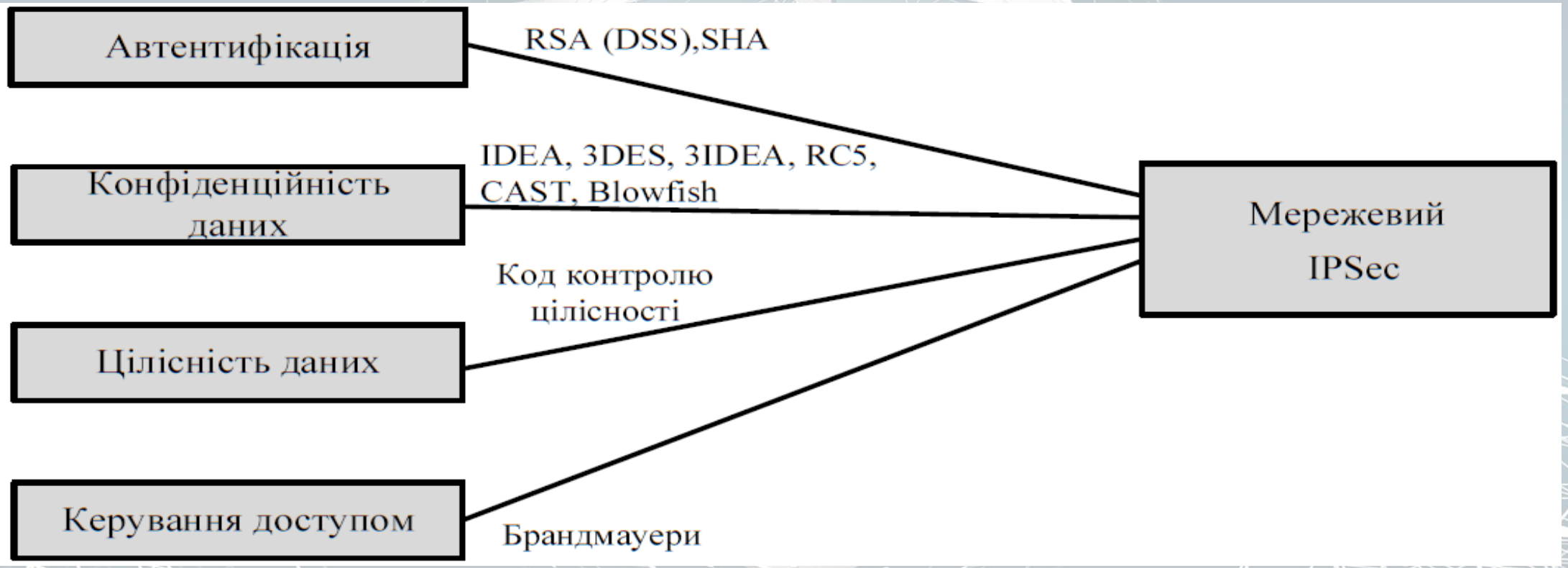
- Системи, що забезпечують захист інформації на прикладному рівні

Послуги і механізми захисту інформації (7)



Системи, що забезпечують захист інформації на сеансовому рівні

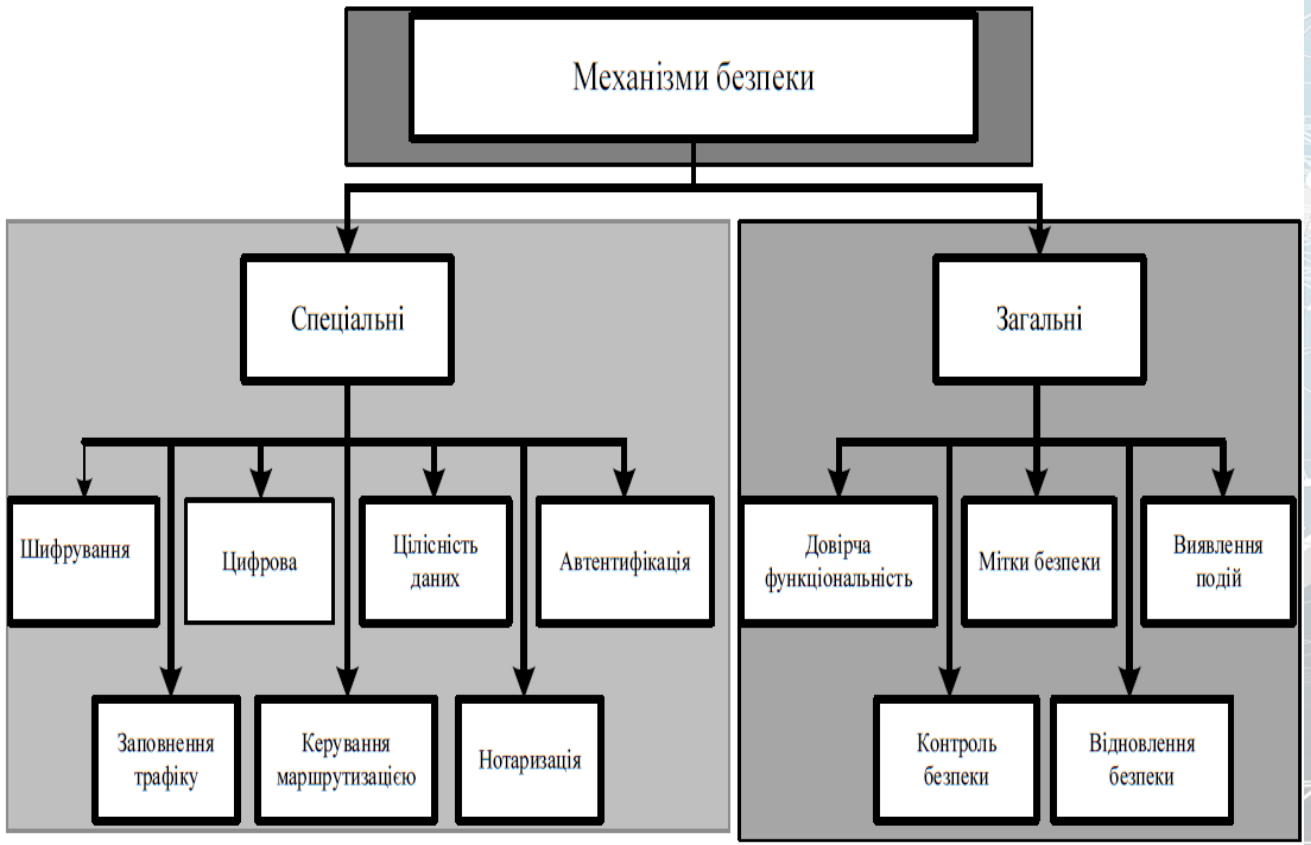
Послуги і механізми захисту інформації (8)

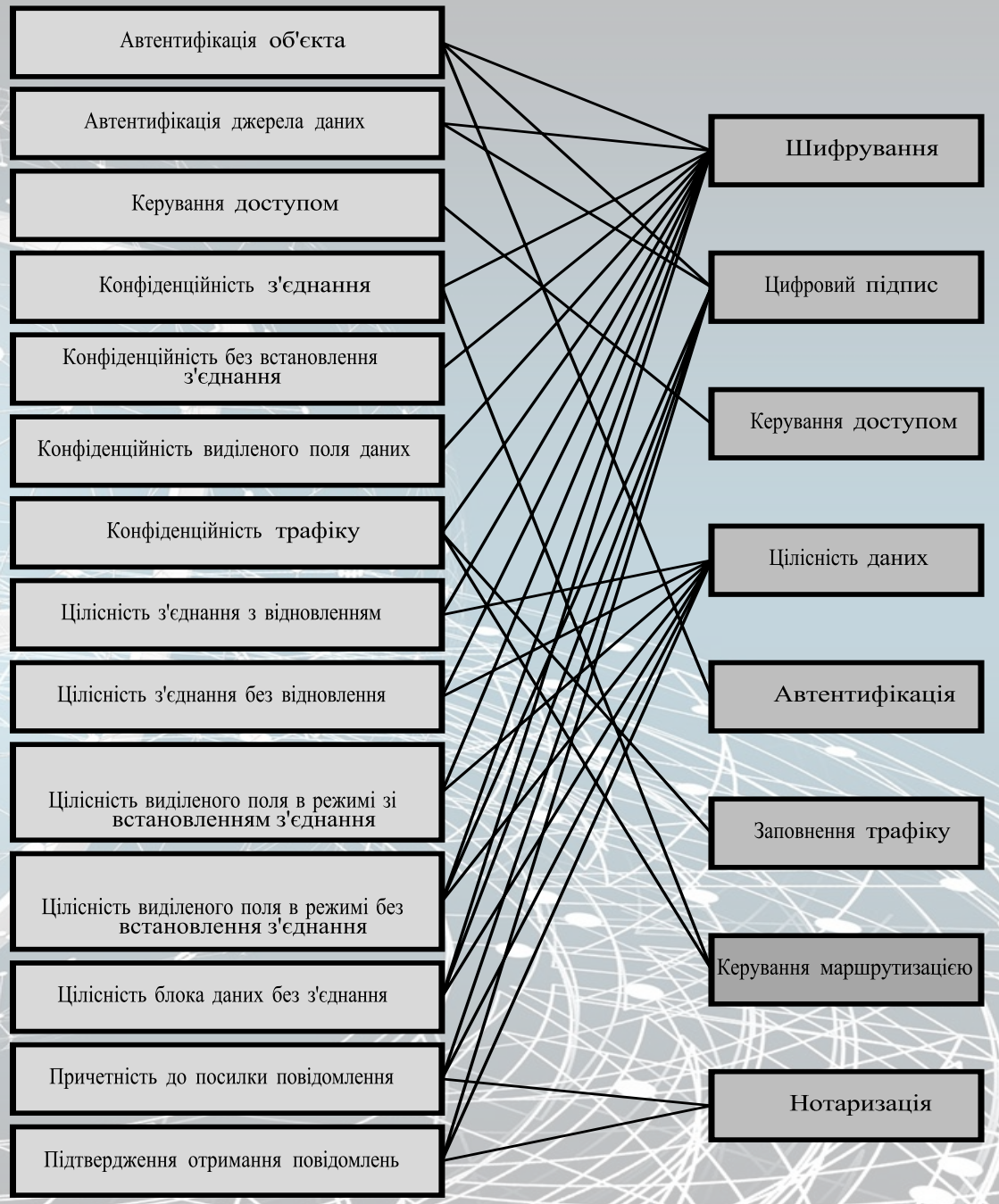


Системи, що забезпечують захист інформації на мережевому рівні

Послуги і механізми захисту інформації (9)

Механізми безпеки є конкретними заходами для реалізації послуг безпеки (рис. праворуч). Взаємозв'язок послуг і механізмів безпеки подано на рис. ліворуч





Послуги і механізми захисту інформації (10)

- Механізми шифрування припускають використання криптографічних перетворень даних для того, щоб зробити їх нечитабельними або неосмисленими. Шифрування застосовується спільно зі зворотною функцією – розшифрування.
- Цифровий підпис є цифровим еквівалентом підпису (друку, штампа та ін..), наявність якого в повідомленні дозволяє з високою точністю визначити джерело повідомлення (документа) і юридично довести, що, з певною ймовірністю, тільки він міг створити і підписати цей документ.
- Механізми керування доступом використовуються для забезпечення послуг керування доступом і реалізують політику керування доступом.
- Механізми другого типу, які зазвичай застосовуються спільно з механізмами захисту цілісності окремого пакета даних, можуть використовуватися для забезпечення послуг цілісності при організації зв'язку в режимі зі встановленням з'єднання.
- Автентифікація джерела даних часто забезпечується шляхом використання механізму захисту цілісності даних спільно з шифруванням або цифрового підпису.
- Механізм заповнення трафіку застосовується для забезпечення конфіденційності трафіку.
- Механізми керування маршрутизацією застосовуються для забезпечення конфіденційності з метою запобігання контролю за шляхом проходження даних від відправника до одержувача.

Послуги і механізми захисту інформації (11)

До загальних механізмів забезпечення безпеки належать:

- довірча функціональність (trusted functionality). Довірча функціональність припускає широке використання нормативної документації при розробленні програмних або апаратних засобів, що реалізовують механізми безпеки. ;
- позначки безпеки (security lables). Зазвичай позначки безпеки використовуються для реалізації методики керування доступом на основі встановлених правил, а також для керування маршрутизацією. ;
- виявлення подій (event detection) в системах захисту інформації служать для виявлення як спроб порушення безпеки, так і для реєстрації легітимної активності користувачів
- контроль безпеки (security audit trail) - незалежний розгляд і аналіз записів безпеки з метою перевірки достатності керування системою, гарантувати відповідність функціонування системи політиці безпеки і рекомендувати необхідні зміни в управлінні, політиці і процесах безпеки;
- відновлення безпеки (security recovery) - виконують функцію реакції системи на порушення безпеки. .

Програмні засоби забезпечення захисту інформації в мережі

Програмні засоби захисту інформації призначені для виконання логічних та інтелектуальних функції захисту і включаються або у склад програмного забезпечення автоматизованих інформаційних систем, або до складу засобів, комплексів та систем апаратури контролю.

- Firewall здатні забезпечити захист окремих протоколів і програмних продуктів. Вони здійснюють контроль доступу ззовні до внутрішньої мережі, і окремих сегментів на основі вмісту пакетів даних, що передаються між двома сторонами, або пристроями мережею.
- Віртуальні приватні мережі (virtual private networks, VPN) – територіально розподілені корпоративні мережі, які використовують для зв’язку між окремими сегментами інтернету.
- Використання антивірусних засобів вважається необхідною умовою при підключенні до інтернету, дозволяє значно знизити втрати інформації в наслідок зараження шкідливими програмами.

Технічні (апаратні) засоби забезпечення захисту інформації

- До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп’ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у випадку порушення працездатності окремих ланок, установку устаткування виявлення і гасіння пожежі, вживання конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів, установлення резервних систем електроживлення, оснащення приміщень замками, установку сигналізації і багато чого іншого.
- Вся сукупність технічних засобів захисту підрозділяється на апаратні і фізичні.
- Апаратні засоби – пристрої, що вбудовуються безпосередньо в обчислювальну техніку, чи пристрою, що сполучаються з нею по стандартному інтерфейсу.

Програмно-апаратні засоби забезпечення безпеки мережі

Виходячи із викладеного, програмно-апаратні засоби мають наступну класифікацію:

- апаратно-незалежні – працюючі без участі апаратних засобів захисту інформації – пароль, програми шифрування, антивіруси;
- апаратно-залежні – забезпечення сполучених апаратних засобів захисту інформації з інших програм або ОС – драйвера, вільне ПЗ;
- автономні – частина систем захисту функціонує;
- комплексні – кілька частин системного захисту використовують загальний елемент і базу ідентифікації або використовують інформацію, отриману від інших частин системи захисту – ключ, використовується і при завантаженні комп'ютера, параметри користувача ігноруються, якщо він не прийшов на роботу, тобто не пройшов контроль;
- інтелектуальні засоби – усі системи безпеки, системи керування безпекою об'єднані в єдине ціле.

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП’ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Порушники безпеки

Однією з двох найпоширеніших загроз безпеки є порушники (другою загрозою є віруси), яких називають хакерами (hacker) або зломщиками (cracker). Дамо класифікацію порушників.

- Імітатор (masquerader) – це особа, що не має права користуватися комп'ютером, але подолала механізм керування доступом і використовує права доступу деякого легального користувача.
- Правопорушник (misfeasor) – це легальний користувач, що намагається дістати доступ до даних, програм або ресурсів, до яких він не має відповідних прав доступу, або користувач, який має в своєму розпорядженні відповідні права доступу, але використовує їх в зловмисних цілях.
- Таємний користувач (clandestine user) – це особа, що заволоділа правами керування системою і використовує ці права для обходу засобів аудиту і керування доступом або для створення перешкод у реєстрації системних подій.

Методика вторгнення порушників

Метою порушника є отримання доступу до системи або розширення прав, наданих йому системою на законній підставі. Для цього порушнику потрібно дістати інформацію, яка підлягає захисту. В більшості випадків вона подана у формі пароля користувача. Можливі такі методи отримання паролів.

1. Перевірка паролів за умовчанням для стандартних облікових записів, що постачаються з системою. Більшість адміністраторів не обтяжують себе роботою зі зміни встановлених за умовчанням значень.
2. Перебирання усіх коротких паролів (від одного до трьох символів).
3. Перевірка слів з системного словника або із списку найбільш ймовірних паролів. Список останніх завжди можна знайти на електронних дошках оголошень хакерів.
4. Збирання інформації про користувачів, включаючи їх повні імена, імена їх дружин, чоловіків, дітей, назви картин і фотографій на робочих місцях і навіть назви їх улюблених книг, за якими можна судити про їх захоплення.
5. Перевірка паролів телефонних номерів, номерів соціальної страховки і номерів кімнат користувачів.
6. Перевірка паролів усіх можливих для даного регіону номерних знаків автомобілів.
7. Використання "троянського коня" для обходу обмежень доступу.
8. Підключення до лінії зв'язку між користувачем і головним вузлом.

Методи протидії порушенням

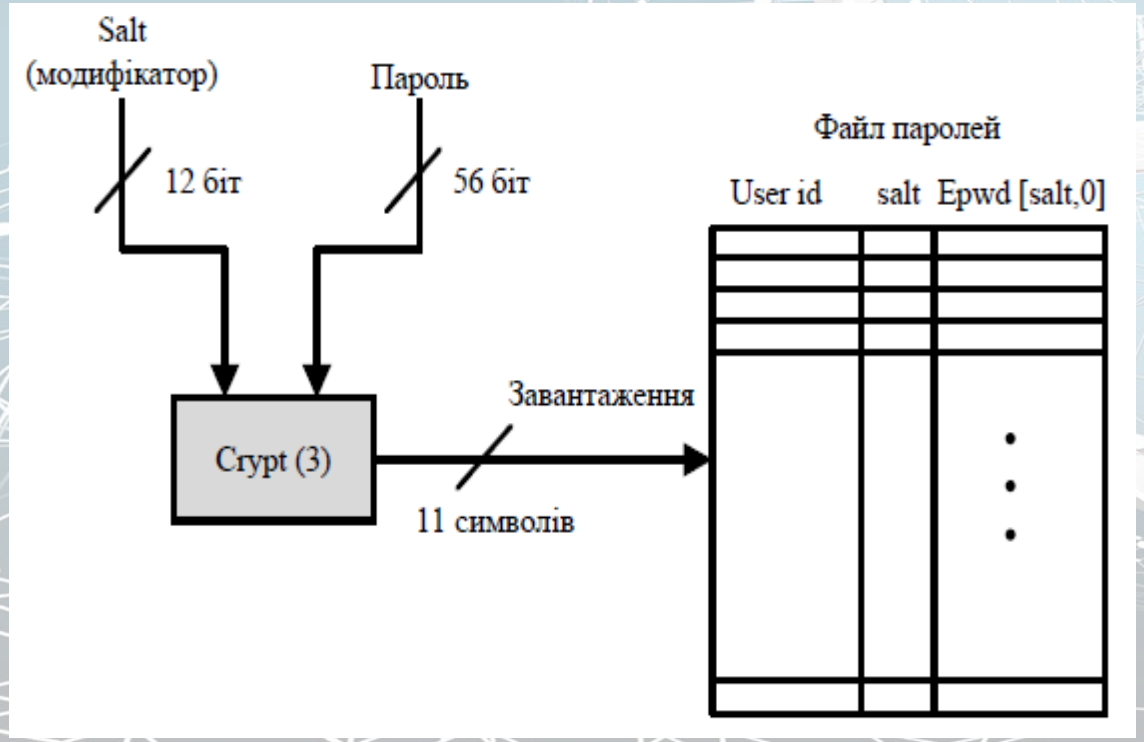
1. Попередження порушень є незмінною метою системи захисту і, в якомусь сенсі, нескінченною битвою з невидимим супротивником.
2. Мета виявлення порушень полягає у вивченні типу використаної атаки до її успішного завершення або після.

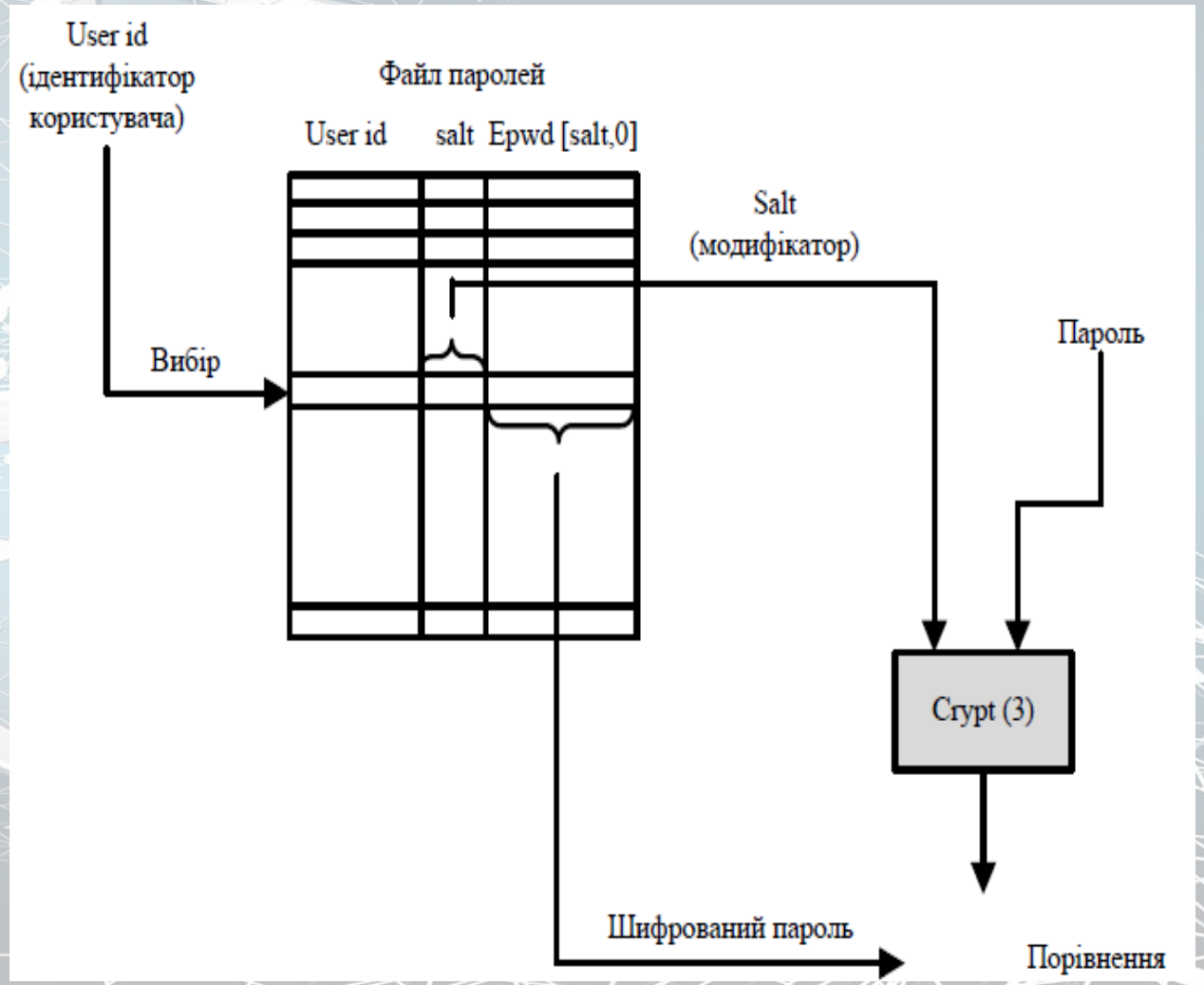
- Першою лінією захисту від порушників є система паролів. Пароль виконує функції автентифікації користувача, що входить до системи.
- Ідентифікатори користувачів відіграють важливу роль при використанні так званого розмежувального контролю доступу (discretionary access control).

Схема використання системи паролів в UNIX

Перевірка пароля

Завантаження нового пароля





Стратегії вибору пароля

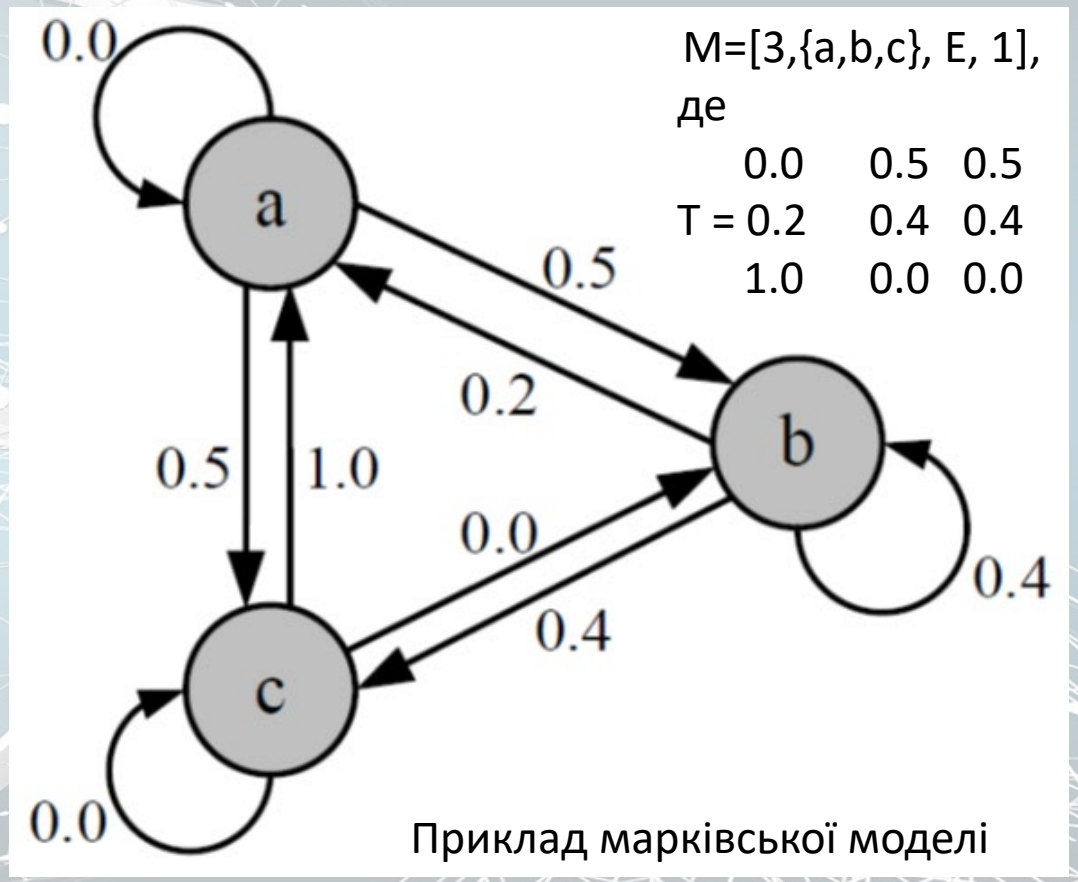
Мета полягає у створенні умов, які виключають вибір користувачем легко вгадуваного пароля і в той же час зберігають можливість вибору пароля, що легко запам'ятовується. Рішення цієї задачі досягається за рахунок таких засобів:

- навчання користувачів;
- генерування паролів комп'ютером;
- реактивна перевірка пароля полягає в тому, що система періодично запускає власну програму підбору паролів, яка виявляє легко паролі, що вгадуються. ;
- попереджувальна перевірка пароля, дозволяє вибирати пароль на свій розсуд, але в процесі вибору система перевіряє пароль на відповідність встановленим вимогам і, якщо необхідно, відкидає його.

.

Попереджувальна перевірка пароля

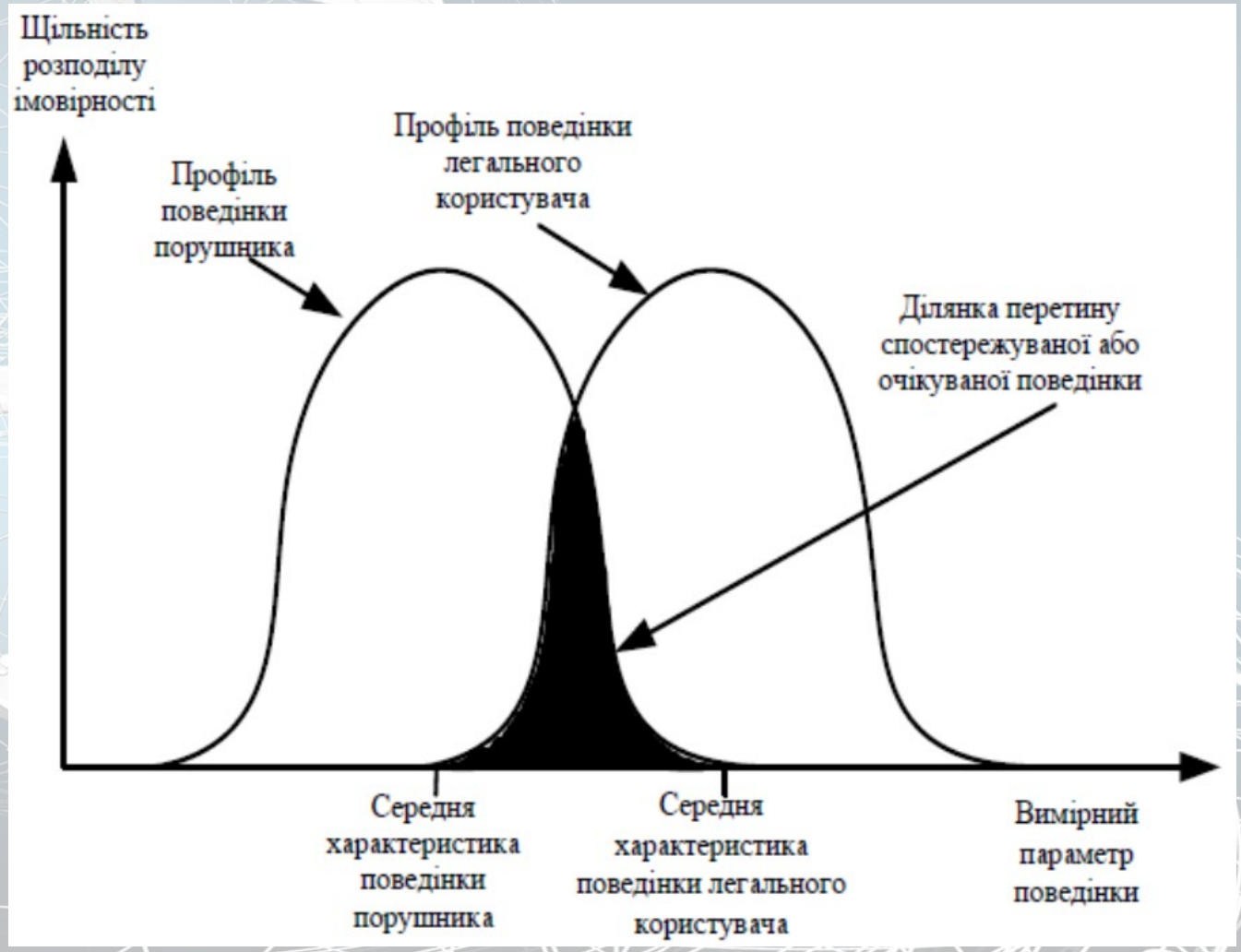
- Перспективний метод будується на основі використання марківської моделі генерування паролів, що вгадуються. На рис.показана спрощена версія такої моделі. Ця модель задає мову, алфавіт якої складається з трьох символів. Стан системи у будь-який момент ідентифікується останнім вибраним символом. Коефіцієнти переходів з одного стану в інший задаються ймовірністю проходження одних символів за іншими. Наприклад, імовірність того, що наступною буквою буде b за умови, що поточною є буква a, в даній ситуації дорівнює 0,5.
- У загальному випадку марківська модель задається чотирма значеннями [т, A, T, k, де т – позначає число станів моделі, A – простір станів, T – матрицю імовірності переходів, а k – порядок моделі. Для моделі порядку k імовірність переходу до того або іншого символу алфавіту залежить від значень k попередніх символів. На рис. показано схему простої моделі першого порядку.



Виявлення порушників (1)

Виявлення порушень ґрунтується на припущенні, що поведінка порушника відрізняється від поведінки легального користувача і відповідні відмінності можна подати в кількісному виразі. Звичайно ж, не можна чекати, що ми зможемо спостерігати абсолютно різне використання ресурсів порушником порівняно з легальним користувачем. Правильніше припустити, що в поведінці того й іншого будуть загальні риси.

На рис в дуже абстрактному вигляді ілюструється природа завдання, що стоїть перед розробником системи виявлення порушень. Хоча типова поведінка порушника й відрізняється від типової поведінки легального користувача, сфери, які характеризують їхню поведінку, все ж таки, перетинаються.



Виявлення порушників (2)

Пропонуються такі підходи до розв’язання проблеми виявлення порушень.

1. Виявлення на базі статистичних відхилень передбачає збирання даних, що характеризують поведінку легальних користувачів, протягом певного часу. Потім ці дані аналізуються із застосуванням статистичних методів, щоб з високим ступенем точності визначити, відповідає поведінка певного користувача поведінці легального користувача чи ні. Найбільш поширеними є:

- використання порогових значень. Даний підхід припускає визначення незалежних від конкретного користувача порогових значень, що характеризують частоту виникнення різних подій.
- використання профілю поведінки. Створюється профіль активності користувача і за допомогою цього профілю виявляються відхилення в поведінці користувача, що реєструється в системі під даним ім'ям.

2. Виявлення на базі правил. Припускає розробку набору правил, на основі яких ухвалюється рішення про те, що даний тип поведінки є поведінкою порушника. Найбільш поширеними є:

- виявлення аномалій. Розробляються правила, що дозволяють виявити відхилення від поведінки, які спостерігались раніше .
- ідентифікація вторгнення. Підхід на основі використання експертної системи, що виявляє підозрілу поведінку.

Виявлення порушників (3)

Основним засобом виявлення порушень є контрольний запис (audit record), який передбачає виконання запису деяких операцій, що здійснюються користувачами для подальшого застосування цих записів як початкових даних системи виявлення порушень. Найчастіше застосовують такі дві стратегії.

- Системні контрольні записи (native audit records). Практично всі операційні системи, розраховані на велику кількість користувачів, містять програми для збору інформації про дії, що виконуються користувачами. Перевага використання цієї інформації полягає у відсутності додаткового програмного забезпечення. Недолік пов'язаний з тим, що системні контрольні записи можуть не містити необхідної інформації або можуть містити її в невідповідній формі.
- Спеціальні контрольні записи (detection-specific audit records). Можуть бути розроблені і застосовані спеціальні засоби збору інформації, які генерують записи, що містять дані, необхідні тільки для роботи системи виявлення порушень. Перевагою такого підходу є незалежність від постачальника системи і здатність до перенесення на різні платформи. Як недолік слід зазначити додаткове навантаження на систему у зв’язку з необхідністю виконання двох програм ведення контрольних записів.

Виявлення порушників (4)

Виявлення за профілем поведінки будується на вивченні попередньої поведінки користувача або групи користувачів і порівнянні цієї поведінки з поточною поведінкою на предмет виявлення значних відхилень.

Даний підхід спирається на аналіз вмісту контрольних записів. Контрольні записи забезпечують введення для функції виявлення порушень таким чином.

Параметрм, які виявляються корисними при виявленні порушень за профілем поведінки, є такі.

- Лічильник (counter).
- Датчик (gauge)
- Інтервальний таймер (interval timer)
- Показник використання ресурсу (resource utilization)

З цими кількісними показниками можна використовувати різні тести для з'ясування правомірності поточної діяльності користувача. При цьому можна використовувати такі методи:

- метод середніх значень і середньоквадратичних відхилень;
- метод багатовимірної моделі;
- метод марківських процесів;
- метод часових рядів;
- операторний метод.

Виявлення порушників (5)

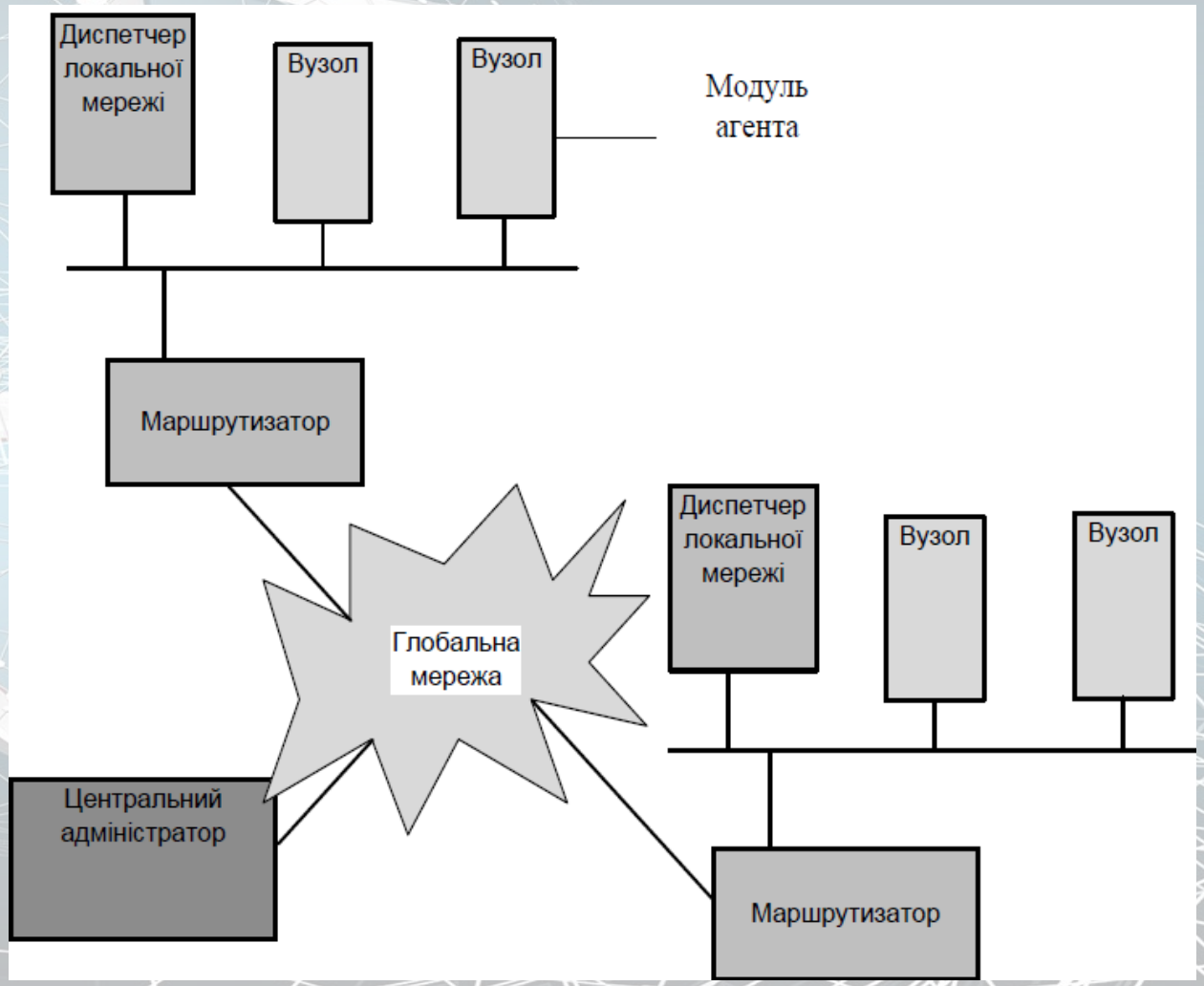
Критерії, використовувані для виявлення порушень

Критерій	Модель	Тип порушень
Вхід до системи і сеанс роботи користувача		
Частота входів до системи по днях і годинах	Середні значення і середньоквадратичні відхилення	Порушники, найімовірніше, намагаються увійти до системи в неробочий час
Час, що пройшов з моменту останнього входу до системи	Операторна модель	Спроба вторгнення до системи за "нічийним" обліковим записом
Тривалість сеансів роботи	Середні значення і середньоквадратич- не відхилення	Значні відхилення можуть означати роботу імітатора
Обсяг даних, що пересилаються в певне місце	Середні значення і середньоквадратич- не відхилення	Дуже великі обсяги даних, передані на видалені вузли, можуть означати просочування важливої інформації
Показник використання ресурсів під час сеансу	Середні значення і середньоквадратич- не відхилення	Показники завантаження процесора або пристроїв введення-виведення, що виходять за рамки звичайних, можуть означати роботу порушника
Число введень неправильних значень пароля при реєстрації	Операторна модель	Спроби проникнення до системи за допомогою вгадування пароля
Невдалі спроби входу до системи з певних терміналів	Операторна модель	Спроби вторгнення до системи
Виконання команд або програм		
Частота запуску програм	Середні значення і середньоквадратич- не відхилення	Може вказувати на присутність порушника, який пробує доступні йому команди, чи на легального користувача, що дістав доступ до привілейованих команд
Використання ресурсів програмами	Середні значення і середньоквадратич- не відхилення	Значення, що виходить за рамки звичайного, може означати впровадження вірусу або троянського коня, які у фоновому режимі виконують операції, які збільшують завантаження системи введення-виведення або процесора
Число відмов виконання	Операторна модель	Може означати спроби легального користувача одержати привілеї вищого рівня
Доступ до файлів		
Частота виконання операцій читання, запису, створення, видалення	Середні значення і середньоквадратич- не відхилення	Частота, що виходить за рамки звичайної, операцій доступу до файлів для читання і запису може означати присутність імітатора або перегляд ресурсів
Підрахунок невдалих спроб читання, запису, створення	Операторна модель	Можуть виявляти користувачів, які постійно намагаються дістати несанкціонований доступ до файлів

Розподілені системи виявлення порушень (1)

На рисунку показана загальна архітектура розподіленої системи виявлення порушень, що складається з таких трьох основних компонентів:

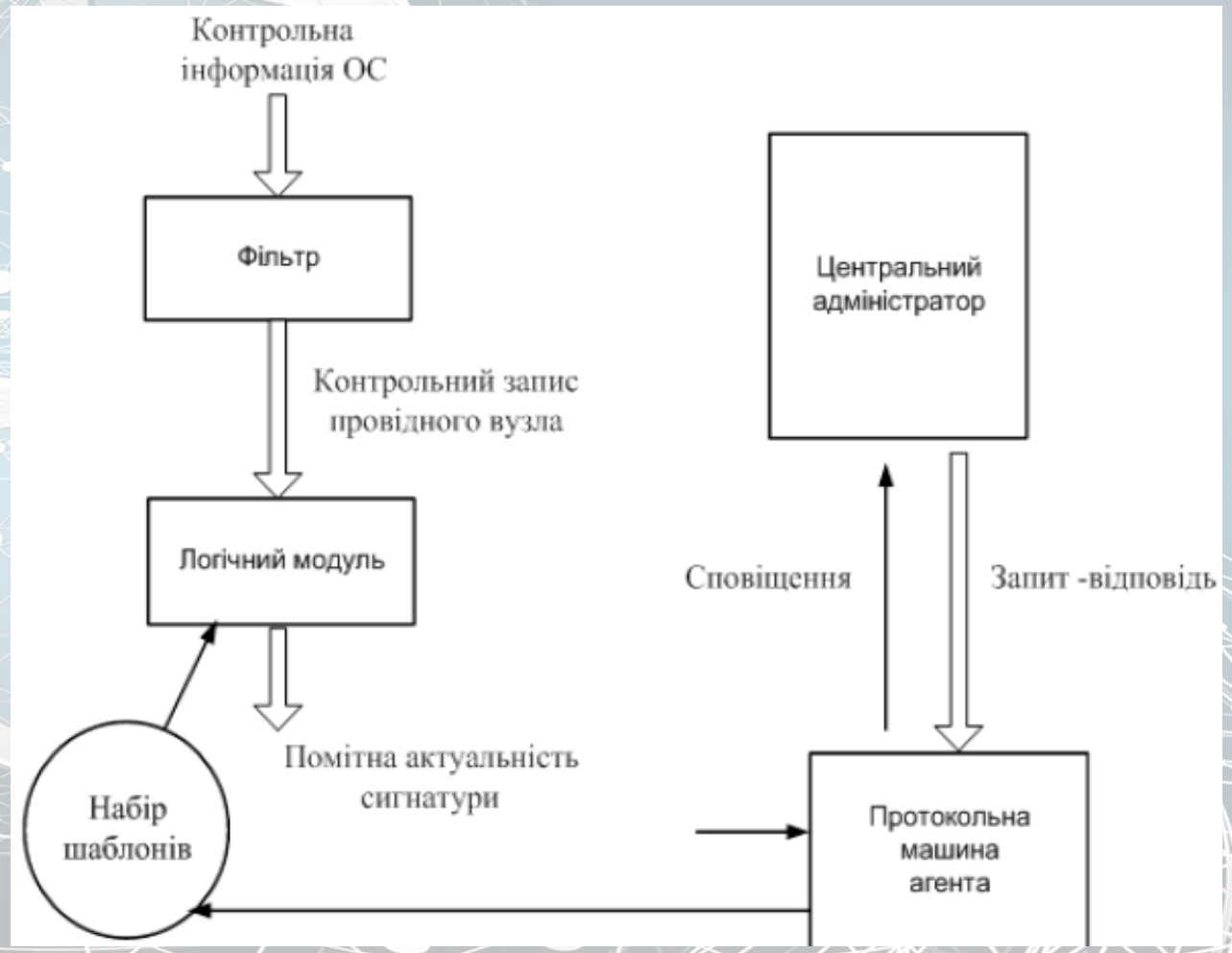
- Модуль агента вузла – це модуль збирання контрольної інформації, що виконується у фоновому режимі в системі, за якою ведеться спостереження.
- Робота модуля агента диспетчера локальної мережі аналогічна роботі модуля агента вузла, але даний модуль аналізує потік даних локальної мережі, теж передаючи одержані дані модулю центрального адміністратора.
- Модуль центрального адміністратора приймає повідомлення, що надходять від агентів вузлів і агента диспетчера локальної мережі, обробляє ці повідомлення, з'ясовуючи їх кореляцію і намагаючись виявити порушення.



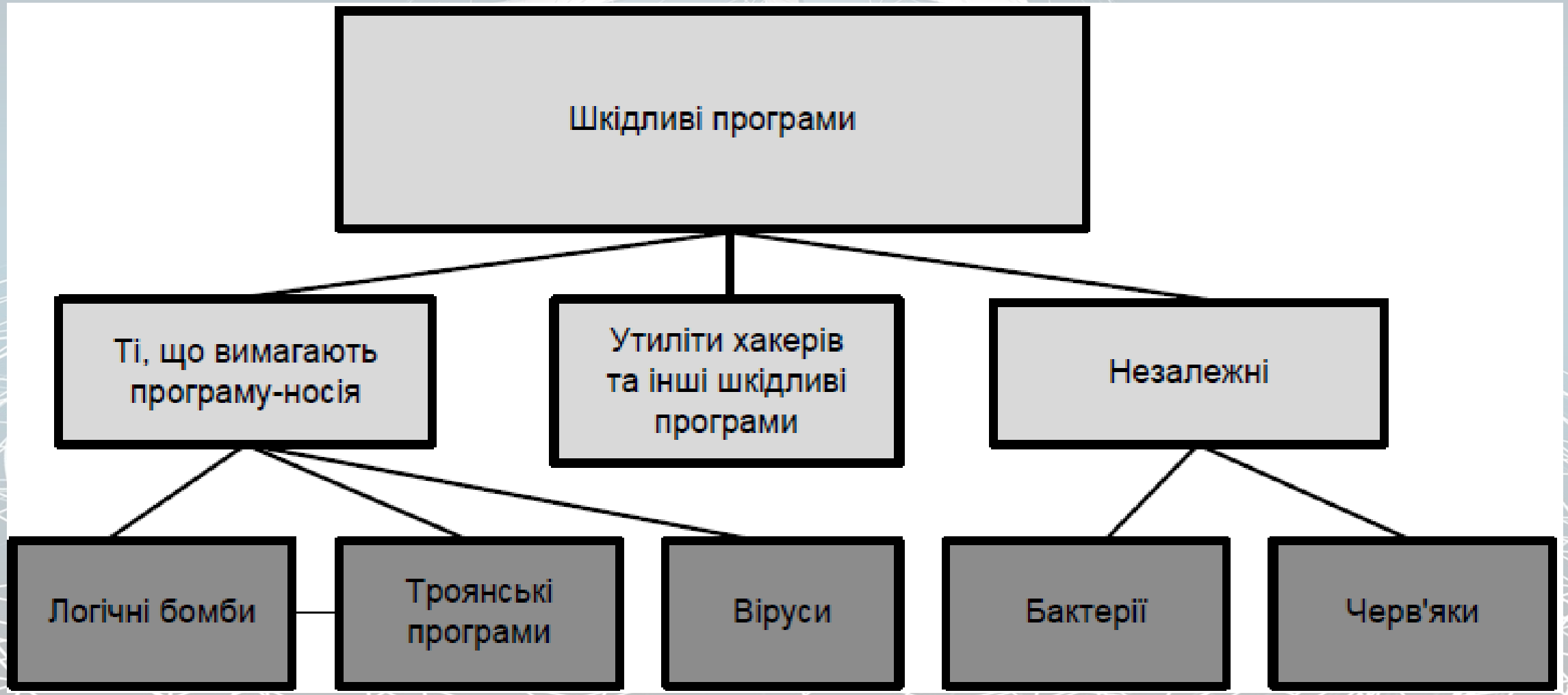
Розподілені системи виявлення порушень (2)

На рис. показана схема загального підходу, що застосовувався в випадку незалежною від операційної системи і конкретних реалізацій системи контролю.

- Агент переглядає кожен контрольний запис, породжений системою реєстрації контрольних параметрів відповідної системи. Записи, що не мають інтересу з погляду захисту, фільтруються. Записи, що залишилися, перетворяться в стандартний формат контрольного запису головного вузла
- Модуль агента диспетчера локальної мережі теж надає зібрані їм дані модулю центрального адміністратора



Класифікація програмних загроз



Основні види програмних загроз

- Комп'ютерний вірус – це програма, що викликає порушення роботи інших програм, псування інформації, неможливість прочитати файли, уповільнення або нестабільність роботи комп'ютера.
- Логічна бомба є програмним кодом, упровадженим в якусь корисну програму, який повинен "вибухнути" при виконанні певних умов.
- ArcBomb – “бомби” в архівах. Є архіви, спеціально оформлені так, щоб викликати нештатну поведінку архіваторів при спробі розархівувати дані – зависання або істотне уповільнення роботи комп'ютера або заповнення диска великою кількістю “порожніх” даних.
- Троянські програми здійснюють різні несанкціоновані користувачем дії: збір інформації і її передачу зловмиснику, її руйнування або зловмисну модифікацію, порушення працездатності комп'ютера, використання ресурсів комп'ютера в незаконних цілях.

Троянські програми

- Backdoor – троянські утиліти видаленого адміністрування.
- Trojan-PSW – це програма, яка викрадає паролі.
- Trojan-AOL – родина троянських програм, що “крадуть” коди доступу до мережі AOL (America Online). Виділені в особливу групу внаслідок своєї чисельності.
- Trojan-Clicker (інтернет-клікери) – родина троянських програм, основна функція яких – організація несанкціонованих звернень до інтернет-ресурсів (зазвичай до веб-сторінок).
- Trojan-Downloader – троянські програми, призначені для завантаження і установки на комп'ютер-жертву нових версій шкідливих програм, установки “трояна” або рекламних систем.
- Trojan-Dropper – це інсталятори інших шкідливих програм.
- Trojan-Proxy (троянські проксі-сервери) – це родина троянських програм, що приховано здійснюють анонімний доступ до різних інтернет-ресурсів. Зазвичай використовуються для розсилки спаму.
- Trojan-Spy – це шпигунські програми.

Ознаки комп’ютерних вирусів

Типи комп'ютерних вірусів розрізняються за такими основними ознаками:

- середовище проживання, можна розділити:
  - на файлові;
  - на завантажувальні;
  - на макровіруси;
  - на скриптові.
- спосіб зараження, поділяються:
  - на ті, що перезаписують (overwriting);
  - на паразитичні (parasitic);
  - на віруси-компаньйони (companion);
  - на віруси-посилання (link);
  - на віруси, що заражають об'єктні модулі (OBJ);
  - на віруси, що заражають бібліотеки компіляторів (LIB);
  - на віруси, що заражають початкові тексти програм.

Інші види комп’ютерних вирусів

- Скрипт-віруси (віруси скрипта) – це підгрупа файлових вірусів, які написані на різних мовах скрипта (VBS, JS, BAT, PHP і та ін.). Вони або заражають інші програми (командні і службові файли MS Windows або Linux) скрипта, або є частинами багатокомпонентних вірусів.
- Бактерії є програмами, які не ушкоджують, самі по собі, жодних файлів. Єдиною метою "бактерії" є відтворення собі подібних.
- Мережевий черв'як – це різновидність шкідливої програми, яка самостійно розповсюджується комп’ютерною мережею.
  - Email-Worm поштові черв'яки для свого розповсюдження використовують електронну пошту.
  - IM-Worm – це черв'яки, що використовують інтернет-пейджери.
  - Окрему категорію становлять черв'яки, що використовують для свого розповсюдження веб- і FTP-сервера.
  - Існують мережеві черв'яки, які паразитують на інших черв'яках та/або троянських програмах віддаленого адміністрування (бекдорах).
  - Також існують складніші P2P-черв'яки, які імітують мережевий протокол конкретної файлообмінної системи і на пошукові запити відповідають позитивно

ПЗ для комп’ютерних вирусів

До категорії утиліт хакерів та інші шкідливі програми належать:

- утиліти автоматизації створення вірусів, черв'яків і троянських програм (конструктори);
- програмні бібліотеки, розроблені для створення шкідливого ПЗ;
- утиліти приховання коду заражених файлів від антивірусної перевірки (шифрувальники файлів);
- “злі жарти”, що ускладнюють роботу з комп'ютером;
- програми, що свідомо повідомляють користувачу помилкову інформацію про свої дії в системі;
- інші програми, які тим або іншим чином навмисно завдають прямого або непрямого збитку даному або віддаленим комп'ютерам.

Інші шкідливі програми

- DoS, DDoS мережеві атаки – це програми , які реалізують віддалені атаки на сервери, посилаючи на них численні запити, що призводить до відмови в обслуговуванні, якщо ресурси сервера, що атакується, недостатні для обробки всіх запитів, що надходять (DoS = Denial of Service).
- Flooder (“засмічення” мережі) – це утиліти хакерів, які використовуються для “забивання сміттям” (непотрібними повідомленнями) каналів Інтернету – IRC-каналів, комп'ютерних пейджингових мереж, електронної пошти і та ін.
- Nuker фатальні мережеві атаки – це утиліти, що відправляють у мережі спеціально оформлені запити на комп'ютери, що атакуються, внаслідок чого система, яка атакується, припиняє роботу.
- Bad-Joke, Hoax (злі жарти, введення користувача в оману) – це програми, які не завдають комп'ютеру жодної прямої шкоди, однак виводять повідомлення про те, що таку шкоду вже завдано або буде завдано за певних умов, або попереджають користувача про неіснуючу небезпеку.
- FileCryptor, PolyCryptor (приховання від антивірусних програм) – це утиліти хакерів, що використовуються для шифрування інших шкідливих програм з метою приховання їх вмісту від антивірусної перевірки.
- PolyEngine (поліморфні генератори) не є вірусами у прямому розумінні цього слова, оскільки до їх алгоритму не закладаються функції розмноження, тобто відкриття, закриття і записи у файли, читання і записи секторів і та ін.

Життєвий цикл типового вірусу

1. Інкубаційний період. Вірус ніяк не виявляється. Врешті-решт вірус буде активізовано певною подією, наприклад, настанням певної дати, присутністю іншої програми або файлу, появою достатнього місця на диску. Інкубаційний період мають не всі віруси.

2. Фаза розповсюдження. Вірус поміщає свою копію до інших програм або в певні системні ділянки на диску. Тепер усі інфіковані програми міститимуть копію вірусу, кожна з яких теж повинна буде коли-небудь пройти свою фазу розповсюдження.

3. Фаза активізації. Вірус активізується для виконання функції, заради якої він створювався. Фаза активізації може бути ініційована самими різними системними подіями, наприклад, наявністю певного числа копій даного вірусу в системі.

4. Фаза виконання. Виконується функція, що міститься у вірусі. Ця функція може бути як цілком нешкідливою (наприклад, виведення повідомлення на екран), так і деструктивною (наприклад, знищення програм і файлів з даними).

Структура вірусу (1)

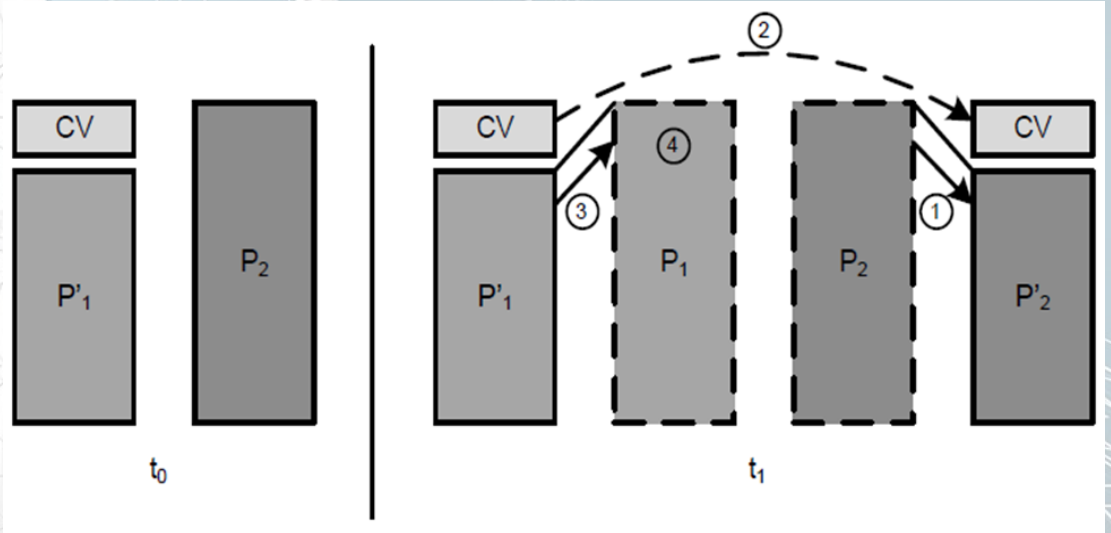
Вірус може бути розміщений на початку або в кінці виконуваної програми, а також вбудовуватися іншим чином. Головна ідея роботи вірусу полягає в тому, щоб при запуску програми-носія спочатку виконався код вірусу і лише потім – код самої програми. У найзагальніших рисах структуру вірусу показано на рис.

```
program V :=
{goto main; 1234567;
subroutine infect-executable :=
{loop:
file :5 get-random-executable-file;
if (first-line-of-file 5 1231567) then goto loop
else prepend V to File;} subroutine do-damage :=
{whatever damage is to be done} subroutine trigger-pulled :=
{return true if some condition holds} main;          main-program :=
{infect-executable;
if trigger-pulled then do-damage; goto next;}
next:
}
```

Структура вірусу (2)

Щоб обійти такі прості методи виявлення, вірус повинен стиснути виконуваний файл, аби інфікована та неінфікована версії файлу були однакової довжини. На рис. показана загальна логіка роботи такого вірусу.

```
program CV :=
{goto main; 01234567;
subroutine infect-executable :=
{loop:
file := get-random-executable-file;
if (first-line-of-file = 01234567) then
                goto loop; compress file;
prepend CV to file;
}
main: main-program :=
{if ask-permission then infect-executable;
uncompress rest-of-file;
run uncompressed file;)
}
```



Антивірусний захист

Ідеальним розв’язанням проблеми вірусів є запобігання інфікуванню: не слід допускати початкового проникнення вірусу до комп'ютерної системи. Для цього потрібно виконати такі вимоги:

- Своєчасне виявлення. Якщо зараження відбулося, воно повинне бути негайно виявлене зі встановленням місцезнаходження вірусу.
- Ідентифікація. Як тільки зараження виявлене, необхідно ідентифікувати тип вірусу, що інфікував програму.
- Видалення. Як тільки вірус ідентифіковано, слід видалити всі сліди вірусу з інфікованих програм і відновити в їх початковому вигляді. Важливо видалити вірус з усіх інфікованих систем, щоб хвороба не розповсюджувалася далі.

Антивірусні програми розділяються на чотири покоління.

1. Перше покоління: звичайні сканери.
2. Друге покоління: евристичні аналізатори.
3. Третє покоління: монітори.
4. Четверте покоління: повнофункціональні системи захисту.

Визначення спаму

Останнім часом почастішали скарги користувачів на збільшення небажаної електронної кореспонденції рекламного характеру. Такі листи називаються в мережі спамом.

Ось найбільш точне визначення спаму: спам – це анонімна, масова, незапитана розсилка.

Деякі приклади небажаної пошти, яку одержувач не замовляв та/або не бажає одержувати:

- Різного роду помилки: автоматичних розсильників – технічний перебій служби розсилки, запити на підтвердження підписки на розсилку або якийсь сервіс; помилки людей, наприклад, людина шукає однокурсника, а одержувач має схоже прізвище і адресу.
- Різноманітна технічна кореспонденція: повідомлення про невідправку листа й інші помилки; автоматичні повідомлення від антивірусних програм про віруси у відправленому з вашої адреси листі; екстраординарні або рутинні повідомлення від адміністраторів сервісів (наприклад, про те, що поштовий сервіс буде недоступний, або про появу вірусу і ін.). Такі листи для одержувача часто виглядають як незапитані.
- Нові можливості спілкування і бізнесу: діловий лист від приватної особи (фірми) приватній особі (фірмі). Такий лист часто може служити початком нового контракту, справи, бізнесу. Прямий лист менеджеру корпорації від рекрутингового агентства – адресу, звичайно, одержано неофіційно, сам лист справедливо трактується компанією як загроза бізнесу, в той же час такі листи дуже корисні для ринку праці і капіталу.

Методи боротьби із спамом (1)

Можна визначити активні і пасивні методи захисту. Пасивні методи захисту включають якісь профілактичні заходи, що дозволяють не допустити попадання вашої поштової адреси до спамера.

Спамери знаходять email-адреси своїх жертв різними способами:

- скануючи веб-сайти;
- скануючи дошки оголошень, форуми, чати, Usenet News і так далі;
- підбираючи “легкі” адреси (jonh@, mary@, alex@, info@, sales@, support@) за словником імен і часто вживаних слів;
- підбираючи “короткі” адреси (aa@, an@, bb@, abc@) простим перебором.

Методи боротьби із спамом (2)

Рекомендації приватному користувачу:

- Заведіть собі дві адреси – приватну, для листування (маловідому, яку ви ніколи не публікуєте в загальнодоступних джерелах), і публічну – для публічної діяльності (форумів, чатів і так далі).
- Адреса для листування ніколи не повинна публікуватися у відкритому доступі.
- Адреса для листування не повинна бути легкою в запам'ятовуванні або “красивою”. Ваше ім'я або красиве слово – не підходять. Vasily.M.Pupkin-IV – підходить цілком. Чим довша адреса і чим менш вона легка для читання, тим краще.
- Якщо потрібно повідомити свою приватну адресу (у конференції, на сайті), робіть це способом, непридатним для автоматичного прочитання складальником адрес. “Ivan-точка-Susanin-собака-mail-точка-ру” – хороший спосіб. “Ivan.Susanin at mail.ru” –набагато гірше, Ivan.Susanin@mail.ru – нікуди не годиться. Якщо йдеться про публікацію на сайті, можна опублікувати адресу у вигляді картинки.
- Адресу для публікації потрібно наперед вважати тимчасовою.
- При реєстраціях завжди указуйте публічну адресу.
- Ніколи не відповідайте спамеру.
- Не намагайтеся скористатися посиланням “відписатися”, якщо ви не упевнені, що вона спрацює.
- Якщо миритися зі спамом вже ніяк не можна, то змініть свою приватну адресу.
- Використовуйте антиспам-фільтр
- Лінію оборони можна організувати на базі вашого ж провайдера.

Сучасні технології спамерів

1. Збирання і верифікація email-адрес одержувачів. Класифікація адрес за типами.
2. Підготовка “точок розсилки” – комп'ютерів, через які розсилатиметься спам.
   - пряма розсилка з орендованих серверів;
   - використання “відкритих релеїв” і “відкритих proxy” – сервісів, помилково конфігурованих їх власниками таким чином, що через них можна розсилати спам;
   - прихована установка на призначених для користувача комп'ютерах програмного забезпечення, що дозволяє несанкціонований доступ до ресурсів даного комп'ютера (бекдорів).
3. Створення програмного забезпечення для розсилки.
4. Пошук клієнтів.
5. Створення рекламних оголошень для конкретної розсилки.
6. Створення розсилки.

Тематики спаму та його шкідливість

Властивості спаму:

- Спам не має мовних меж.
- Спам дуже різноманітний.
- “Нігерійськими листами”

Лідируючі тематики спаму:

- спам “для дорослих”;
- здоровий спосіб життя і медикаменти;
- комп'ютери й Інтернет;
- особисті фінанси;
- освіта.

Чим шкідливий спам:

- зниженням продуктивності компанії;
- неконтрольованою втратою важливих повідомлень при ручному чищенні електронної пошти;
- загрозою стабільності роботи поштових серверів;
- небезпечним змістом: вірусами, троянами, забороненими законом матеріалами. В наш час 75–90 % вхідних повідомлень є спамом. Це означає, що три чверті свого дискового простору і процесорної потужності поштовий сервіс витрачає зараз на обслуговування бізнесу спамерів!;
- паразитним трафіком;
- для провайдерів – витратами на службу підтримки, конфліктами з клієнтами.

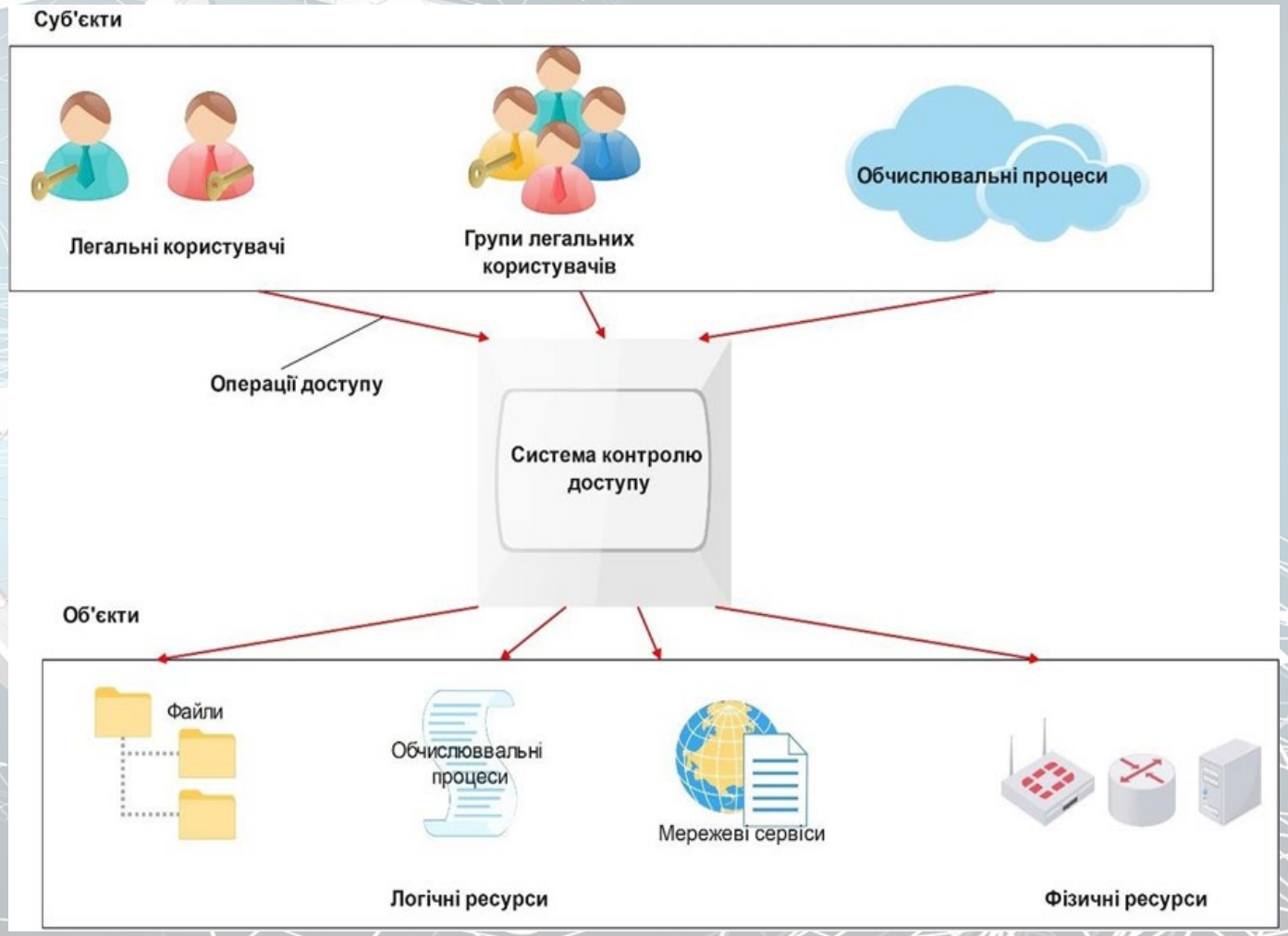
Контрольні запитання

1. Дайте класифікацію порушників.
2. Перерахуйте методи отримання паролів.
3. Які методи протидії порушникам існують?
4. Проілюструйте схему використання паролів у системі UNIX.
5. Які стратегії вибору паролів?
6. Перерахуйте причини необхідності виявлення порушників.
7. Проілюструйте профілі поведінки порушників.
8. Які підходи до розв'язання проблеми виявлення порушників?
9. Проілюструйте розподілену систему виявлення порушень.
10. Наведіть класифікацію програмних загроз.
11. Наведіть приклади троянських програм, логічних бомб та класичних вірусів.
12. Який життєвий цикл типового вірусу?
13. Опишіть просту процедуру роботи вірусу, що використовує стиснення.
14. Які антивірусні програми ви знаєте?
15. Дайте визначення спаму.
16. У чому відмінність спаму від цільових комерційних пропозицій і небажаної пошти?
17. Перерахуйте методи боротьби зі спамом.

ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ І УПРАВЛІННЯ ДОСТУПОМ

Ідентифікація, автентифікація і авторизація

- Ідентифікація – це присвоєння об’єктам і суб’єктам інформаційної системи унікальних імен – ідентифікаторів.
- Автентифікація – це процедура підтвердження суб’єктом/об’єктом того, що він є те (тим), за що (кого) він себе видає.
- Авторизація – це процедура контролю доступу суб’єктів (користувачів, обчислювальних процесів, пристроїв) до об’єктів (файлів, додатків, сервісів, пристроїв) і надання кожному із них саме тих прав, які для них визначені правилами доступу.



Ідентифікація, автентифікація і авторизація

Аспекти проблеми аутентифікації.

- Завдання аутентифікації користувача - це користувач, який має доступ до певних ресурсів системи, яким він стверджує?
- Завдання справжності станції полягає в тому, чи є станція, яка відповіла на запит користувача, саме такою, як вона називається?
- Завдання аутентифікувати повідомлення - чи відповідає повідомлення, відправлене через канали, його початковому вигляду?

Фактори автентифікації людини

Автентифікатори, які використовуються при цьому, поділяють на три класи:

- «щось, що знаю» – до цього типу належать багаторазові й одноразові паролі, правила перетворення інформації;
- «щось, що маю» – різні мініатюрні пристрої, які називаються апаратними автентифікаторами/ключами;
- «щось, чим я є» – різні біометричні показники автентифікованого.

Автентифікація на основі паролів

Пароль - це рядок символів, який користувач повинен ввести в систему будь-яким способом (введення, набір на клавіатурі і т.д.).

- Найпоширенішим методом аутентифікації
- Головна перевага аутентифікації пароля - простота і звичність.
- Надійність пароля заснована на здатності запам'ятовувати їх і тримати в таємниці.

Типи паролів

- Простий пароль.
- Одноразовий пароль.
- Пароль на основі зразка символів.
- Метод запиту-відповіді
- Пароль на основі алгоритму

При роботі з паролями рекомендуються наступні правила створення:

- Не друкуйте паролі та не відображайте їх на екрані.
- Кожен користувач повинен зберігати свій пароль і не дозволяти незнайомцям про це знати.
- Завжди шифруйте паролі та захищайте їх недорогими та ефективними інструментами.
- Переконайтеся, що в роздруківці немає паролів
- Не записувати паролі на столі, стіні або терміналі. Зберігайте його в пам'яті
- Виберіть пароль, який важко вгадати: спробуйте використовувати малі і великі літери, цифри, або виберіть знамениту приказку і візьміть звідти кожну четверту букву. Ще краще, нехай ваш комп'ютер сам згенерує ваш пароль; Не використовуйте пароль, який є вашою адресою, псевдонімом, ім'ям дружини, номером телефону або чимось очевидним
- Вправильно вибрати довжину пароля - чим він довший, тим вище ступінь безпеки забезпечить система, так як важче буде вгадати пароль.

Правила адміністрування паролів

- періодично змінювати паролі та не робити цього за розкладом
- зашифрувати або виконати інші дії з файлами паролів, які зберігаються на комп ' ютері, щоб захистити їх від несанкціонованого доступу.
- обмеження кількості невдалих спроб входу (це ускладнить використання методу грубої сили);
- Призначення лише найнадійнішої особи адміністратором паролів
- Обмеження доступу до файлу паролів
- Не використовувати однаковий пароль для всіх працівників групи
- Змінення паролів під час виходу користувача з програми
- змусити користувачів підписувати паролі
- встановити і впровадити правила паролів і переконатися, що всі знають їх

Стійкість захисту паролем

- Середній час безпеки
  $T_b = (d*C/R)*S^{L/2}$
- Кількість спроб пароля в часі T, $N_2=T/(d*C/R)=(T*R)/(d*C)$.
- Нижня межа для ймовірності P
  $P_o=N_2/S^L = (T*R)/(d*C*S^L)$
- Ймовірність порушення безпеки
  $P>=(T*R)/(d*C*S^L)$
- Оскільки $S^L = (T*R)/(P_o*d*C)$, то довжина паролю
  $L= [\log(T*R)-\log(P_o*d*C)]/ \log(S)$
- взаємозв'язок між часом, доступним потенційному «зломщику», і іншими параметрами системи захисту
  $T = P*S^L * d*(C/R)$

Порівняння стійкості паролів

Множина символів	Кількість комбінацій		Час підбору паролю	
	6 знаків	8 знаків	6 знаків	8 знаків
Цифри від 1 до 9	1 мільйон комбінацій	100 мільйонів комбінацій	Практично миттєво	10 секунд
26 лише великих або лише малих літер латинського алфавіту	309 мільйонів комбінацій	200 мільярдів комбінацій	30 секунд	Менше 6 год. (в 720 разів довше, ніж для 6 знаків)
Поєднання 52 великих і малих літер латинського алфавіту	19 мільярдів комбінацій	53 трильйона комбінацій	Півгодини	Два місяці (майже в 3000 раз довше, ніж для 6 знаків)
Великі і малі літери, цифри і всі символи	782 мільярди комбінацій	7,2 квадрильйона комбінацій	22 години	57 років (приблизно в 22700 раз довше, ніж для 6 знаків)

Способи захисту паролів

- Найпростіший спосіб - зашифрувати таблицю паролів
- Використовувати "одноразові" паролі
- Кодування паролів, заснований на ідеї «особистого фізичного ключа»
- Використання систем з відкритими ключами

Критерії	Метод не потребує запам'ятовування	Перешкоджання виділеному фрагменту	Легко піддається обробці	Запобігає перехопленню та копіюванні	Не становить загрози злому шифрування	Запобігає обману	Можливість реалізації негайно	Відносна вартість реалізації
Шифрування паролів			+				+	Низьким
Одноразові паролі				+		+	+	Середній
Магнітні карти	+	+	+		+		+	Середній
Особисті ключі			+		+		+	Низьким
Відкрити ключі з динамічним паролем	+	+	+	+	+	+		Висока

Токен

- це об'єкт (пристрій), який підтверджує справжність користувача.

Види токенів

- Картки з магнітною смугою
- Інтелектуальні токени
  - Статичний обмін паролями
  - Динамічне створення пароля
  - Системи запиту-відповіді

Поряд з безсумнівними перевагами, токени пам'яті мають певні недоліки. Перш за все, вони значно дорожчі за паролі. Вони повинні бути зроблені, розподілені для користувачів, що об'ївться випадками втрати. Їм потрібні спеціальні пристрої для читання. Вони не дуже зручні у використанні, особливо якщо організація створила інтегровану систему безпеки.

Біометрична «природня» автентифікація

Біометрична автентифікація – це процес доказу і перевірки автентичності заявленого користувачем імені, через пред’явлення користувачем свого біометричного образу і шляхом перетворення цього образу відповідно до заздалегідь визначеного протоколу автентифікації

В даний час широко використовується велика кількість методів біометричної автентифікації, які поділяються на два класи.

- Статичні методи біометричної автентифікації засновані на фізіологічних характеристиках людини, присутніх від народження і до смерті, що знаходяться при ньому протягом всього його життя, і які не можуть бути втрачені, вкрадені і скопійовані.
- Динамічні методи біометричної автентифікації ґрунтуються на характерних підсвідомих рухах людини в процесі відтворення або повторення будь-якої звичайної дії.

Статичні та динамичні методи біометричної автентифікації

Статистичні методи

- Ідентифікація за відбитками пальців
- Автентифікація по сітківці ока
- Автентифікація по геометрії руки
- Автентифікація по геометрії обличчя
- Автентифікація по термограмі обличчя

Динамічні методи

- Автентифікація по голосу
- Автентифікація по рукописному почерку

«Природні» характеристики

Біометричний параметр	Біологічне повторення об'єкта	Функції	
		Позитивний фактор	Негативний фактор
Долоня	<2%	• Стійкість параметру • Простота алгоритму • Малий ідентифікаційного коду	• Громіздкий зчитувач розраховується для правій руці • Використовується тільки з PIN-кодом • Прямий контакт з обладнанням
Відбитків пальців	$<10^{-5}$ %	• Стійкий варіант • Компактний зчитувач • Малий ідентифікаційний код • Складність підроблення • Можливість пошуку за масивом даних • Привичне використання	• Складність алгоритмів ідентифікації • Прямий контакт з обладнанням
Сітківка ока	$<10^{-10}$ %	• Надзвичайна складність підробки • Відсутність прямого контакту з обладнанням • Можливість пошуку по базі даних	• Складність читання • Мінливість фактичного ідентифікаційного параметра • Складність алгоритмів ідентифікації • Дискомфорт від думки про шкідливий вплив на зір

Протоколи автентифікації віддалених користувачів

Для забезпечення надійної автентифікації віддалених користувачів потрібне виконання наступних вимог:

- проведення автентифікації обох взаємодіючих сторін – як віддаленого користувача, так і сервера віддаленого доступу – для виключення маскування зловмисників;
- оперативне узгодження використовуваних протоколів автентифікації;
- здійснення динамічної автентифікації взаємодіючих сторін в процесі роботи віддаленого з'єднання;
- застосування криптозахисту переданих секретних паролів або механізму одноразових паролів для виключення перехоплення і несанкціонованого використання автентифікуючої інформації.

Протокол PPP має вбудовані засоби, які можуть бути використані для організації автентифікації при віддаленій взаємодії. У стандарті RFC 1334 визначено два протоколи автентифікації:

- протокол автентифікації по паролю (Password Authentication Protocol, PAP);
- протокол автентифікації по «рукостисканню» (Challenge Handshake Authentication Protocol, CHAP).

Протокол PAP

Протокол PAP є простим методом перевірки достовірності віддаленого пристрою.

Для налаштування автентифікації в каналі PPP необхідно виконати наступні команди:

1. В режимі глобального конфігурування за допомогою команди username ім’я password пароль задати ім’я користувача і пароль. Це ім’я має точно і з урахуванням регістру збігатися з ім’ям вузла віддаленого маршрутизатора.

Left(config)#username Right password sameone

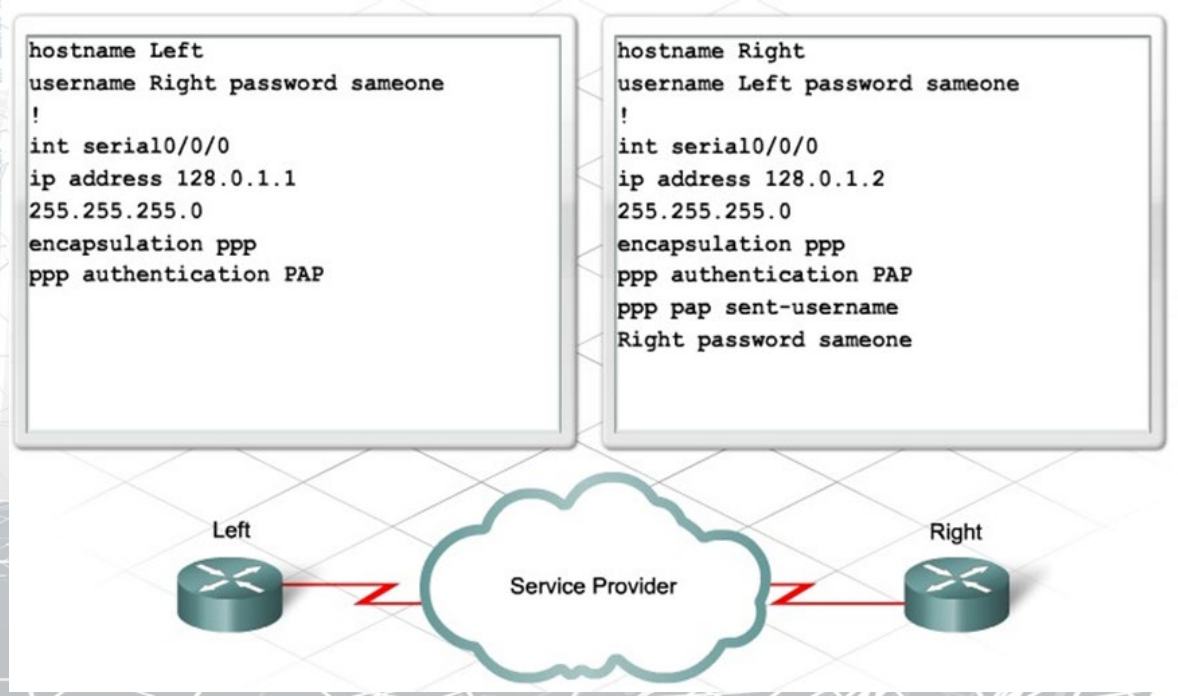
2. В режимі конфігурування інтерфейсу задати тип автентифікації за допомогою команди:
ppp authentication {chap | chap pap | pap chap | pap}.

3. Якщо вказано кілька типів, наприклад, chap pap, маршрутизатор спочатку пробує використовувати перший з перерахованих типів, і, тільки якщо віддалений маршрутизатор пропонує, пробує використовувати другий тип.

Left(config)#interface serial 0/0/0

Left(config-if)#ppp authentication pap

У протоколі CHAP використовується секретний статичний пароль. На відміну від протоколу PAP, в протоколі CHAP пароль кожного користувача для передачі по лінії зв’язку шифрується на основі випадкового числа отриманого від сервера.



Протокол CHAP

Для ініціалізації процесу автентифікації по протоколу CHAP сервер віддаленого доступу після встановлення сеансу зв’язку повинен вислати віддаленому комп’ютеру пакет LCP, що вказує на необхідність застосування протоколу CHAP, а також необхідного алгоритму хешування. Якщо віддалений комп’ютер підтримує запропонований алгоритм хешування, то він повинен відповісти пакетом LCP про згоду із запропонованими параметрами. Інакше виконується обмін пакетами LCP для узгодження алгоритму хешування.

Після цього починається автентифікація на основі обміну пакетами протоколу CHAP.

У протоколі CHAP визначені пакети чотирьох типів:

- Виклик (Challenge);
- Відгук (Response);
- Підтвердження (Success);
- Відмова (Failure).

Протокол S/Key

Одним з найбільш поширених протоколів автентифікації на основі одноразових паролів є стандартизований в Інтернеті протокол S/Key (RFC 1760). Цей протокол реалізований в багатьох системах, що вимагають перевірки достовірності віддалених користувачів, зокрема в системі TACACS+ компанії Cisco.

Перехоплення одноразового пароля, що передається по мережі в процесі автентифікації, не надає зловмисникові можливості повторно використовувати цей пароль, оскільки при наступній перевірці достовірності необхідно пред'являти вже інший пароль. Тому, схема автентифікації на основі одноразових паролів, зокрема S/Key, дозволяє передавати по мережі одноразовий пароль у відкритому виді і, таким чином, компенсує основний недолік протоколу автентифікації PAP.

Протокол автентифікації на основі одноразових паролів S/Key застосовують, зокрема, для поліпшення характеристик протоколів централізованого контролю доступу до мережі віддалених користувачів TACACS і RADIUS.

Автентифікація на основі апаратних автентифікаторів (токенів)

Види апаратних автентифікаторів

- Ідентифікатори IButton мають ПЗП, що містить 64-розрядний код, однопровідний порт і схему, яка реалізує логіку управління.
- USB-ключі, або USB-токени, підключаються безпосередньо до USB- порту комп’ютера, виключаючи необхідність використання дорогих зчитувальних пристроїв.
- Смарт-карти (Smart Card – інтелектуальна карта) можуть бути як контактними, так і безконтактними.
- Радіочастотні ідентифікатори, або RFID-ідентифікатори (Radio- Frequency Identification, RFID), виготовляються у вигляді пластикового брелка, що не має ніяких зовнішніх інформаційних входів-виходів, а також ніяких дисплеїв і інших видимих засобів відображення інформації.



IButton



Смарт-карта



USB-ключ



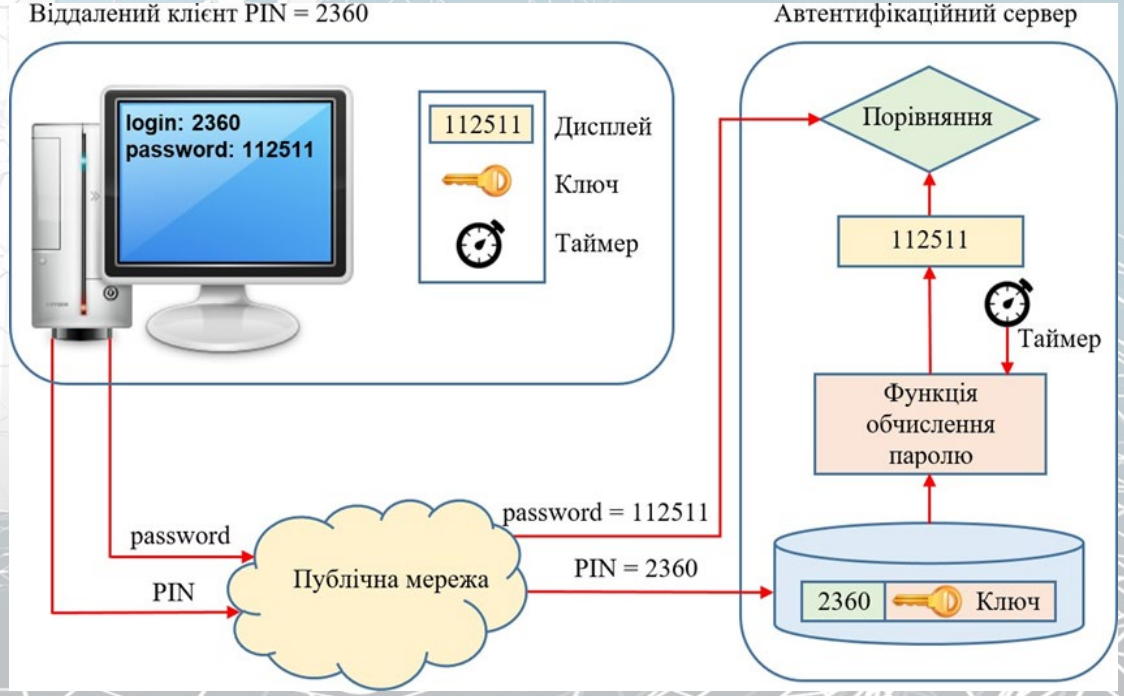
RFID-ідентифікатори

Автентифікація на основі апаратного генератора одноразових паролів

- Алгоритми автентифікації, що базуються на багаторазових паролях, не надто надійні. Паролі можна підглянути, розгадати або просто вкрасти. Більш надійними виявляються схеми на основі програмних або апаратних генераторів одноразових паролів



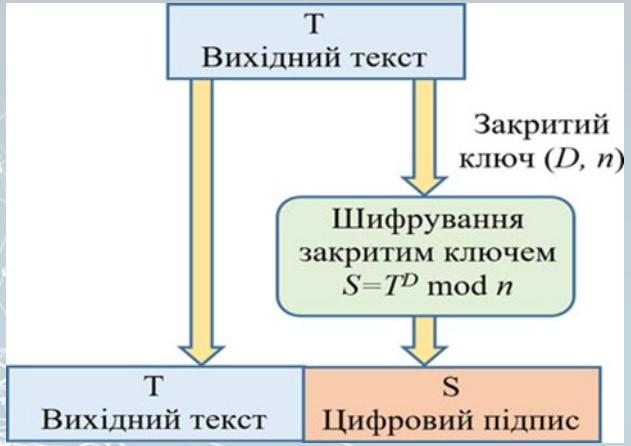
Автентифікація на основі часової синхронізації



Автентифікація інформації. Цифровий підпис

Автентифікація даних може бути вирішена за рахунок електронно-цифрового підпису, а саме:

- підтвердження цілісності даних та програм, що зберігаються і передаються по мережі, тобто встановлення факту того, що вони не піддавалися модифікації;
- доказ авторства повідомлення (документа, програми), в тому числі і для недопущення відмови від авторства;
- доказ легальності придбання програмного забезпечення.



Цифровий підпис S обчислюється за допомогою закритого ключа (D, n) за формулою: $S=T^D \bmod n$

Повідомлення надсилається у вигляді пари (T, S). Кожен користувач, який має відповідний відкритий ключ (E, n), отримавши повідомлення, відокремлює відкриту частину T, розшифровує цифровий підпис S і перевіряє рівність: $T=S^E \bmod n$

Для зменшення «довжини» цифрового підпису замість S=TD mod n використовується формула: $S=(H(T))^D \bmod n$. Тут H(T) – хеш-функція, яка перетворює вихідне повідомлення в короткий дайджест.

Автентифікація на основі цифрових сертифікатів (1)

Автентифікація з застосуванням цифрових сертифікатів є альтернативою застосуванню паролів і видається природним рішенням в умовах, коли число користувачів мережі (нехай і потенційних) вимірюється мільйонами. Сертифікати видаються спеціальними уповноваженими сертифікуючими організаціями (СО) – центрами сертифікації (Certificate Authority, CA).

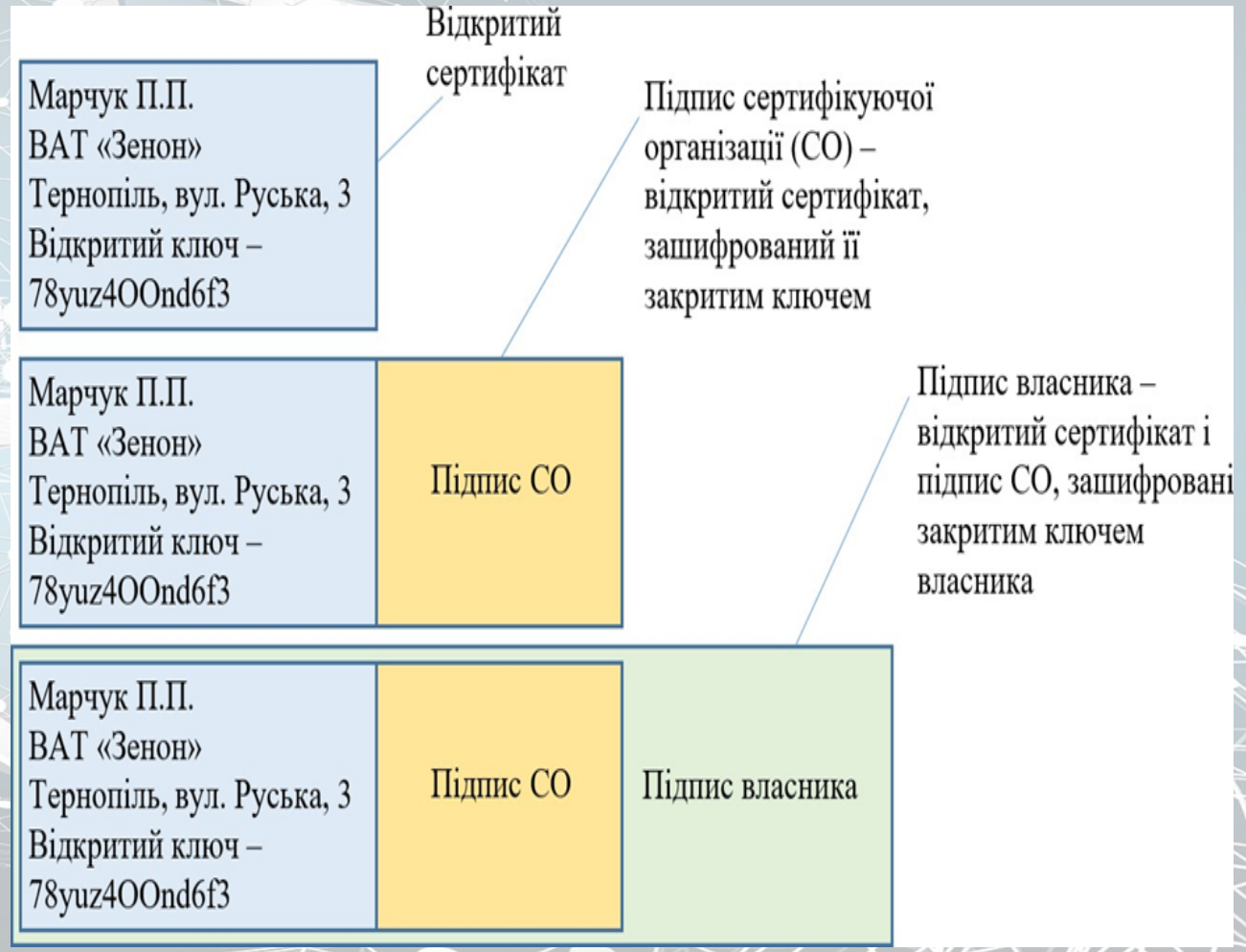
Сертифікат являє собою електронну форму, в якій міститься наступна інформація:

- відкритий ключ власника даного сертифікату;
- відомості про власника сертифіката, такі, наприклад, як ім’я, адреса електронної пошти, найменування організації, в якій він працює, і т. п.;
- назва сертифікуючої організації, що видала цей сертифікат;
- електронний підпис сертифікуючої організації, тобто зашифровані закритим ключем цієї організації дані, що містяться в сертифікаті.

Автентифікація на основі цифрових сертифікатів (2)

Сертифікати можуть бути представлені в трьох формах (рис):

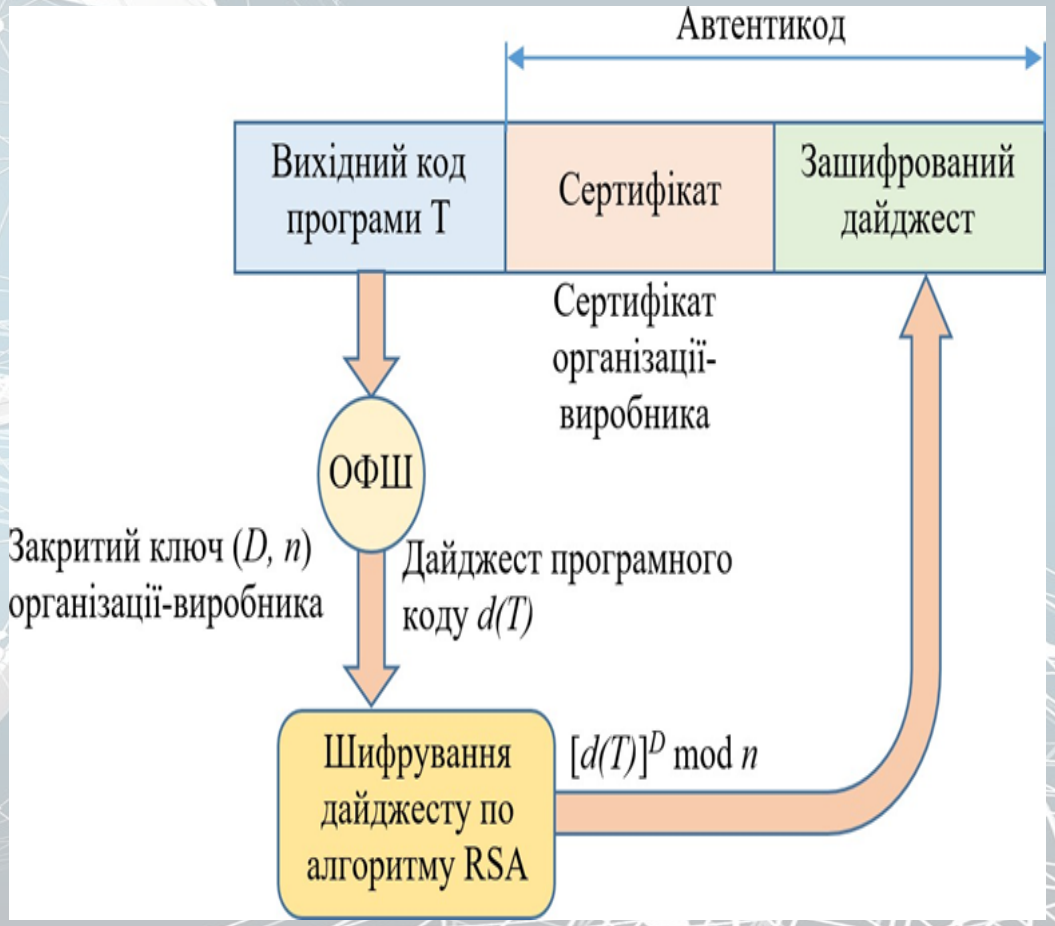
- у відкритій формі сертифікат містить всю інформацію в незашифрованому вигляді;
- в формі з двох частин – відкритій, що містить всю інформацію в незашифрованому вигляді, і закритій, що являє собою відкриту частину, зашифровану закритим ключем сертифікуючої організації;
- в формі з трьох частин – по-перше, відкритій, по-друге, відкритій, але зашифрованій закритим ключем сертифікуючої організації, по- третє, частини, що являє собою перші дві частини, зашифровані закритим ключем власника.



Автентифікація програмних кодів

Цифровий підпис і сертифікати можуть застосовуватися для доказу автентичності (достовірності) програм. Користувачу важливо бути впевненим, що програма, яку він завантажив з будь-якого сервера Інтернету, дійсно містить коди, розроблені певною компанією. Компанія Microsoft запропонувала для цих цілей технологію автентикоду (Authenticode).

Організація, яка бажає підтвердити своє авторство на програму, повинна вбудувати в розповсюджуваний код так званий підписуючий блок – автентикод (рис. 4.7). Цей блок складається з двох частин. Перша частина – це сертифікат організації-розробника даної програми, отриманий звичайним чином від будь-якого центру сертифікації. Другу частину утворює зашифрований дайджест, отриманий в результаті застосування хеш-функції до розповсюджуваного коду. Шифрування дайджесту виконується за допомогою закритого ключа організації.



Форми подання обмежень доступу (1)

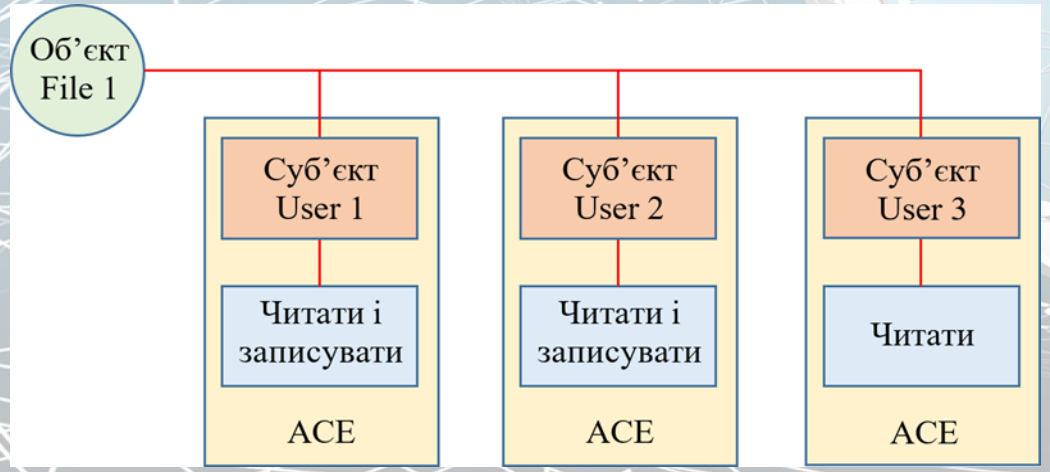
При вирішенні задачі управління доступом необхідно керуватися принципом мінімальних привілеїв. Відповідно до нього, кожному суб’єкту в системі повинен бути призначений мінімально можливий набір прав, достатній для вирішення лише тих завдань, на які він уповноважений.

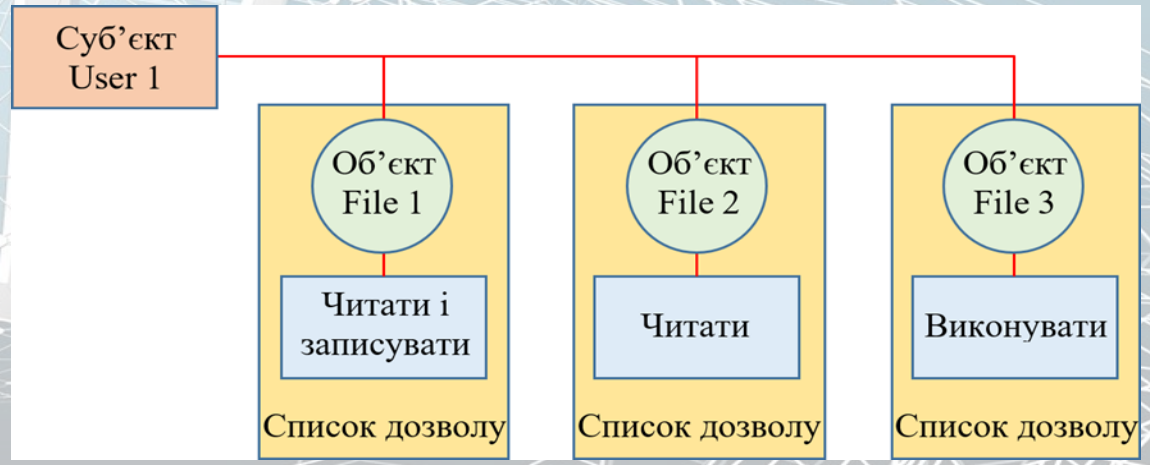
- Обмеження доступу може задаватись у формі правил.
- Для обмеження доступу використовуються також контентно- і контекстно- залежні правила.
- Ефективним засобом обмеження доступу є конфігурація користувацького інтерфейсу.

Форми подання обмежень доступу (2)

- Матриця прав доступу
- Список управління доступом до об’єкту
- Список дозволів користувача

Суб’єкти / Об’єкти	User 1	User 2	User 3
File 1	Читати і записувати	Читати і записувати	Читати
File 2	Читати і записувати	Немає доступу	Читати
File 3	Записувати	Немає доступу	Читати





Форми подання обмежень доступу (3)

Спосіб призначення прав – авторизація – істотно впливає на спосіб управління доступом.

Існує два основні підходи до авторизації:

- для авторизації виділяється особливий повноважний орган (Authority), який приймає всі рішення про наділення користувачів правами щодо всіх об’єктів;
- функції прийняття рішень по авторизації делегуються деяким суб’єктам. Таким чином, управління доступом може бути реалізовано множиною різних способів, що відображають різні підходи до задання і приведення у виконання обмежень, проте більшість реалізованих на практиці способів може бути віднесено до однієї з наступних категорій:
  - дискреційний метод доступу (Discretionary Access Control, DAC), званий також вибірковим, або довільним;
  - мандатний метод доступу (Mandatory Access Control, MAC), званий також примусовим;
  - рольовий доступ (Role-based Access Control, RBAC), званий також недискреційним методом доступу (Nondiscretionary Access Control).

Крім цих методів, взятих «в чистому вигляді», система управління доступом може базуватися на їх комбінації.

Дискреційний метод управління доступом

Дискреційний метод являє собою засіб обмеження доступу до об’єктів, що базується на унікальних ідентифікаторів суб’єкта та/або груп, до яких цей суб’єкт відноситься.

Головні особливості дискреційного методу:

- Права доступу в методі DAC описуються у вигляді списків ACL, які дають можливість гнучкого визначення набору дозволених операцій для кожного окремого користувача по відношенню до кожного окремого ресурсу, причому і користувачі і ресурси задаються унікальними ідентифікаторами.
- У методі DAC право призначати права на доступ до об’єктів делегуються окремим користувачам – власникам об’єктів. Тобто їм дозволяється діяти «на свій розсуд» і призначати іншим користувачам права на доступ до тих об’єктів, власниками яких вони є.

Основною перевагою методу DAC є його гнучкість, обумовлена свободою користувачів наділяти правами або анулювати права інших користувачів на доступ до своїх ресурсів, а також можливостями тонкої настройки набору дозволених операцій.

Недолік дискреційного методу пов’язаний з тим, що тут права на доступ визначаються по відношенню до об’єкта, а не до його вмісту.

Мандатний метод управління доступом

Мандатний доступ дозволяє реалізувати системи, що відповідають найсуворішим вимогам безпеки, як правило, вони використовуються в урядових і військових установах або в інших організаціях, для яких надзвичайно важливий високий рівень захисту даних. До основних рис мандатного методу управління доступом можна віднести наступні:

- авторизацію і управління доступом здійснює центральний повноважний орган, який відповідає за безпеку (зазвичай, в ролі такого органу виступає операційна система);
- рішення про надання права доступу приймається операційною системою динамічно на основі простого правила, яке розробляється уповноваженими на те особами на основі політики безпеки.

Правило, що визначає право доступу, будується на аналізі обох частин міток безпеки об’єкта і суб’єкта. Доступ дозволяється, якщо виконуються наступні дві умови:

- класифікація суб’єкта рівна або вище класифікації об’єкта;
- щонайменше одна з категорій об’єкта, до якого намагається отримати доступ суб’єкт, збігається хоча б з однією з категорій даного суб’єкта.

Рівень допуску суб’єктів / Рівень секретності об’єктів	Рівень від цілком таємно і нижче	Рівень від таємного і нижче	Рівень даних для службового використання
Цілком таємно	Доступ дозволений	0	0
Таємно	Доступ дозволений	Доступ дозволений	0
Дані для службового користування	Доступ дозволений	Доступ дозволений	Доступ дозволений

Рольовий метод управління доступом

- Метод управління доступом RBAC, базується на ролях, в порівнянні з методами DAC і MAC більш наближений до реального життя. Ролі встановлюються для цілей авторизації. Набір ролей в системі RBAC повинен певним чином (не однозначно) відповідати переліку різних посад, що існують на підприємстві, до якого ця система відноситься.
- Кожному користувачу може бути призначено кілька ролей (з деякими обмеженнями). Всі користувачі, які відіграють одну і ту ж роль, мають ідентичні права.
- Ієрархія ролей створюється визначенням для них відносин, званих успадкуванням: відповідно до цього визначення якщо роль R2 є спадкоємицею R1, то всі права ролі R1 приписуються до прав ролі R2, а всі користувачі ролі R2 приписуються до користувачів ролі R1
- До характерних особливостей рольового управління доступом можна віднести наступне:
  - RBAC поєднує в собі риси мандатного і дискреційного способів управління доступом.
  - Рольову систему управління доступом легше адмініструвати і контролювати, ніж дискреційну. • RBAC є централізованим методом управління доступом – так само, як і в мандатному методі, користувач позбавлений можливості керувати призначенням прав.

Автентифікація користувачів ОС

- Існує дві принципово відмінні схеми автентифікації, що реалізуються операційними системами і спеціальними мережевими службами. В одній з них, яку називають локальною системою автентифікації, операційна система працює в межах одного комп'ютера: вона використовує базу автентифікаційних даних користувачів комп'ютера з цієї ОС, і результати автентифікації можуть застосовуватися тільки для доступу до ресурсів цього комп'ютера.
- За іншою схемою працює так звана система автентифікації домену: вона базується на центральній базі автентифікаційних даних користувачів групи комп'ютерів (доменна автентифікація), що зберігається на одному з серверів мережі, і результати автентифікації служать для доступу до ресурсів даного домену.
- Локальна система автентифікації ОС працює при логічному вході користувача як з терміналу комп'ютера, так і через мережу. Перший варіант називають інтерактивним логічним входом, другий – віддаленим (мережевим, або неінтерактивним).

Управління доступом в операційних системах

В універсальних ОС – Unix/Linux, Mac OS X, MS Windows – домінує дискреційна модель управління доступом; згідно цієї моделі, власник ресурсу (користувач, який його створив або якому передано володіння) самостійно визначає, хто має доступ до цього ресурсу і які операції з ним він може виконувати.

Мандатна модель – це особливість спеціалізованих ОС, розрахованих на застосування в середовищі з підвищеними вимогами до безпеки. Проте існує набір модулів ядра Linux під назвою SELinux (Security Enhanced Linux), який реалізує багато властивостей мандатної моделі в середовищі Linux.

Модель рольового управління доступом застосовується в універсальних ОС частково у вигляді механізму вбудованих груп з наперед визначеними правами, співіснуючи з моделлю дискреційного доступу для індивідуальних користувачів і груп.

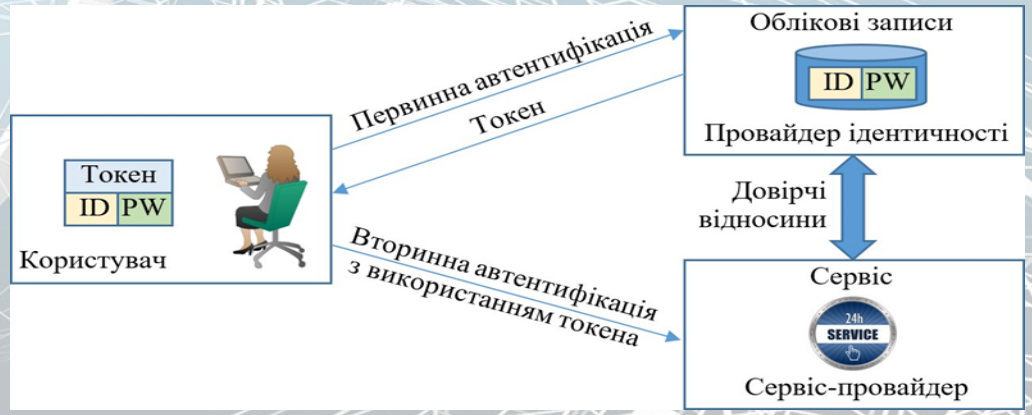
ОС сімейства Windows підтримує три класи операцій доступу, які відрізняються типом суб'єктів і об'єктів, що беруть участь в цих операціях.

- Дозволи (Permissions) – це множина операцій, які можуть бути визначені для суб'єктів усіх типів по відношенню до об'єктів будь-якого типу: файлів, каталогів, принтерів, секцій пам'яті і т. д. Дозволи за своїм призначенням відповідають правам доступу до файлів і каталогів в ОС Unix.
- Права користувачів (User Rights) визначаються для суб'єктів типу група на виконання деяких системних операцій: установку системного часу, архівування файлів, виключення комп'ютера і т. п. У цих операціях бере участь особливий об'єкт доступу – операційна система в цілому.
- Можливості користувачів (User Abilities) визначаються для окремих користувачів на виконання дій, пов'язаних з формуванням їх операційного середовища: наприклад, зміна складу головного меню програм, можливість користуватися пунктом меню Run (Виконати) і т. п.

Централізовані системи автентифікації та авторизації

Метою єдиного логічного входу (Single Sign On, SSO) є створення такого порядку автентифікації, при якому користувач виконує вхід в мережу тільки один раз, доводячи свою автентичність за допомогою будь-якого способу автентифікації, а потім результат цієї автентифікації прозорим для користувача способом застосовується кожен раз, коли йому потрібно доводити свою автентичність якому-небудь серверу або додатку.

- У цій схемі є три елементи:
- Користувач володіє деякою інформацією, достатньою для його автентифікації. Це може бути інформація будь-якого типу зі згаданих раніше – багаторазовий пароль, одноразовий пароль, цифровий сертифікат, біометричні дані та т. п. На рисунку показаний варіант автентифікації на основі багаторазового паролю, тут ID – ідентифікатор, PW – багаторазовий пароль.
- Провайдер ідентичності (Identity Provider) – це система, яка може автентифікувати користувача на основі бази даних облікових записів користувачів. Цей елемент може мати й інші назви, наприклад сервер автентифікації.
- Сервіс-провайдер (Service Provider) – це система, що надає послуги користувачам. Такими сервісами можуть бути файловий сервіс, поштовий сервіс, веб-сервіс, сервіс баз даних і т. п. Передбачається, що сервіс надається тільки автентифікованим користувачам.



Система Kerberos

Kerberos – це мережева служба, яка призначена для централізованого вирішення завдань автентифікації в великих мережах. Kerberos реалізує процедуру єдиного логічного входу в межах домену, де клієнти і сервери підтримують цей протокол.

В основі функціонування цієї досить громіздкої системи лежить кілька простих принципів:

- в мережах, що використовують систему безпеки Kerberos, всі процедури автентифікації між клієнтами і серверами мережі виконуються через посередника, якому довіряють обидві сторони процесу автентифікації, причому таким авторитетним арбітром є сама система Kerberos;
- в системі Kerberos клієнт повинен доводити свою автентичність для доступу до кожної служби, послуги якої він запитує;
- усі обміни даними в мережі виконуються в захищеному вигляді із застосуванням симетричного алгоритму шифрування AES (або DES в ранніх реалізаціях Kerberos).

Шлях клієнта до ресурсу в системі Kerberos складається з трьох етапів:

1. Визначення легальності клієнта, логічний вхід в мережу, отримання дозволу на продовження процесу отримання доступу до ресурсу.
2. Отримання дозволу на звернення до ресурсного сервера.
3. Отримання дозволу на доступ до ресурсу.



Централізований контроль віддаленого доступу (1)

Для управління віддаленими з’єднаннями невеликої локальної мережі цілком достатньо одного сервера віддаленого доступу.

При використанні в одній локальній мережі декількох серверів віддаленого доступу вимагається централізований контроль доступу до комп’ютерних ресурсів.

Розглянемо особливості централізованого контролю віддаленого доступу на прикладі протоколу TACACS (рис.)

Визначено три типи з’єднань:

1. AUTH – виконується тільки автентифікація;

2. LOGIN – виконується автентифікація і фіксується логічне з’єднання з користувачем;

3. SLIP – виконується автентифікація, фіксується логічне з’єднання, підтверджується IP-адрес клієнта.

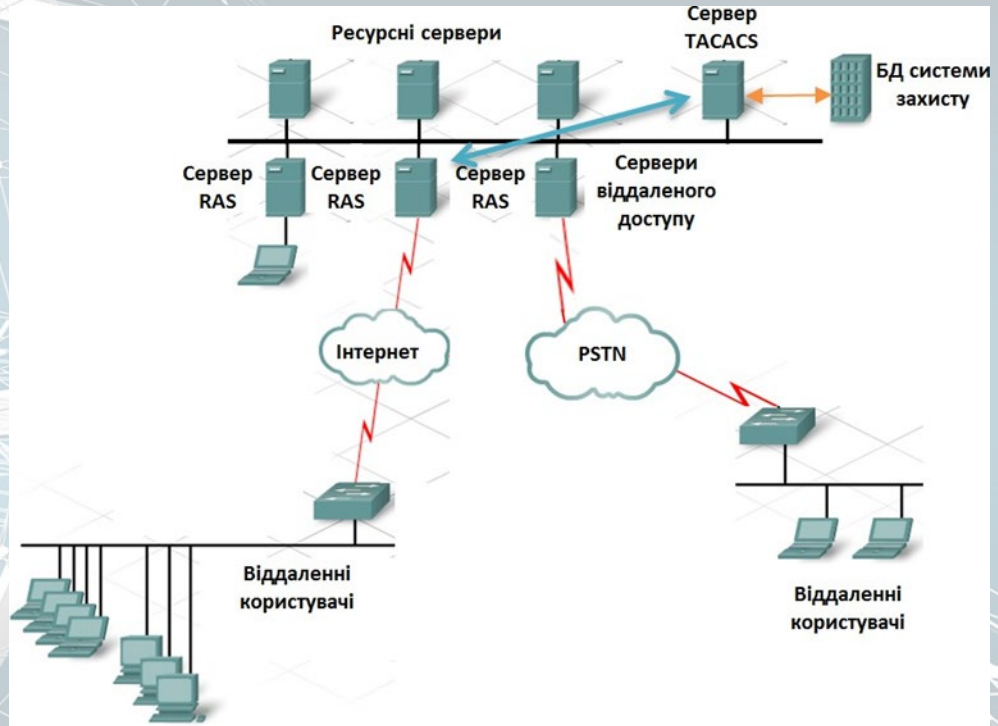


Схема централізованого контролю віддаленого доступу з використанням протоколу TACACS

Централізований контроль віддаленого доступу (2)

Сервер TACACS може виконувати автентифікацію і авторизацію віддалених користувачів різними способами:

- використовувати вбудований механізм автентифікації тієї ОС, під управлінням якої працює сервер;
- використовувати централізовані довідкові системи ОС;
- використовувати системи автентифікації, побудовані на одноразових паролях, наприклад систему SecurID;
- передавати запити іншим системам автентифікації, наприклад, системі Kerberos.

RADIUS - Повний опис цього протоколу міститься в RFC-2138 і RFC-2139, він використовує у своїй основі протокол UDP (а тому відносно швидкий), процес авторизації відбувається в контексті процесу автентифікації (тобто авторизація як така відсутня), реалізація RADIUS-сервера орієнтована на одно процесне обслуговування клієнтів (хоча можливо і багатопроцесне – питання досі відкрите), підтримує досить обмежене число типів автентифікації (PAP, CHAP), має середній рівень захищеності

TACACS+ - базується на використанні протоколу TCP, тому потенційно повільніше RADIUS, але зате дозволяє вести мультипроцесну обробку запитів (у кожен момент часу можуть обслуговуватися декілька користувачів). Рівень захищеності – високий (зашифровано усе тіло пакету).

Характеристики	RADIUS	TACACS+
Базовий протокол	UDP	TCP
Підтримувані сервіси	Автентифікація, авторизація	Автентифікація, авторизація, аудит
Безпека	Шифрується пароль	Шифрується усе тіло пакету
Підтримувані типи автентифікації	(ASCII, PAP) CHAP	(ASCII, PAP) CHAP ARAP
Можливість перенаправлення запиту	+	-



Криптографія

Частина 1

Криптографічні методи захисту дозволяють вирішити наступні завдання

- для аутентифікації користувачів системи (особливо віддалених);
- закривати і контролювати цілісність інформації, що передається по каналах зв'язку;
- закривати конфіденційну інформацію в AS (на системному рівні для захисту критичної інформації операційної системи і самої системи безпеки, на прикладному рівні - закривати секретну і конфіденційну інформацію користувачів).
- моніторинг цілісності даних

- Криптографія займається пошуком і вивченням математичних методів перетворення інформації. Завдання криптографа - забезпечити максимально можливу секретність і справжність (справжність) переданої інформації
- криптоаналізу - вивчення можливості розшифровки інформації без знання ключів.
- Сучасна криптографія включає в себе чотири основні розділи
  - 1. Симетричні криптосистеми.
  - 2. Криптосистеми з відкритим ключем.
  - 3. Системи електронного підпису.
  - 4. Управління ключами.

Термінологія

- Алфавіт - це кінцевий набір символів, що використовується для кодування інформації.
- Текст - це впорядкований набір елементів алфавіту
- Шифрування є перетворюючим процесом: оригінальний текст, який ще називають відкритим текстом, замінюється зашифрованим текстом.
- Розшифровка - це протилежне шифруванню. Ключ - це інформація, необхідна для безперебійного шифрування і розшифровки текстів.
- Ключ - це інформація, необхідна для безперебійного шифрування і розшифровки текстів.
- Криптографічна система являє собою сімейство Т-перетворень відкритого тексту.

Термінологія

- У симетричних криптосистемах один і той же ключ використовується як для шифрування, так і для дешифрування
- Системи з відкритим ключем використовують два ключі, відкритий і закритий ключ, які математично пов'язані один з одним.
- Електронний (цифровий) підпис - це прикріплене до тексту криптографічне перетворення, що дозволяє при отриманні тексту іншим користувачем перевірити авторство і справжність повідомлення.
- Криптостійкість - це характеристика шифру, яка визначає його стійкість до розшифровки без знання ключа (тобто криптоаналізу).

Термінологія

- Захист від імітації - захист від нав'язування неправдивих даних.
- Криптографічний захист – це захист даних за допомогою криптографічного перетворення, під яким розуміється перетворення даних шляхом шифрування та/або імітації.
- Синхронпосилка - це початкові публічні параметри алгоритму криптографічного перетворення.
- Рівняння шифрування - це відношення, яке описує процес формування зашифрованих даних з відкритих даних в результаті перетворень, заданих алгоритмом криптографічного перетворення.
- Рівняння розшифровки - це відношення, яке описує процес формування відкритих даних із зашифрованих даних в результаті перетворень, заданих алгоритмом криптографічного перетворення.

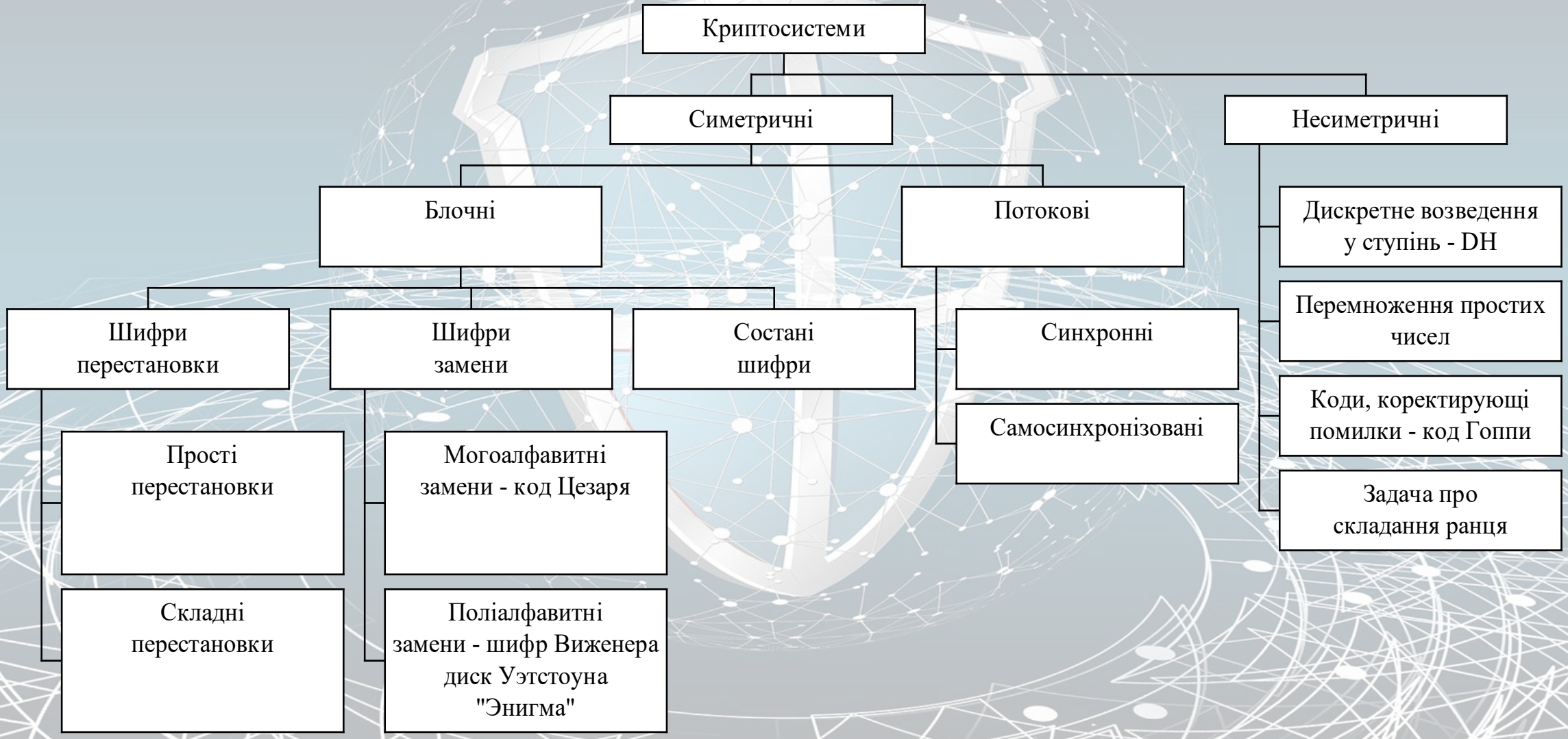
Вимоги до криптосистем

- Законний одержувач зможе скасувати перетворення та розшифрувати повідомлення.
- Криптоаналітик-противник, який перехоплює повідомлення, не зможе реконструювати з нього вихідне повідомлення без таких витрат часу і коштів, які зроблять цю роботу непрактичною.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

- Зашифроване повідомлення має бути читабельним, лише якщо є ключ.
- Кількість операцій, необхідних для визначення використаного ключа шифрування за фрагментом зашифрованого повідомлення і відповідним йому відкритим текстом, не повинна бути менше загальної кількості можливих ключів;
- кількість операцій, необхідних для розшифровки інформації шляхом перерахування всіляких ключів, повинно мати суворо меншу оцінку і виходити за рамки можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);
- знання алгоритму шифрування не повинно впливати на надійність захисту;
- Незначна зміна ключа має призвести до значної зміни зовнішнього вигляду зашифрованого повідомлення, навіть якщо використовується той самий ключ.
- Тощо……

Загальна класифікація криптосистем



Шифрування

Шифрування забезпечуючи наступні властивості системи управління даними

- Конфіденційність.
- Автентифікація
- Цілісність
- Контроль доступу

Як виконується шифрування (подвійне)

1. Отримання вихідного коду
2. Попереднє шифрування
3. Вторинне шифрування
4. Передача або запис даних
5. попередня розшифровка
6. остаточна розшифровка
7. Отримання вихідного коду

Класифікація симетричних криптосистем

Основні складові:

- Моно- і багатоалфавітні заміни.
- Перестановоки
- Гамування
- Блокові шифри

Поєднання цих складових створює сучасні криптографічні системи

Перестановки

- Проста безключова перестановка
- Перестановка по ключу

з н а к
3 4 2 1
\ \ / /
/ / \ \
1 2 3 4
к а з н

- подвійна перестановка
- Rubicon

- Криптографічне перетворення T для алфавіту Zm є послідовністю автоморфізмів: T={T(n):1Jn<Ґ}**

T(n): Z m,n Zm,n, * n®*<Ґ*

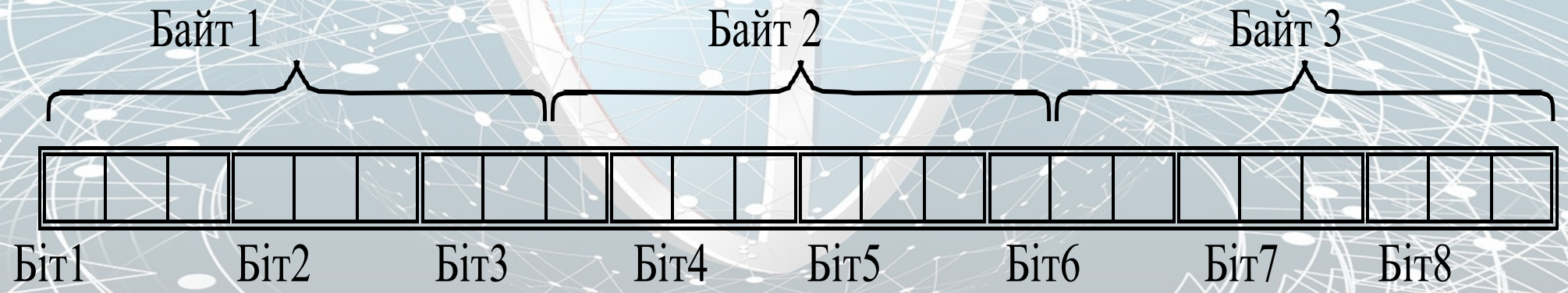
- К. Шеннон про те, що абсолютно міцний шифр можна отримати, тільки використовуючи «стрічку одноразового використання», тобто унікальні параметри для кожного шифрування.

Перестановки

- Магічні квадрати

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

- Метод «заплутаної шини»



- Шифр збивання

Системи заміщення (підстановок)

Підстановка — це відображення скінченної множини M сам по собі.

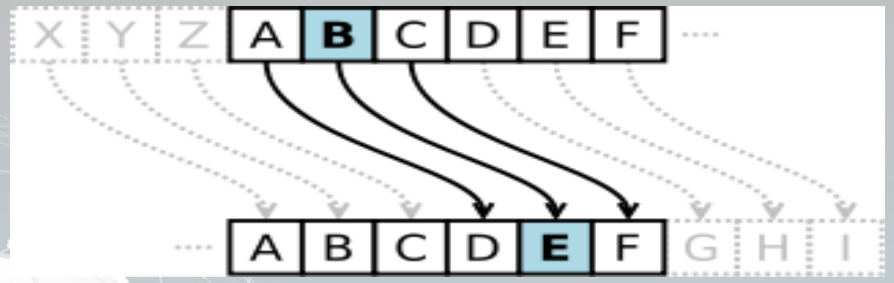
Якщо при цій підстановці S число j переходить в Ij, то підстановка позначається символом S:

$$S = \begin{bmatrix} 1 & 2 & & n \\ I_1 & I_2 & & I_n \end{bmatrix}$$

У цьому позначенні числа 1,2,...,n можна довільно переставляти, відповідно переставляючи числа I 1,I 2,... Iн.

Результатом послідовного виконання двох підстановок S1 і S2 однакового ступеня також є підстановка, яка називається добутком підстановок S1 і S2 і позначається S1S2. Добуток замін має властивість асоціативності

Шифри підстановки



- **Шифр Цезаря** або шифр зсуву — симетричний моноалфавітний алгоритм шифрування, в якому кожна буква відкритого тексту заміняється на ту, що віддалена від неї в алфавіті на сталу кількість позицій. Римський імператор Юлій Цезар використовував для приватного листування шифр зсуву з ключем 3 — замість літери A підставляв D, замість B — E і так далі.
  - Як і будь-який моноалфавітний шифр, Цезарів вразливий до частотного криптоаналізу. Навіть легше зламати його простим перебором, бо кількість можливих ключів зовсім невелика — для українського алфавіту 33 варіанти.
  - Принцип дії полягає в тому, щоб циклічно зсунути алфавіт, а ключ — це кількість літер, на які робиться зсув.
  - Якщо зіставити кожному символу алфавіту його порядковий номер (нумеруючи з 0), то шифрування і дешифрування можна виразити формулами: $y = (x + k) \bmod n$ $x = (y - k) \bmod n,$

Квадрат Полібія

- Квадрат Полібія. також відомий як шахова дошка Полібія — оригінальний код простої заміни, одна з найдавніших систем кодування, запропонована Полібієм (грецький історик, полководець, державний діяч, III століття до н. е.). Цей спосіб кодування спочатку застосовувався для грецької абетки, але потім поширився на інші мови. До кожної мови окремо складається таблиця шифрування з однаковою (не обов'язково) кількістю пронумерованих рядків та стовпців, параметри якої залежать від її потужності (кількості букв в абетці). Беруться два цілих числа, добуток яких найближче до кількості букв у мові — отримуємо потрібну кількість рядків і стовпців. Потім вписуємо в таблицю всі букви алфавіту поспіль — по одній на кожну клітину. При нестачі клітин можна вписати в одну дві букви (рідко вживані або схожі за вживанням).

- Для шифрування на квадраті знаходили букву тексту і вставляли в шифровку нижню від неї в тому ж стовпці. Якщо буква була в нижньому рядку, то брали верхню з того ж стовпця.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Шифр Плейфера

Шифр Плейфера використовує матрицю 5x5 (для латинського алфавіту, для кириличного алфавіту можливо збільшити розмір матриці до 4x8), що містить ключове слово або фразу.

Для того щоб зашифрувати повідомлення, необхідно розбити його на біграми (групи з двох символів) . Два символи біграми відповідають протилежним кутам прямокутника в ключовий матриці. Визначаємо положення кутів цього прямокутника відносно один одного. Потім, керуючись наступними 4 правилами, зашифровуємо пари символів вихідного тексту:

1. Якщо два символи біграми збігаються (або якщо залишився один символ), додаємо після першого символу «X», зашифровуємо нову пару символів і продовжуємо. У деяких варіантах шифру Плейфера замість «X» використовується «Q».

2. Якщо символи біграми вихідного тексту зустрічаються в одному рядку, то ці символи замінюються на символи, розташовані в найближчих стовпцях праворуч від відповідних символів. Якщо символ є останнім в рядку, то він замінюється на перший символ цього ж рядка.

3. Якщо символи біграми вихідного тексту зустрічаються в одному стовпці, то вони перетворюються в символи того ж стовпця, що знаходяться безпосередньо під ними. Якщо символ є нижнім в стовпці, то він замінюється на перший символ цього ж стовпця.

4. Якщо символи біграми вихідного тексту знаходяться в різних стовпчиках і різних рядках, то вони замінюються на символи, що знаходяться в тих же рядках, але відповідні іншим кутам прямокутника.

Для розшифровки необхідно використовувати інверсію цих чотирьох правил

Шифр Хілла

Кожній букві спершу зіставляється число. Для латинського алфавіту часто використовується найпростіша схема: A = 0, B = 1, …, Z = 25, але це не є істотною властивістю шифру. Блок з n букв розглядається як n-мірний вектор і множиться на n × n матрицю по модулю 26. (Якщо як основа модуля використовується число більше ніж 26, то можна використовувати іншу числову схему для зіставлення буквах чисел і додати прогалини і знаки пунктуації.) Матриця повністю є ключем GYBNQKURPшифру. Матриця повинна бути оборотною в щоб була можлива операція розшифрування.

$\mathbb{Z}_{26}$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 3 \\ 14 \\ 6 \end{pmatrix} = \begin{pmatrix} 360 \\ 323 \\ 388 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 11 \\ 24 \end{pmatrix} \pmod{26}$$

Для того, щоб розшифрувати повідомлення, необхідно звернути шифротекст назад в вектор і потім просто помножити на зворотню матрицю ключа (IFKVIVVMI в буквеному вигляді). (Існують стандартні методи обчислення зворотніх матриць, дивіться способи знаходження Оберненої матриці для подробиць.) В зворотна матриця до використаної в прикладі шифрування буде

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 471 \\ 1054 \\ 786 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 14 \\ 6 \end{pmatrix} \pmod{26}$$

Приклади підстановок (ASCII-code)

- Шифр перейменування
  - Суть методу полягає в створенні таблиці з 256 елементів з неоднаковими значеннями (за випадковим законом). Кожен байт замінюється елементом цієї таблиці з індексом, рівним байту. Після цього таблиця вводиться в тіло файлу, а адреса таблиці у файлі є ключем. Таким чином, довжина файлу збільшується на 256 байт. Розшифровка проводиться в зворотному порядку.
- Метод псевдовипадкової інверсії
  - Суть методу полягає в тому, що ключ містить початкову адресу байта, який буде інвертуватися, а кількість таких байт поділити на 256. Після інвертування байта обчислюється наступна адреса за допомогою псевдовипадкового коду. Причому це відбувається до тих пір, поки не буде інвертовано потрібну кількість байт.

Багатоалфавітні системи

- **Шифр Віженера** - поліалфавітний шифр, який як ключ використовує слово.

Якщо пронумерувати літери алфавіту від 0 до 32 (а → 0, б → 1, в → 2, …), то шифрування Віженера можна подати формулою:

$C_i = (P_i + K_j) \bmod 33$,

де K_j — j-та літера ключового слова, P_i — і-а літера вихідного слова.

Ключове слово повторюється, поки не отримано гаму, рівну довжині повідомлення.

Дешифрування відбувається за наступною формулою:

$C_i = (P_i + 33 - K_j) \bmod 33$

Табличне представлення

_ а б в г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я
а а б в г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я
б б в г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я а
в в г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я а б
г г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я а б в
ґ ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я а б в г
……

Шифр Гронсфельда

- поліалфавітний підстановочний шифр створений графом Гронсфельдом (керівником першої дешифрувальної служби Німеччини) в XVII столітті. Шифр можна вважати удосконаленням шифру Цезаря (надійність) і Віженера / Бофора (швидкість).

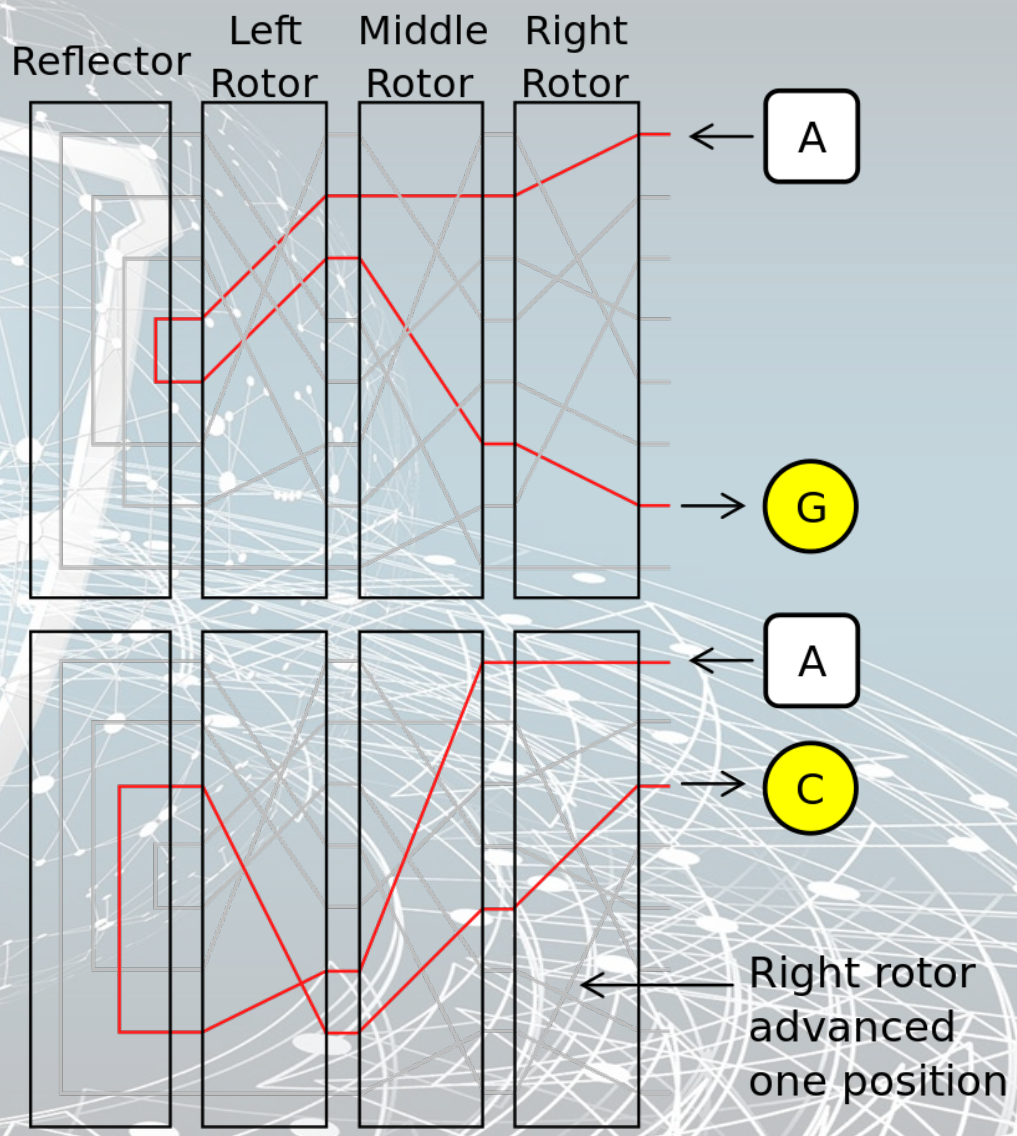
Шифрування. Кожен символ Мі відкритого тексту М потрібно змістити вправо на Кі (відповідний символ ключа К) кроків.

- Або користуючись таблицею Гронсфельда (Тх у, де х — номер рядка, а у — номер стовпця, відлік ведеться з нуля):
-

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

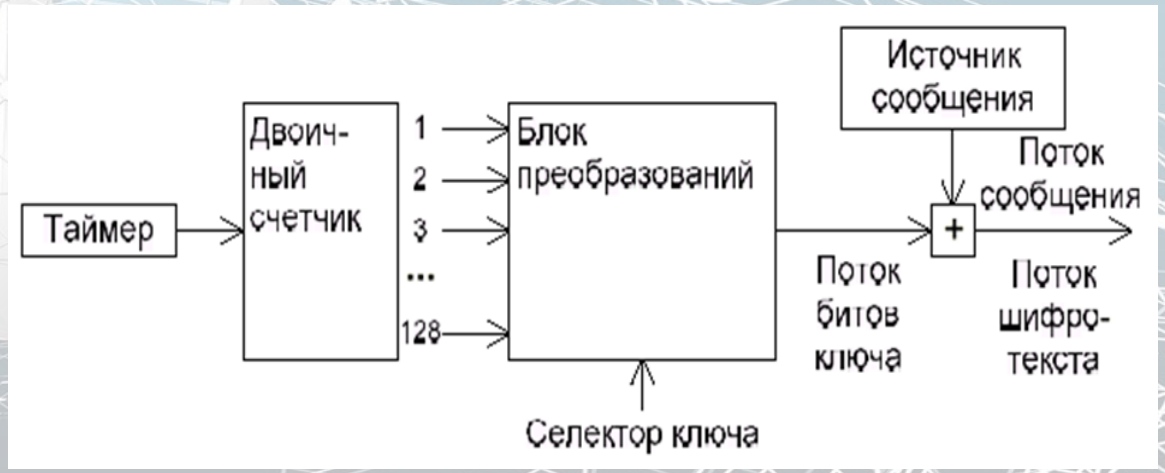
Шифр машини Enigma

- «Ени́гма» (англ. Enigma) — шифрувальна машина часів Другої світової війни. оскільки основою її механізму є диски з 26-ма перепайками.
- постійна зміна електричного кола, через яке йшов струм, внаслідок обертання роторів дозволяла реалізувати багатоалфавітний шифр підстановки, що давало високу стійкість шифру для того часу.



Шифр Вернама

- (інша назва: англ. one-time pad - схема одноразових блокнотів) — у криптографії, система симетричного шифрування, винайдена в 1917 році співробітниками AT&T Мейджором Джозефом Моборном і Гільбертом Вернамом. Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна криптографічна стійкість.
- Для утворення шифротексту повідомлення об'єднується операцією XOR з ключем (названим одноразовим блокнотом або шифроблокнотом). При цьому ключ повинен мати чотири критично важливі властивості:
  - Бути справді випадковим;
  - Збігатися за розміром з заданим
  - відкритим текстом;
  - Застосовуватися тільки один раз;
  - Повинен зберігатися в повній таємниці сторонами, що спілкуються.



Генерація ключа для моделювання системи Vernam



Криптографія

Частина 2

Гаммування

- Суть методу полягає в тому, що ключ до розшифровки байта розраховується на основі попереднього байта. При цьому сам ключ можна змінювати з байта на байт. Алгоритм кодування наступний:
  - 1) ввести ключ;
  - 2) виконати одну з дій з безлічі {+,-,} з файловим байтом (ігноруючи перенесення);
  - 3) отриманий байт є ключем до наступного байту файлу;
  - 4) Поки ми не дійдемо до кінця файлу, повторюємо крок 3.
- Розшифровка виконується за аналогічним алгоритмом.

Датчики ПВЧ

- Принцип шифрування полягає в тому, щоб згенерувати шифр гами за допомогою датчика псевдовипадкових чисел (ПВЧ) і накладати отриману гаму на відкриті дані оборотним способом (наприклад, при використанні логічної операції «ексклюзивні АБО»).
- Процес розшифровки даних зводиться до повторної генерації шифру гами відомим ключем і накладення такої гами на зашифровані дані.
- основні вимоги до криптографічно сильної псевдовипадкової послідовності або гамма-генератору:
  - 1. Гамма-період повинен бути досить великим, щоб шифрувати повідомлення різної довжини.
  - 2. Гамма повинна бути важко передбачувана. Це означає, що якщо знати тип генератора і шматок гами, то неможливо передбачити наступний шматок гамма-біта з ймовірністю вище х. Якщо криптоаналітику стане відомо про якусь частину шкали, він все одно не зможе визначити біти, які передують або слідують за нею.
  - 3. Гамма-генерація не повинна бути пов'язана з великими технічними та організаційними труднощами.

Алгоритми генерації

- дробова частина многочлена першого ступеня:

$$Y_n = E_n t\ (a * n + b)$$

- Генератор Лемера $G_{n+1}=KG_n+C \bmod M$
- лінійний конгруентний датчик

$$x_{n+1} = (ax_n + c) \mod m$$

- Мультиплікативний конгруентний метод

$$x_i = (a_1 x_{i-1}) \mod m$$

- Генератори типу «Xorshift» $x_n = x_{n-1} \operatorname{xor} (x_{n-1} \operatorname{shl} a)$
- послідовність Фібоначчі {0, 1, 1, 2, 3, 5, 8, 13, 21, 34...}.

Датчики послідовності М

$$a_k[n+1] = \begin{cases} a_0[n] + a_1[n], & k = 3 \\ a_{k+1}[n], & \text{otherwise} \end{cases}$$

- М-послідовності є періодичними з періодом $N=2^k-1$
- Протягом одного періоду М-послідовності кількість символів, які приймають значення одиниця, на одиницю більша, ніж кількість символів, які приймають значення нуль;
- Будь-які комбінації символів довжини n на довжині одного періоду М-послідовності за винятком комбінації з n нулів зустрічаються не більше одного разу. Комбінація з n нулів заборонена, оскільки на її основі може генеруватися лише послідовність з одних нулів;
- Сума по модулю 2 будь-якої М-послідовності з її довільним циклічним зсувом також є М-послідовністю;
- Періодична АКФ будь-якої М-послідовності має постійний рівень бічних пелюсток, що дорівнює 1/N

Псевдовипадковий гамма-метод

$$K_i = ((K_{i-1} - 1) \times C - 1) \bmod N$$

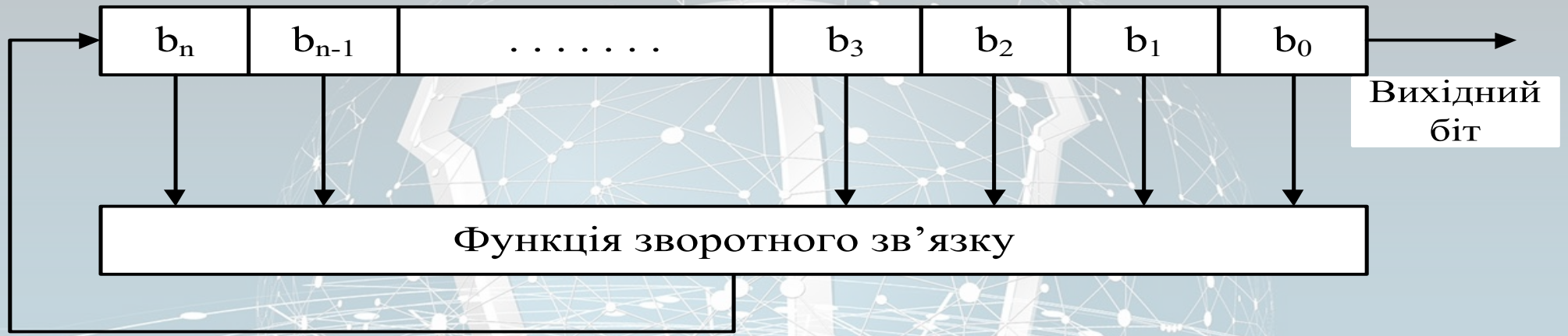
де C mod 4 = 1,

- N+1 — максимальне псевдовипадкове число цього ряду,
- K_{i-1} - ключ для попередньої ітерації;
- K_i є ключем до нової ітерації

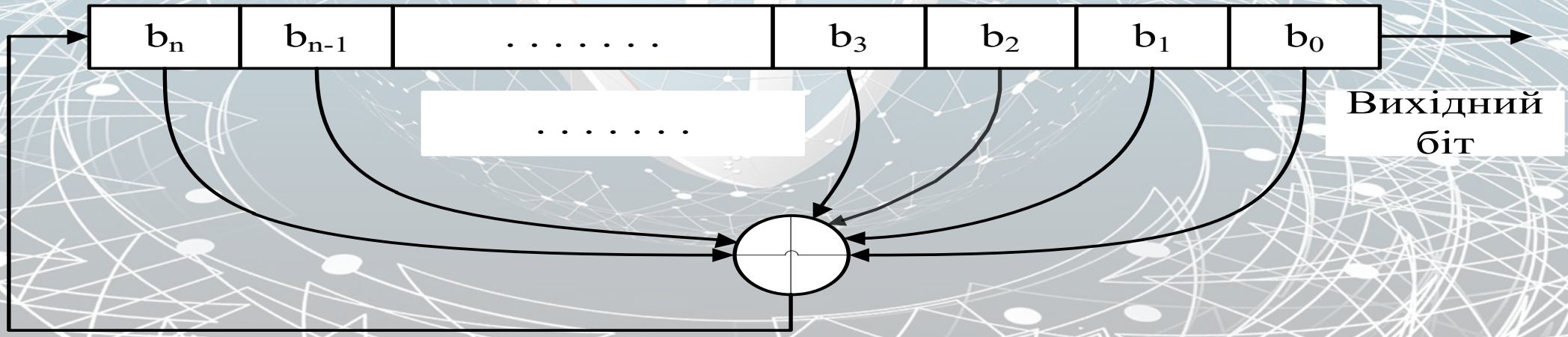
Ланцюговий гамма-метод

- . Суть методу: існує послідовність ключів (наприклад, 16). Кожен ключ містить 12 цифр номера ключа для кодування і 4 біти для вказівки наступного ключа в ланцюжку. Після використання ключа візьміть новий за адресою, вказаною в поточному ключі.

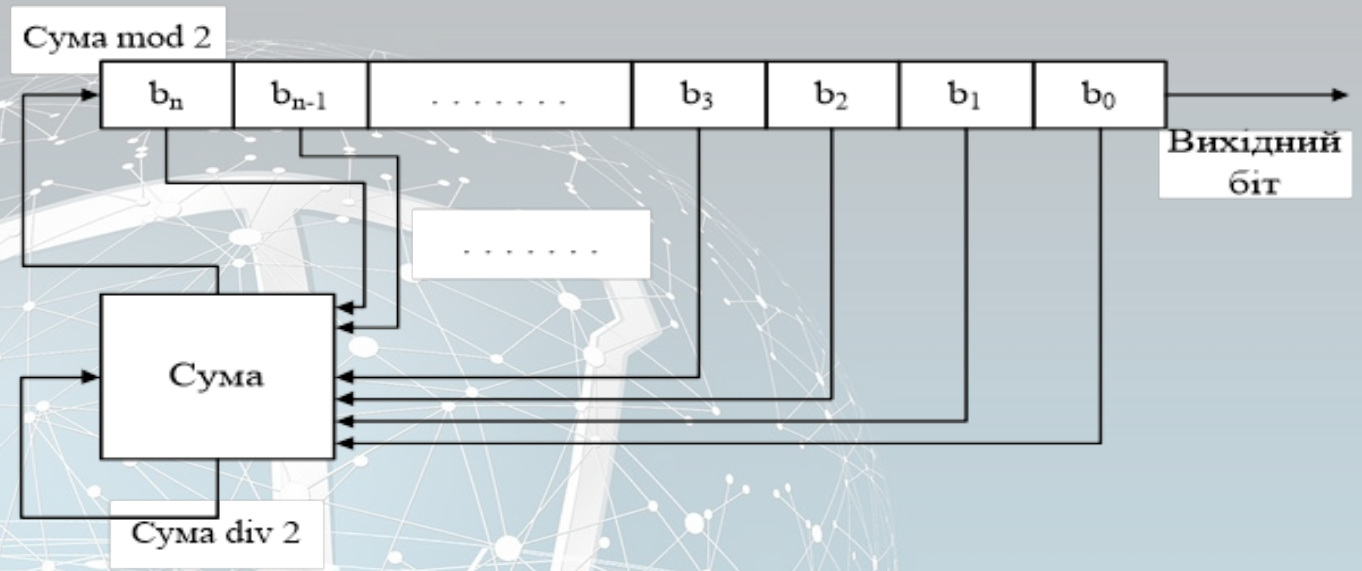
Регістри зсуву з зворотним зв‘язком



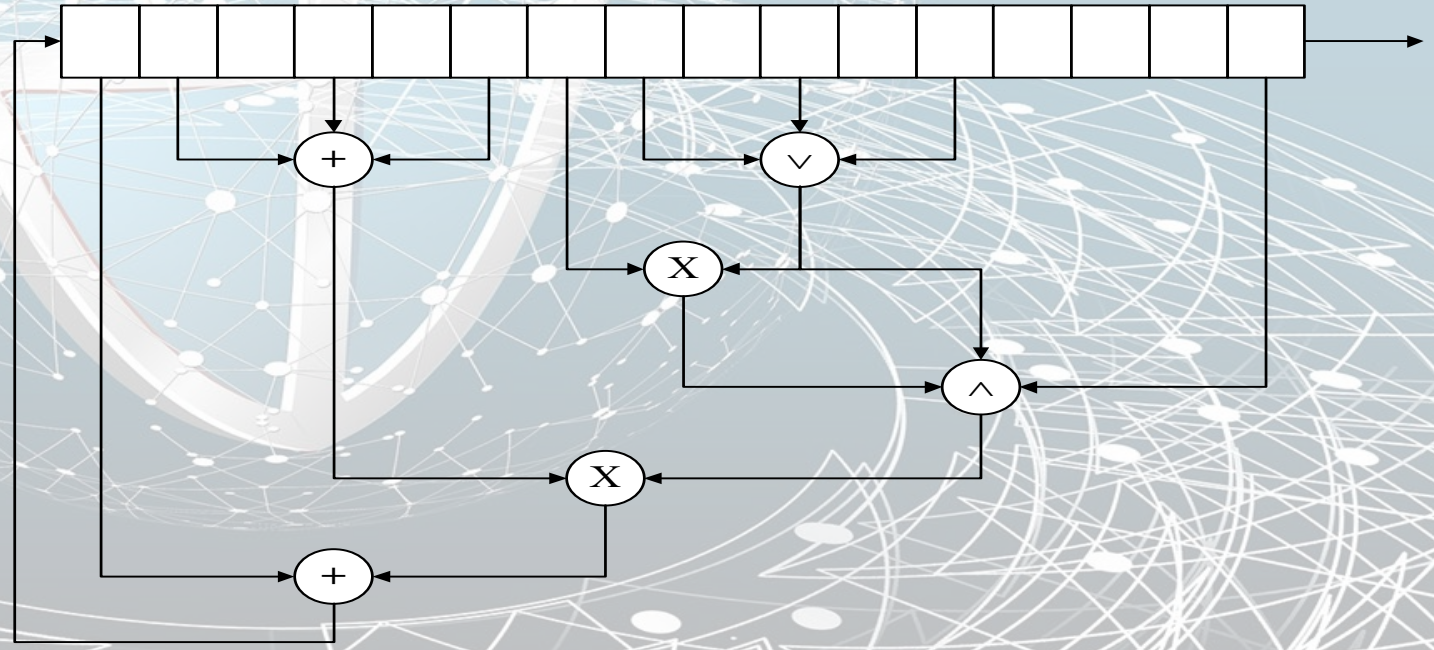
Регістри зсуву з лінійним зворотним зв‘язком



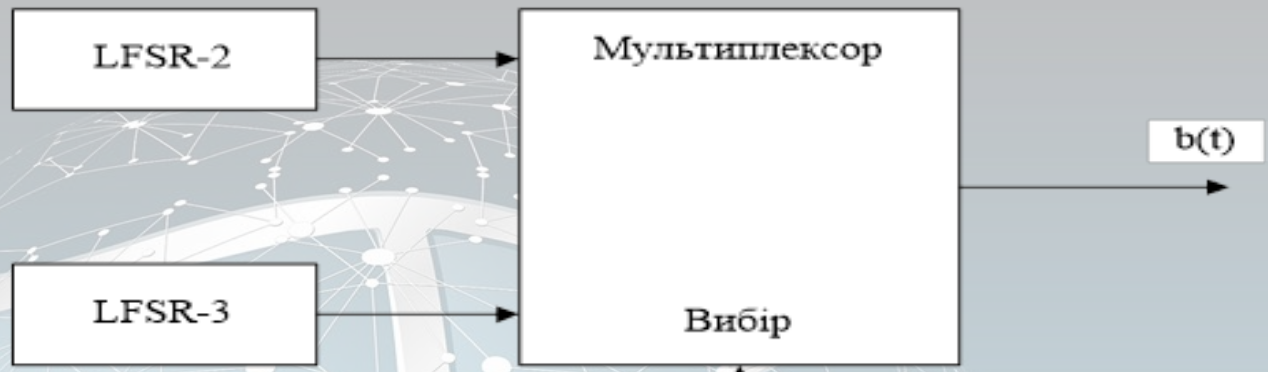
Регістри зсуву з зворотним зв‘язком по входу



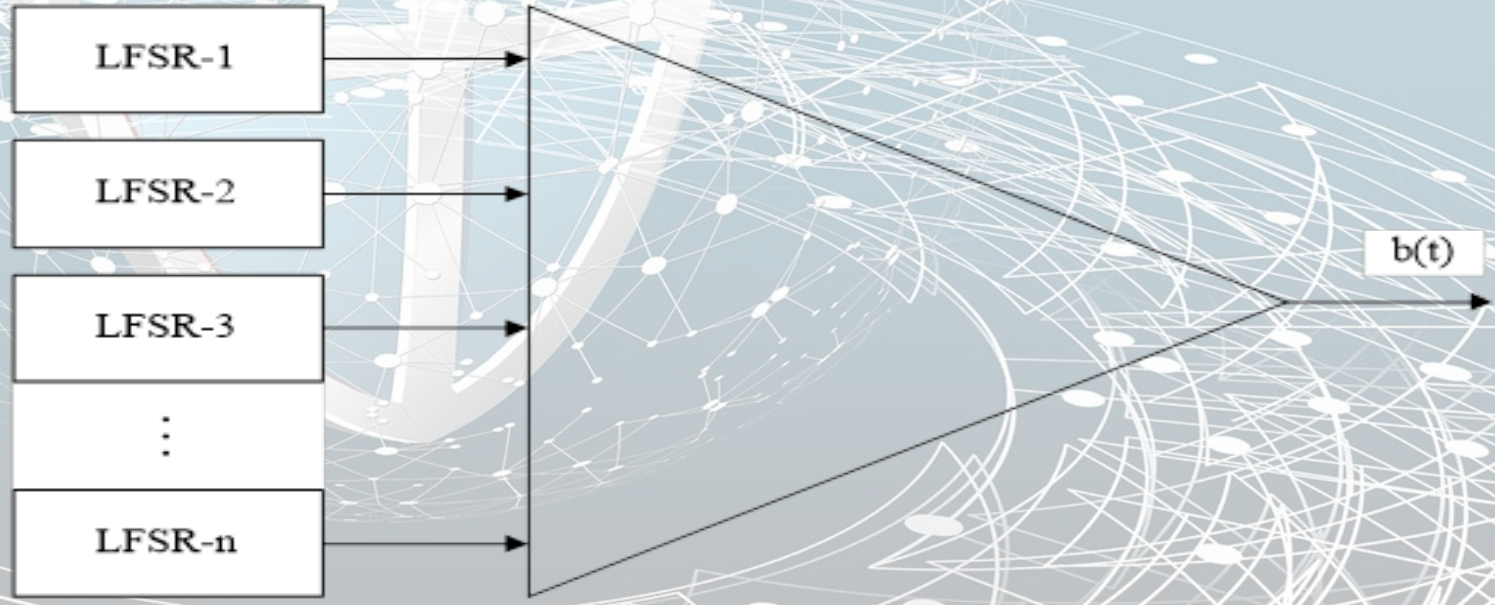
Регістри зсуву з нелінійним зворотним зв‘язком



Генератор Геффа



Граничний генератор



Інші види генераторів на основі регістру зсуву

- Узагальнений генератор Геффа
- Генератор "стоп-пішов " (Stop-and-Go) Both-Piper
- Генератор, що чергується, "стоп-пішов«
- Двосторонній генератор "стоп-пішов«
- Граничний генератор
- Самопроріджуючі (Self-Decimated) генератори
- Багатошвидкісний генератор із внутрішнім добутком
- Підсумовуючий генератор
- динамічний генератор випадкової послідовності
- Каскад Голлманна
- Проріжувачий генератор
- Генератор, що самопроріджується

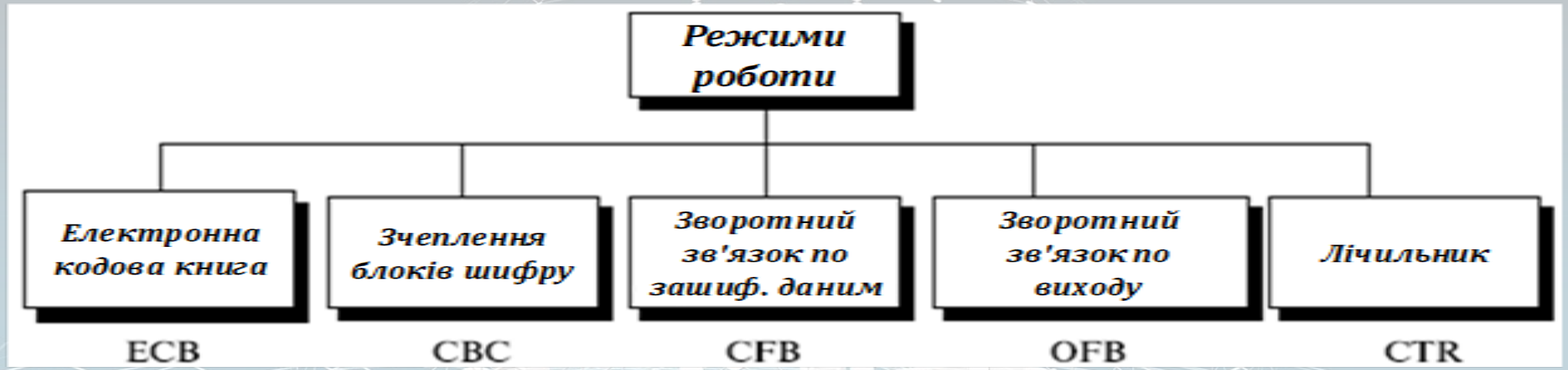
Комбінований генератор



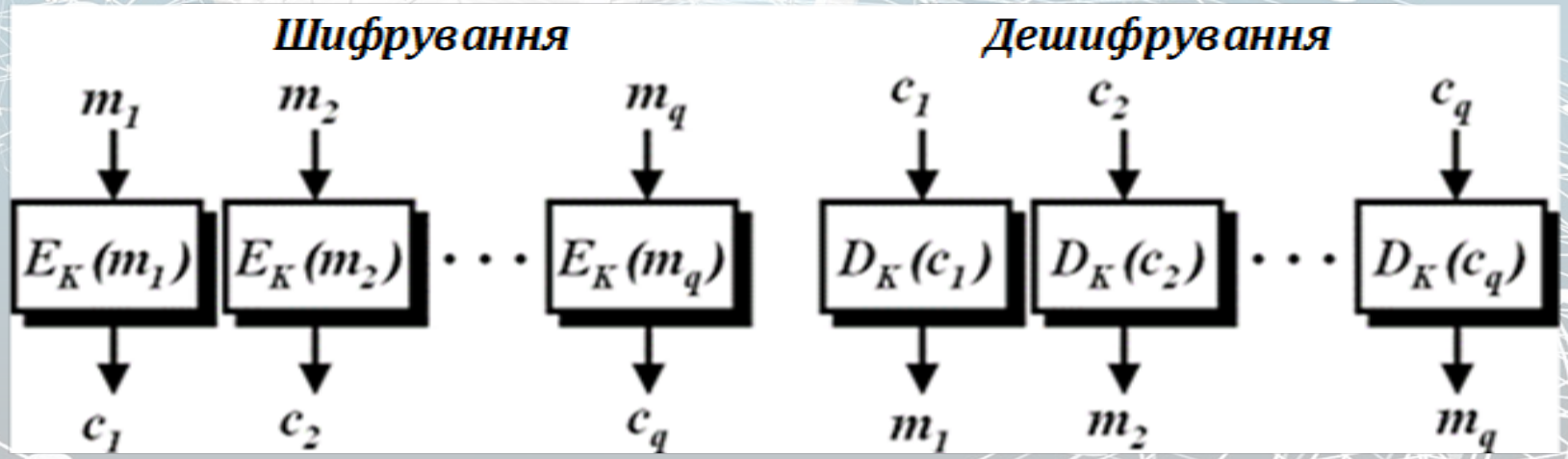
Іншими генераторами, що є розвитком аналогічних ліній, є :

- Генератор парності FCSR. Всі регістри - FCSR, а об'єднуюча функція - XOR.
- Генератор парності LFSR/FCSR. Використається суміш LFSR й FCSR, поєднуваних за допомогою XOR.
- Граничний генератор FCSR. Всі регістри - FCSR, а об'єднуючою функцією є мажорування.
- Граничний генератор LFSR/FCSR. Використається суміш LFSR й FCSR, поєднуваних за допомогою мажорування.
- Підсумовуючий генератор FCSR. Всі регістри - FCSR, а об'єднуюча функція - додавання з переносом.
- Підсумовуючий генератор LFSR/FCSR. Використається суміш LFSR й FCSR, поєднуваних за допомогою додавання з переносом.

Криптографічні режими

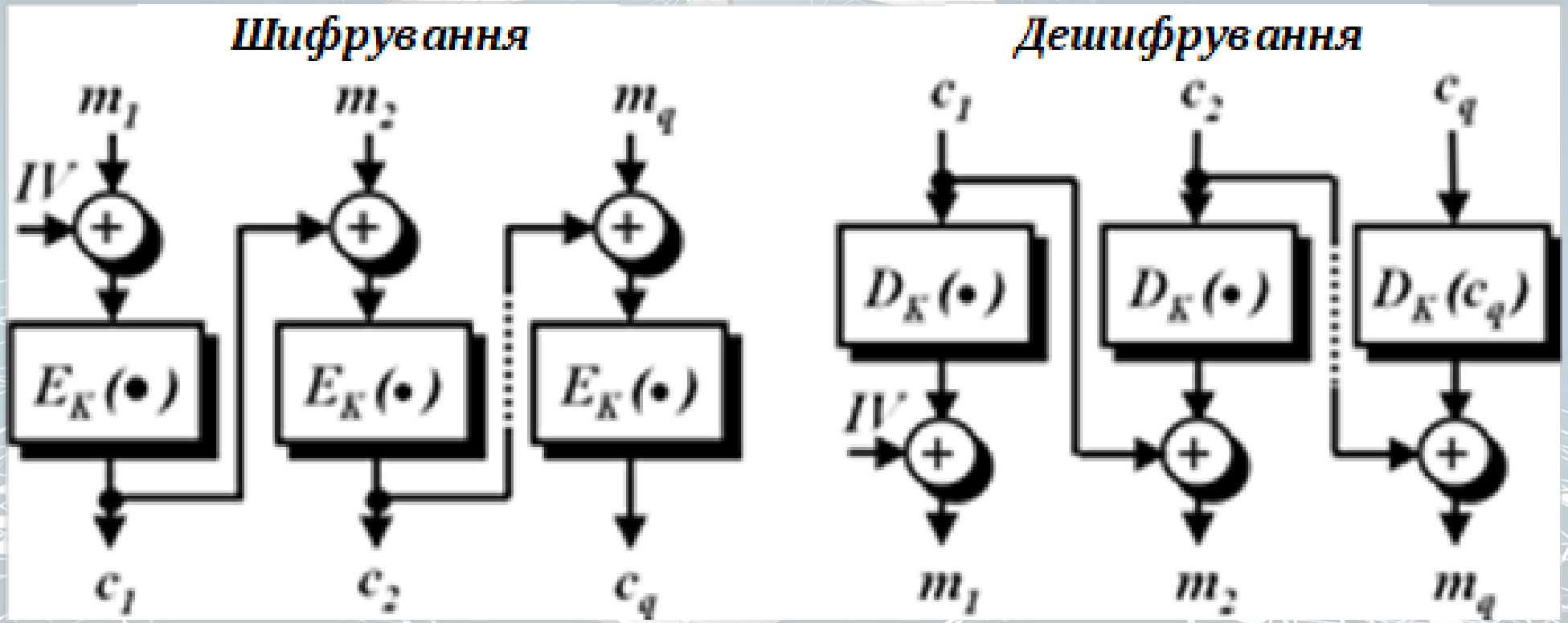


- Режим електронної книги шифрів ECB



Шифрування: $C_i = E_K(M_i)$ Розшифровка: $M_i = D_K(C_i)$

Режим конкатенації (зчеплення) блоків шифру CBC



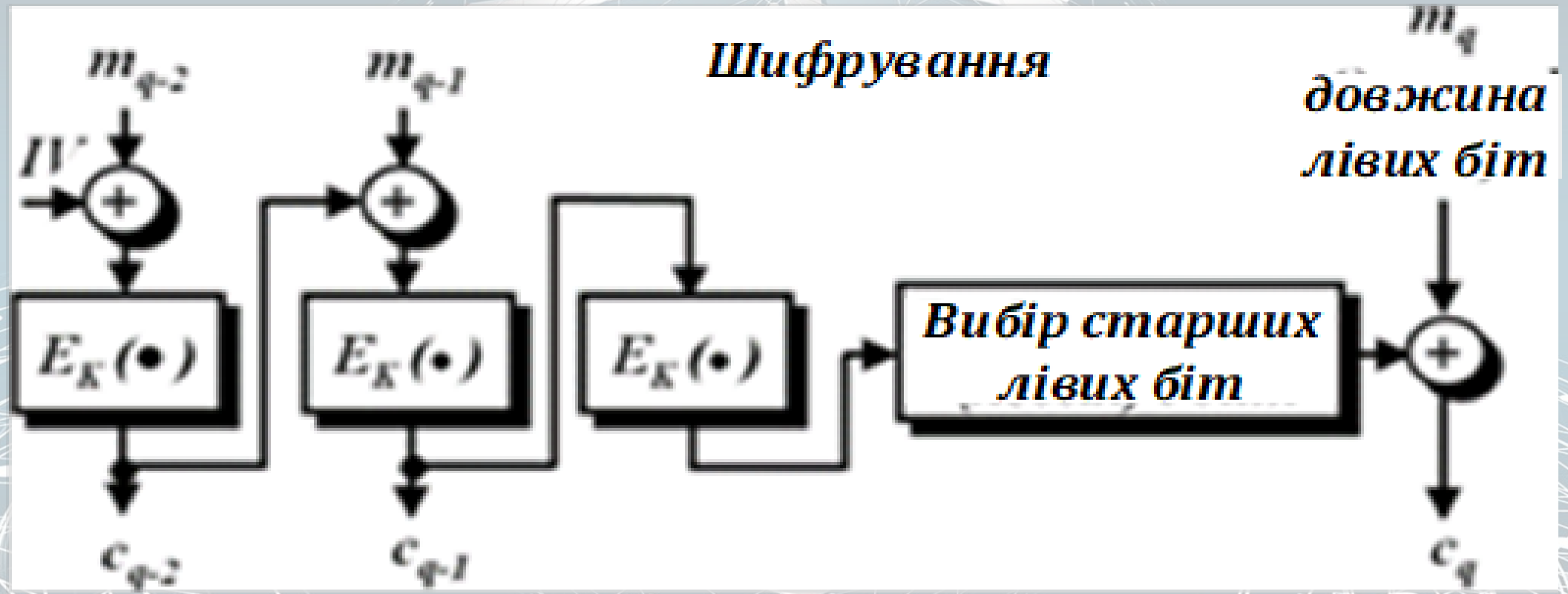
Шифрування: $C_0 = IV$

$C_1 = E_K(M_i \oplus C_{i-1})$

Дешифрування: $M_0 = IV$

$M_1 = D_K(C_i) \oplus C_{i-1}$

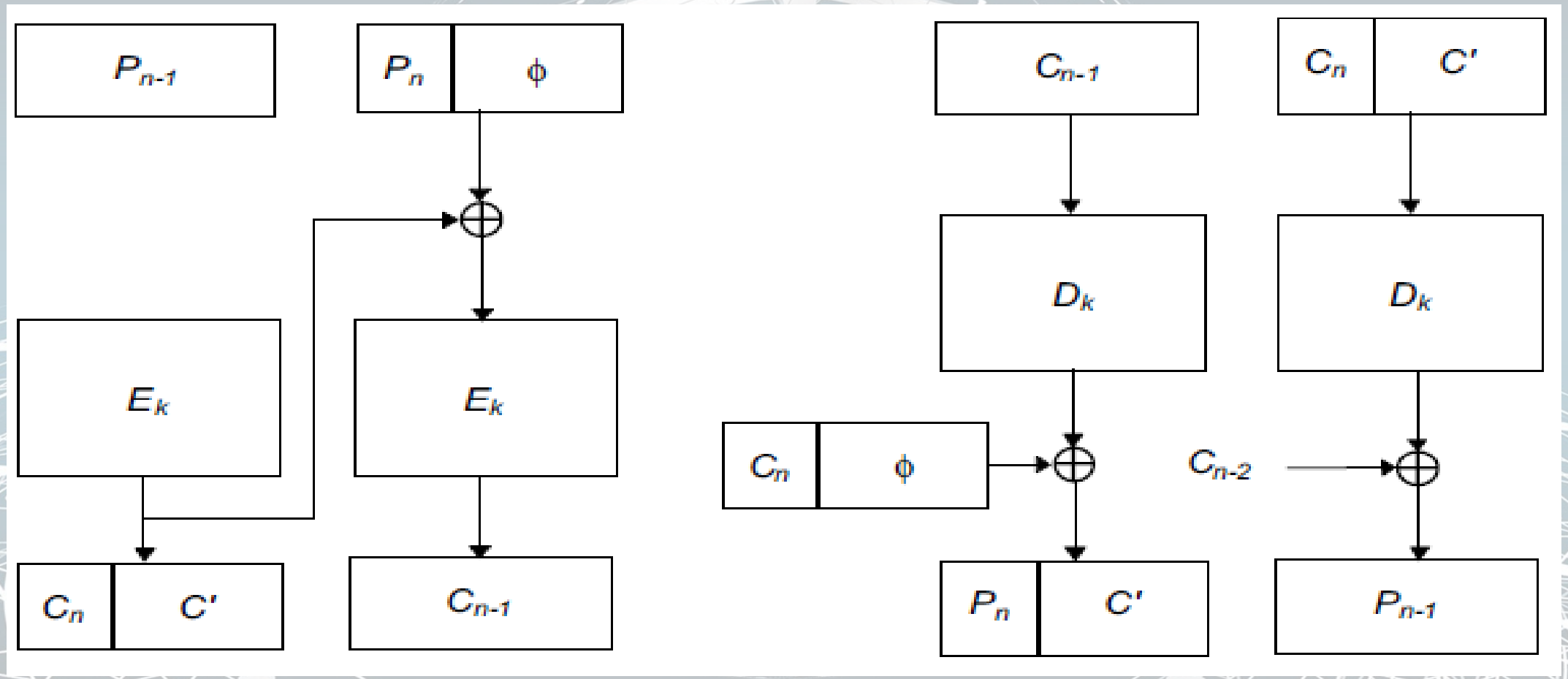
Шифрування короткого останнього блоку в режимі CBC



шифрування і дешифрування обернені один до одного.

$$M_1 = D_K(C_i) \oplus C_{i-1} = D_K(E_K(M_i \oplus C_{i-1})) = M_i \oplus C_{i-1} \oplus C_{i-1} = M_i$$

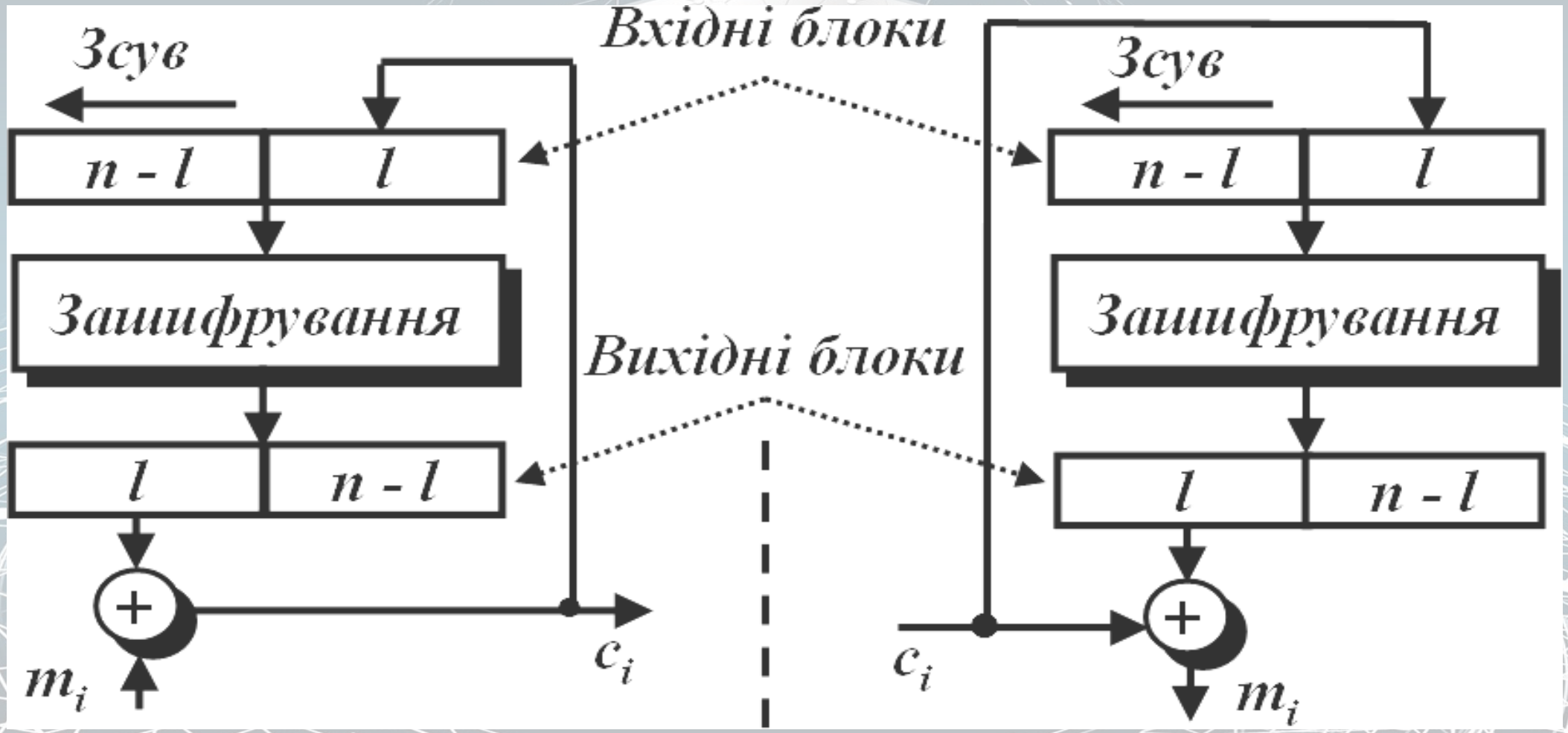
Захоплення шифротексту в режимі CBC



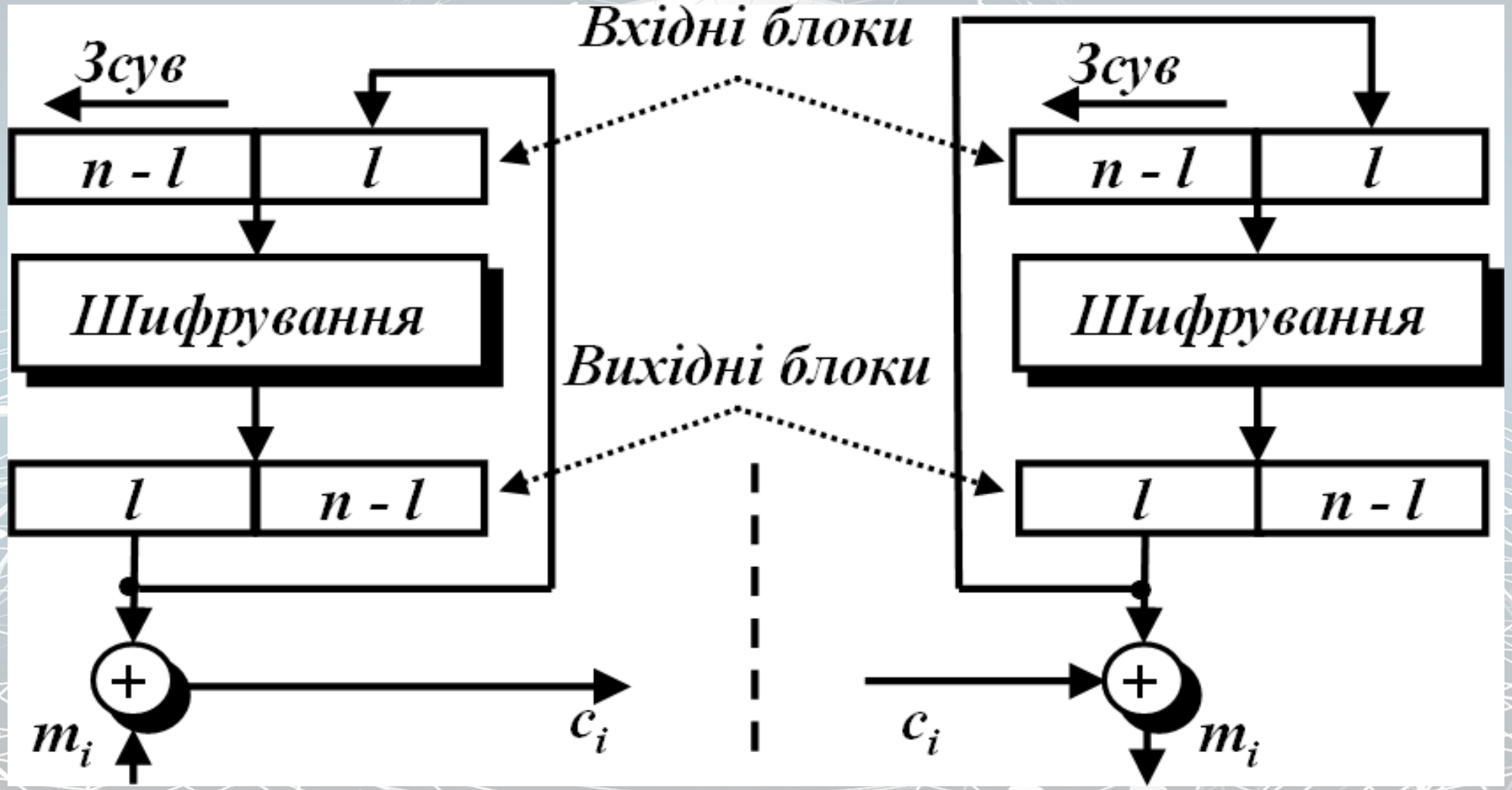
Шифрування

Дешифрування

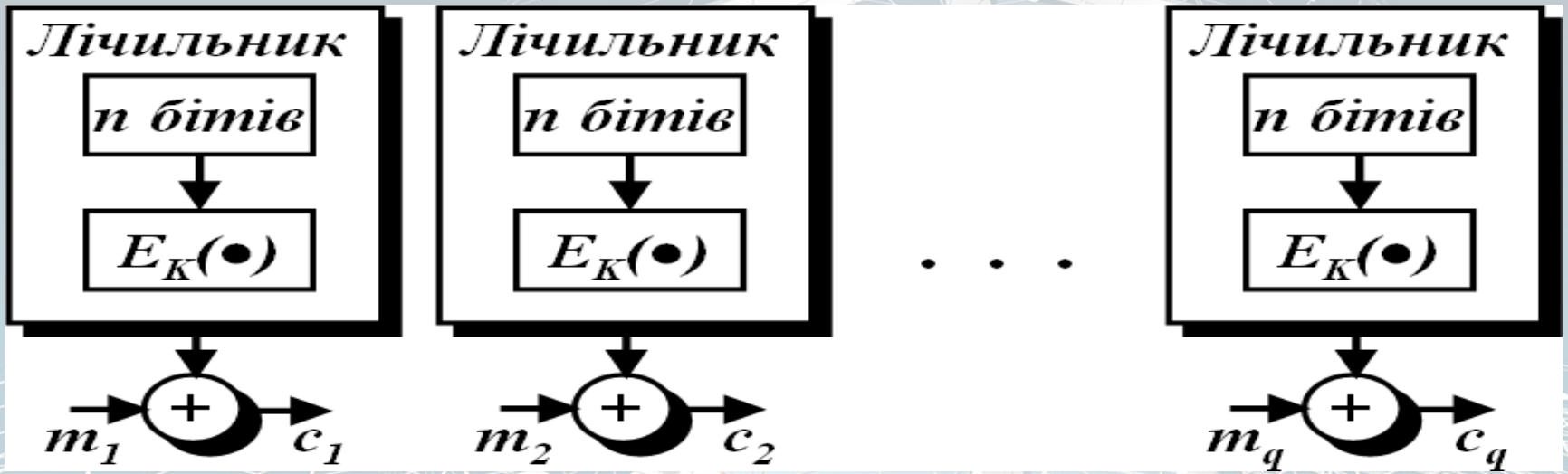
Зворотній зв'язок шифру (CFB)

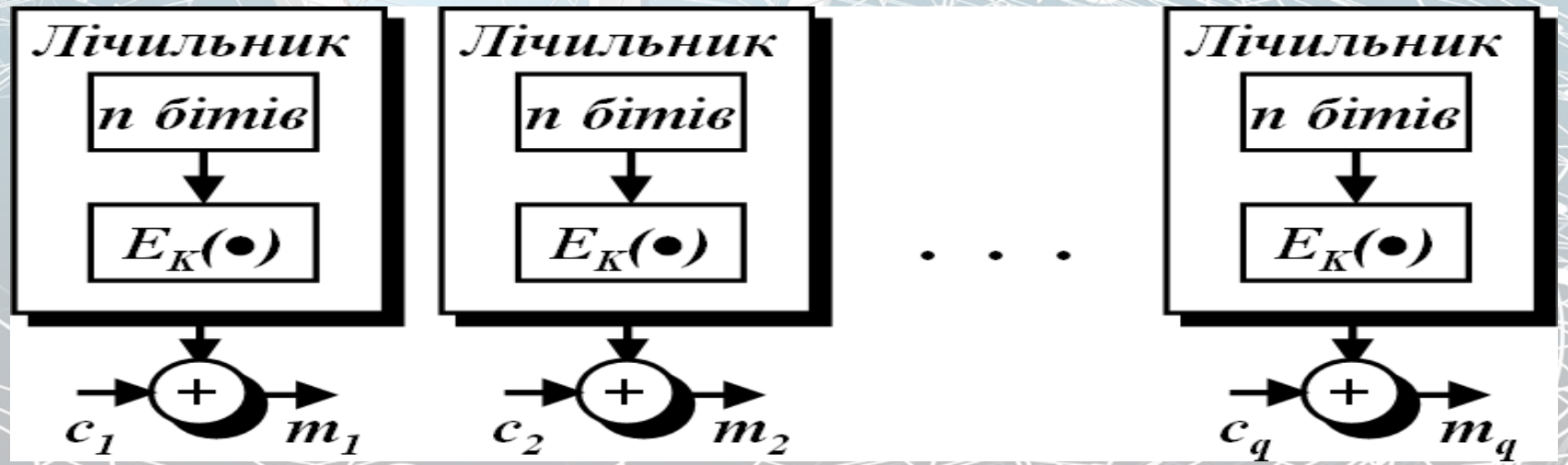


Вихідний зворотний зв'язок (OFB)

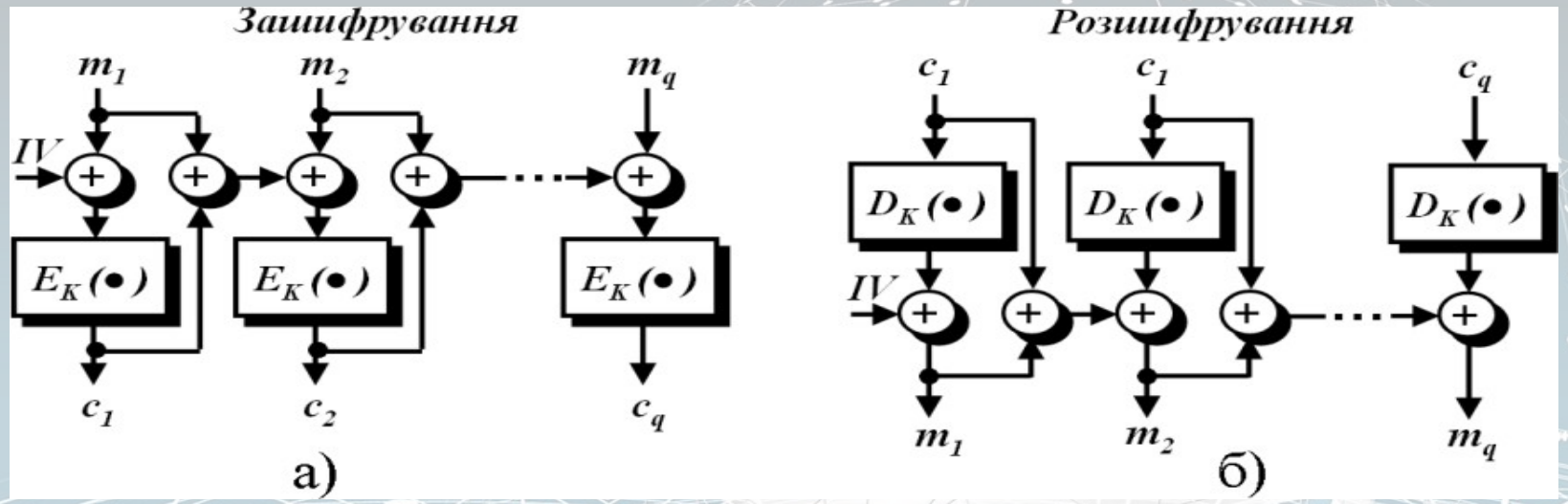


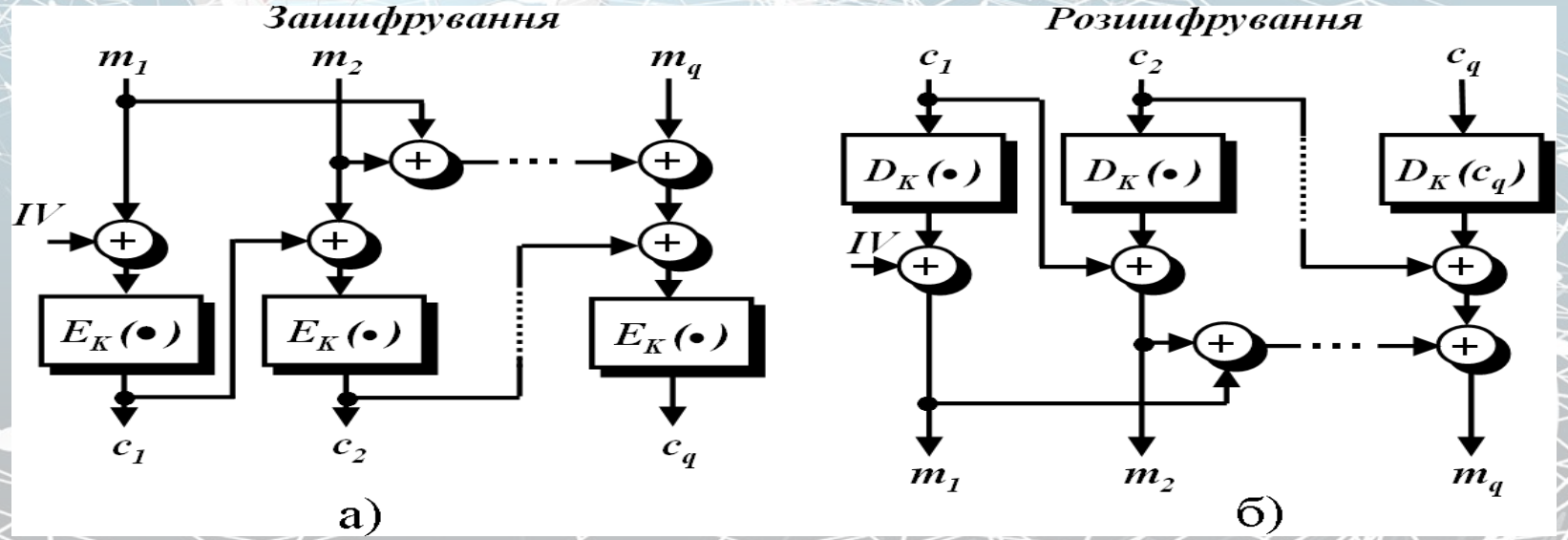
Режим лічильника (CTR)





Інші режими шифрування

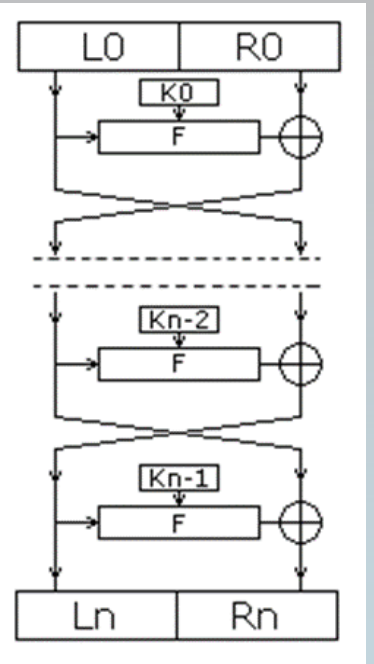




Мережа Фейстеля

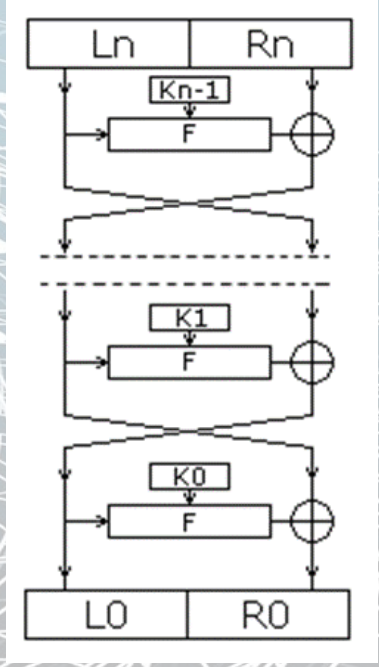
- блок відкритого тексту ділиться на 2 рівні частини (L та R)
- в кожному раунді вираховується (i=1,2 n} — номер раунду)

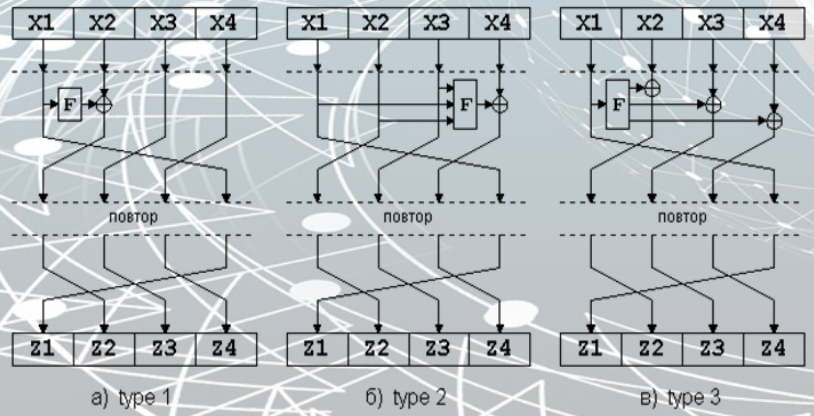
$$L_i = R_{i-1} \oplus f(L_{i-1}, K_{i-1})$$
$$R_i = L_{i-1}$$

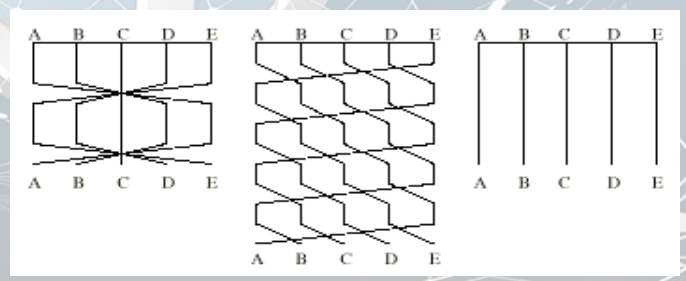


- розшифрування
- мережі Фейстеля з великою кількістю потоків

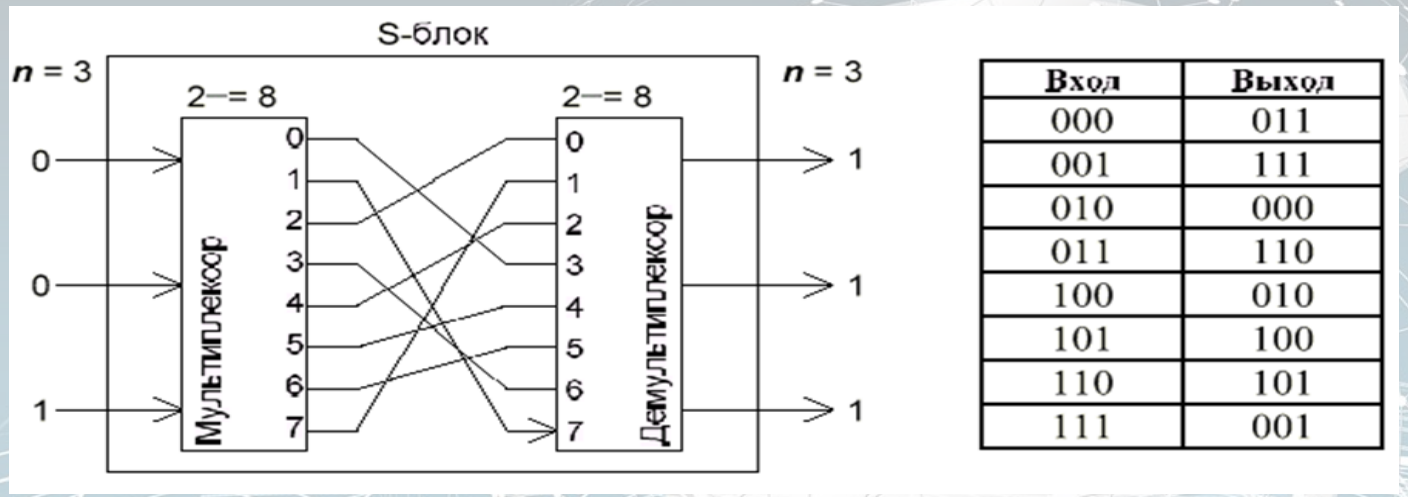
$$L_{i-1} = R_i \oplus f(L_i, K_{i-1})$$
$$R_{i-1} = L_i$$



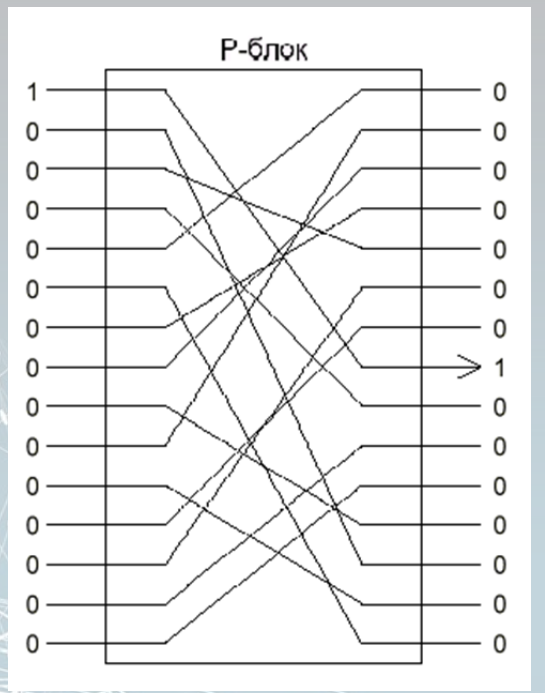


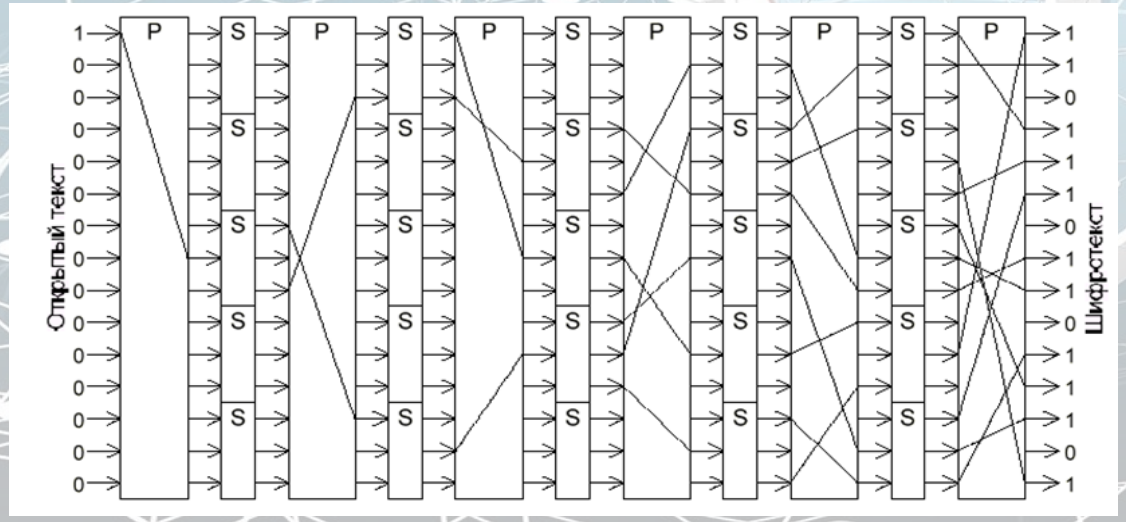


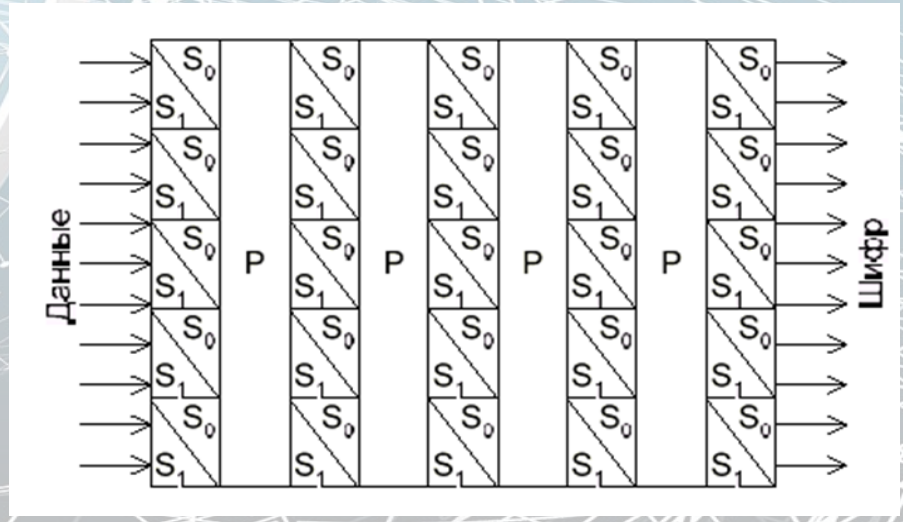
Шифр Lucifer фірми IBM



Вход	Выход
000	011
001	111
010	000
011	110
100	010
101	100
110	101
111	001







DES є американським стандартом шифрування даних

- Він використовує єдиний 56-бітний секретний ключ.
- Являє собою суперпозицію елементарних шифрів, що складається з 16 послідовних циклів шифрування
- У кожному проході використовується лише 48 біт ключа, але вони вибираються випадковим чином з повного 56-бітного ключа.
- використовується як для шифрування, так і для встановлення автентичності (аутентифікації) даних

Алгоритм DES

початкова перестановка

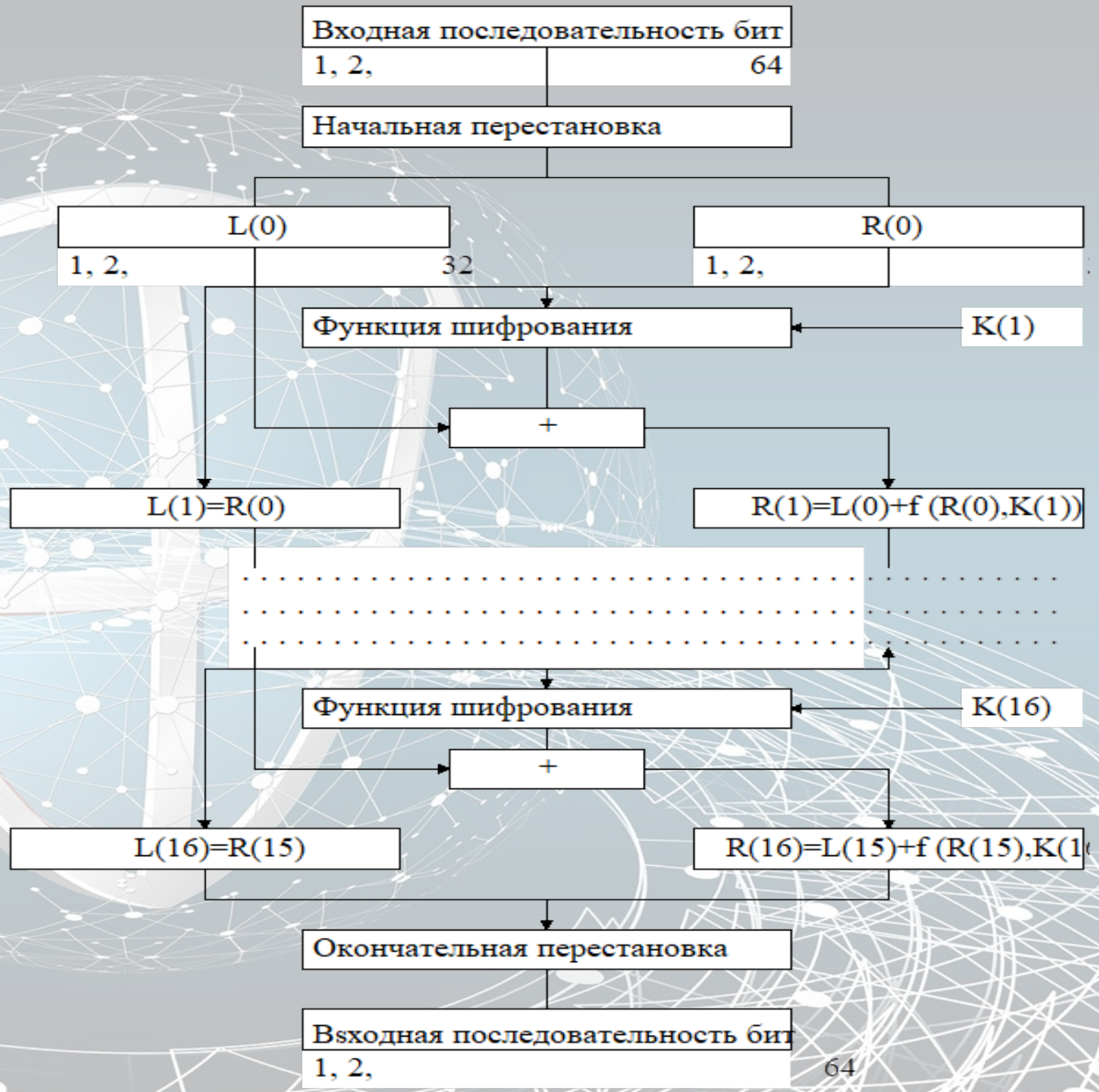
58	50	42	34	26	18	10
60	52	44	36	28	20	12
62	54	46	38	30	22	14
64	56	48	40	32	24	16
57	49	41	33	25	17	9
59	51	43	35	27	19	11
61	53	45	37	29	21	13
63	55	47	39	31	23	15

ітеративний процес шифрування

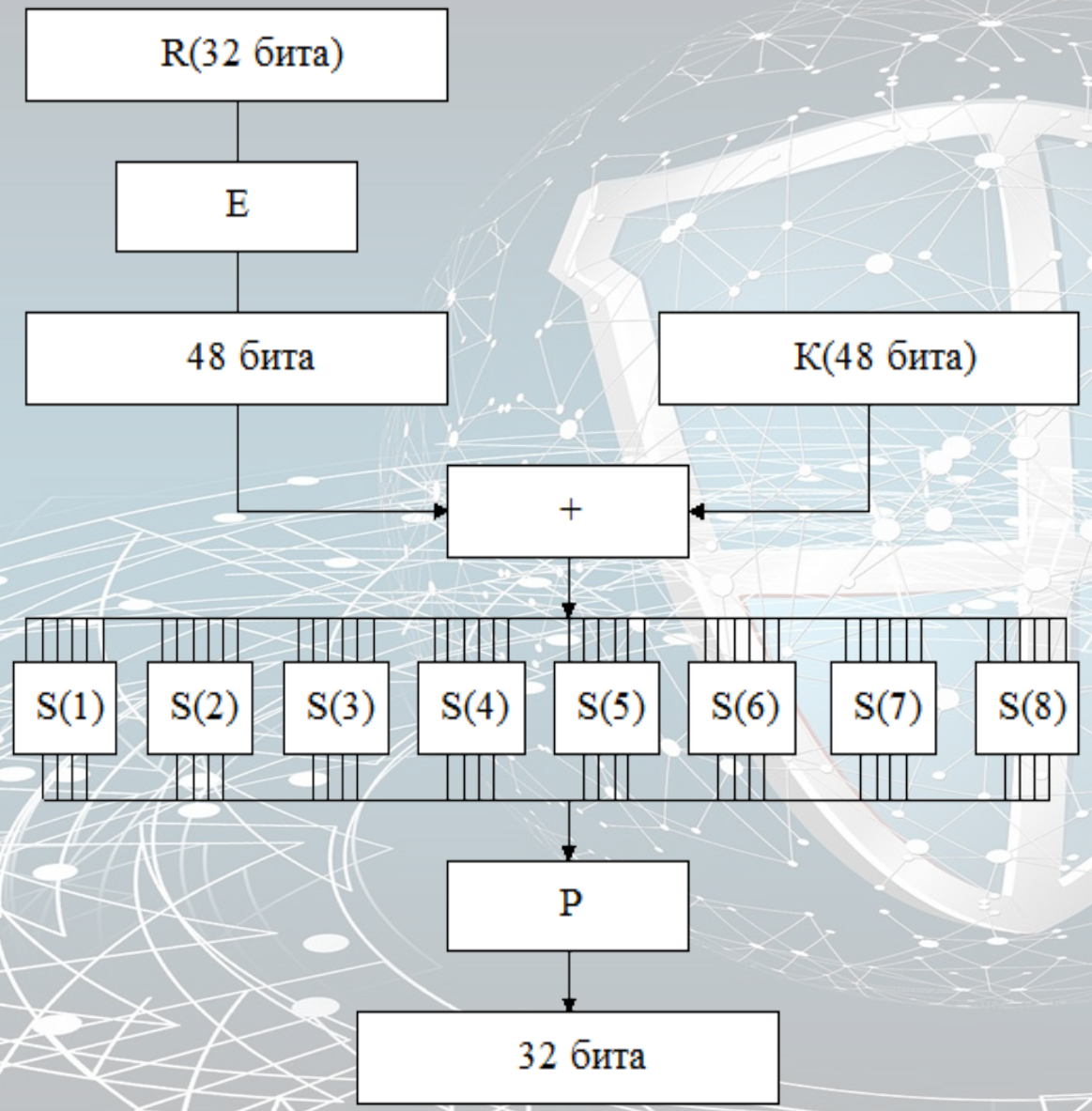
$$L_{(i)} = R(i-1),\ i = 1, 2, ..., 16;$$
$$R(i) = L(i-1) + f(R(i-1), K(i)),\ i = 1, 2, ..., 16.$$

остаточна перестановка

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



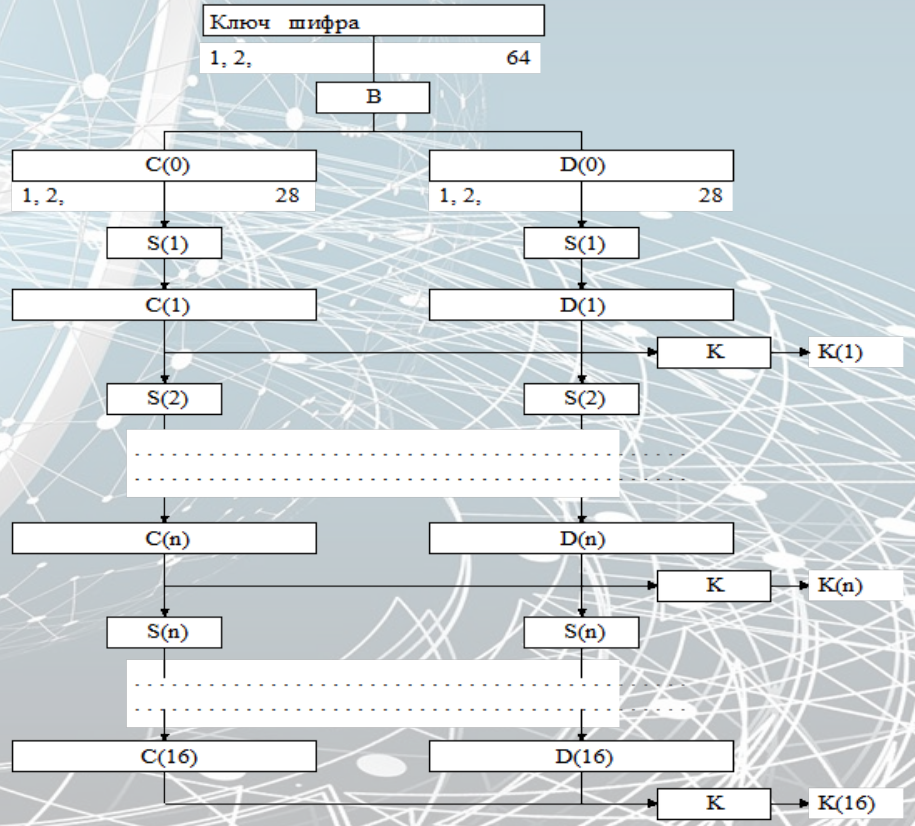
Функція шифрування f(R,K)



Функція розширення E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

алгоритм отримання ключів K(i),



Потрійний DES

Формула потрійного DES

- EK 1(DK2(EK1(Дані8))),
- EK1 - DES Encryption операція по ключу K1,
- DK2 - операція розшифровки DES по ключу K2,
- Data8 - дані довжиною 8 байт.

Види потрійного шифрування DES:

- DES-EEE3: Зашифровано 3 рази за допомогою 3 різних ключів.
- DES-EDE3: 3 операції шифрування-дешифрування-шифрування DES з 3 різними ключами.
- DES-EEE2 і DES-EDE2: Як і попередні, за винятком того, що перша і третя операції використовують один і той же ключ

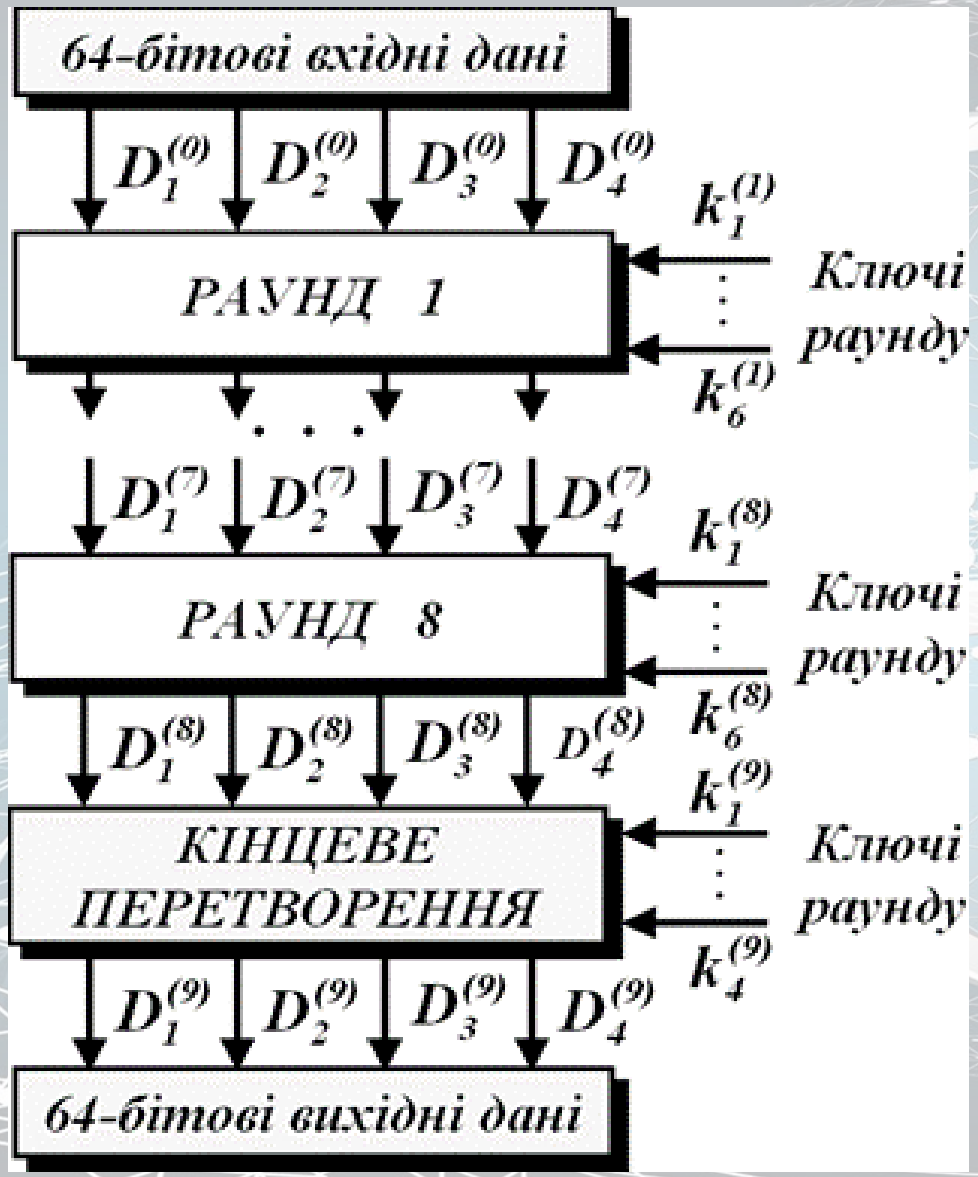
Шифрування	Клавіші	Обчислення	Зберігання	Тип атаки
Одного	1	2^56	-	відомий відкритий текст
Одного	1	2^38	2^38	Вибраний відкритий текст
Одного	1	-	2^56	Вибраний відкритий текст
Подвійний	2	2^112	-	відомий відкритий текст
Подвійний	2	2^56	2^56	відомий відкритий текст
Подвійний	2	-	2^112	Вибраний відкритий текст
Тримісний	2	2^112	-	відомий відкритий текст
Тримісний	2	2^56	2^56	2^56 Вибраний відкритий текст
Тримісний	2	2^(120-т)	-	2^t відомий відкритий текст
Тримісний	2	-	2^56	Вибраний відкритий текст
Тримісний	3	2^112	2^56	відомий відкритий текст
Тримісний	3	2^56	2^112	Вибраний відкритий текст

International data encryption algorithm (IDEA)

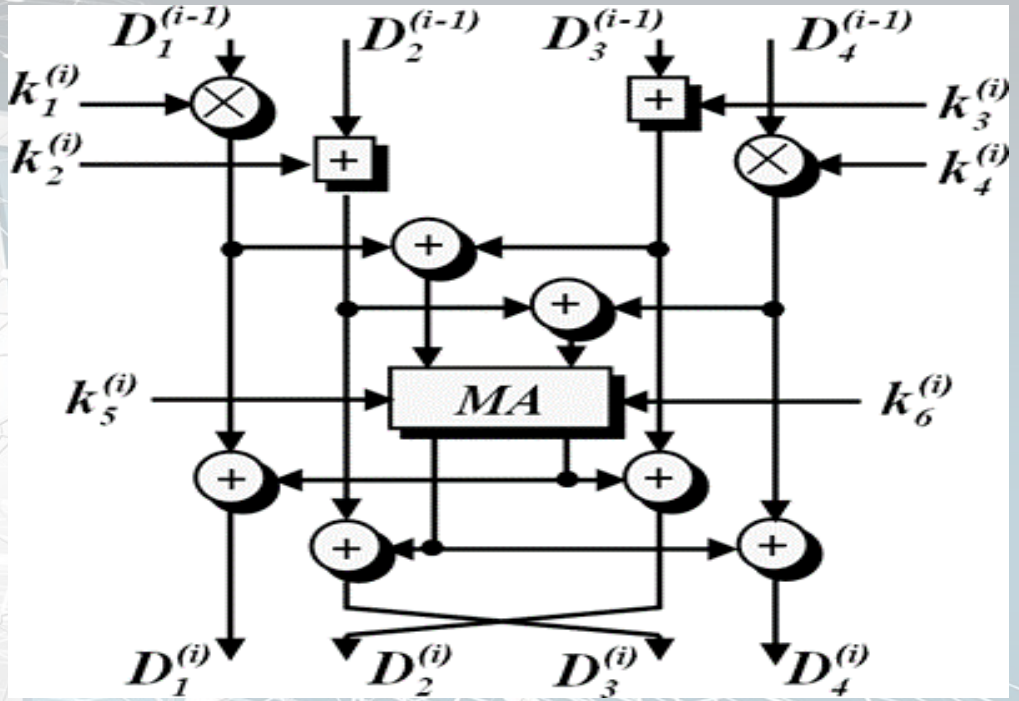
Характеристики IDEA, що характеризують криптографічну стій- кість алгоритму:

- довжина блока повинна бути достатньою, щоб приховати всі статистичні характеристики початкового повідом- лення. З іншого боку, складність реалізації криптографічної функції зростає експоненціально відповідно до розміру блока. Використання блока розміром у 64 біти в 90-ті рр. XX ст. означало достатню силу. Більше того, використання режиму шифрування CBC гово- рить про подальше посилення цього аспекту алгоритму;
- довжина ключа повинна бути досить великою для того, щоб запобігти можливості простого перебору ключа. За довжини ключа 128 бітів IDEA вважається досить безпечним;
- зашифровані дані повинні залежати від ключа склад- ним і заплутаним способом;
- кожний біт початкових даних повинен впливати на кож- ний біт зашифрованих даних. Поширення одного незашифрованого біта на велику кількість зашифрованих бітів приховує статистичну структуру початкових даних. Визначити, як статистичні характери- стики зашифрованих даних залежать від статистичних характерис- тик початкових даних, повинно бути непросто. IDEA з цього погля- ду є дуже ефективним алгоритмом.

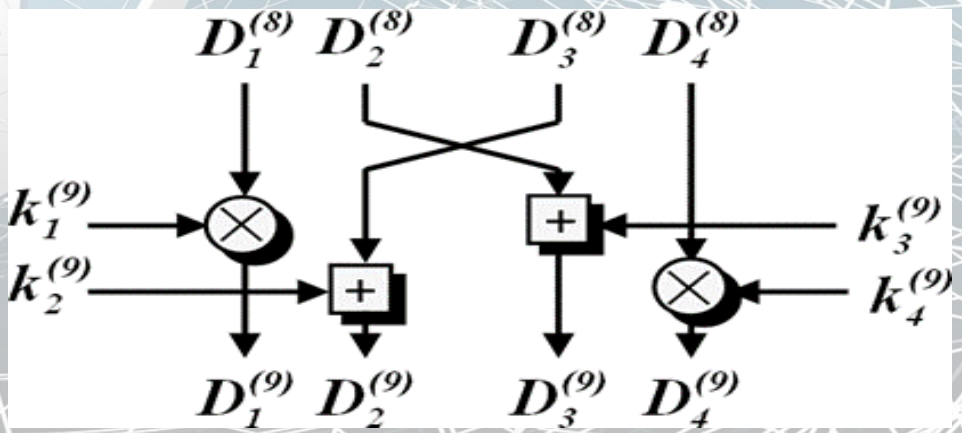
Структура алгоритму IDEA



Один раунд перетворення даних в IDEA



Кінцеве перетворення (раунд 9) в IDEA

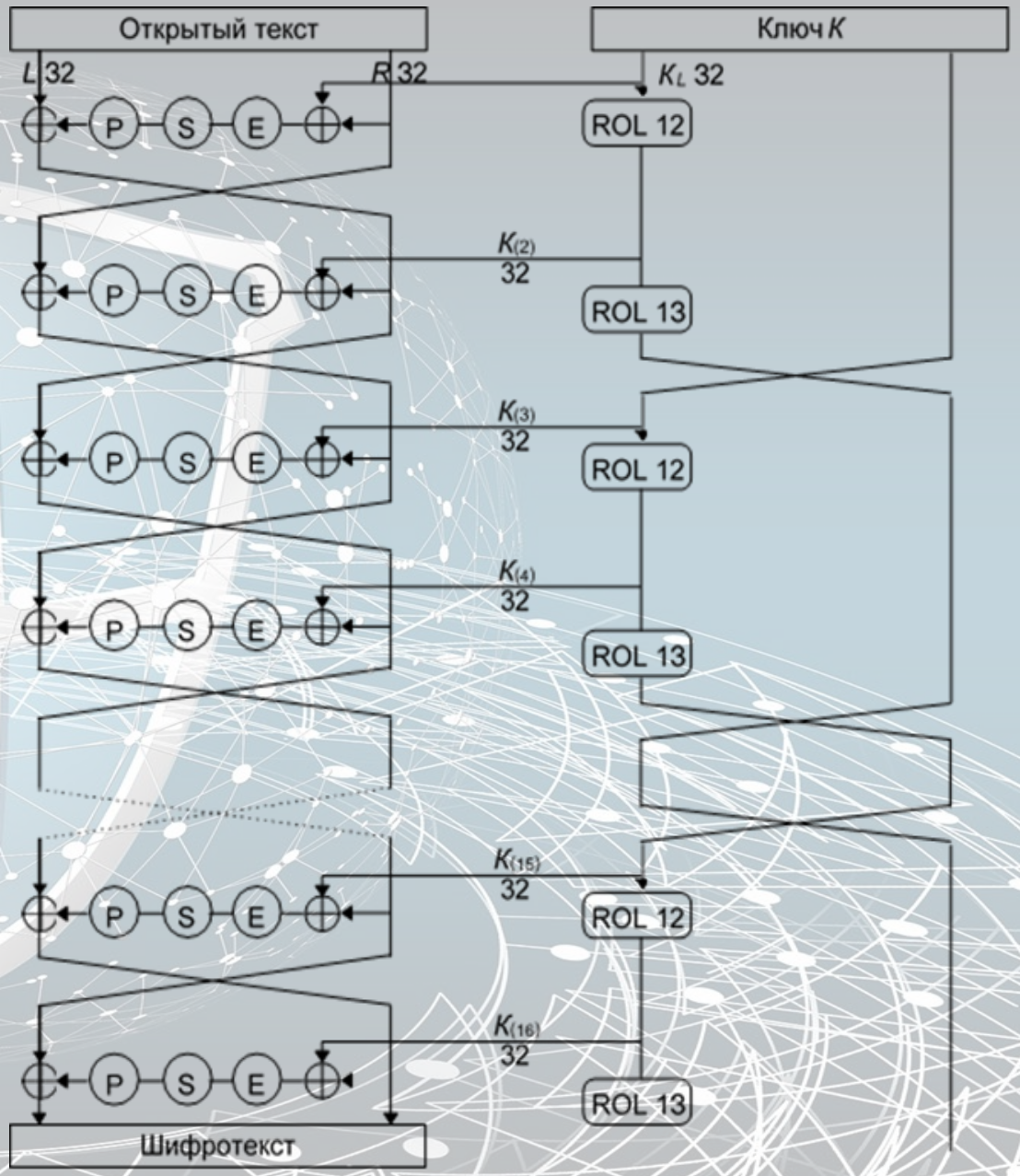


Процес отримання раундових ключів зашифрування

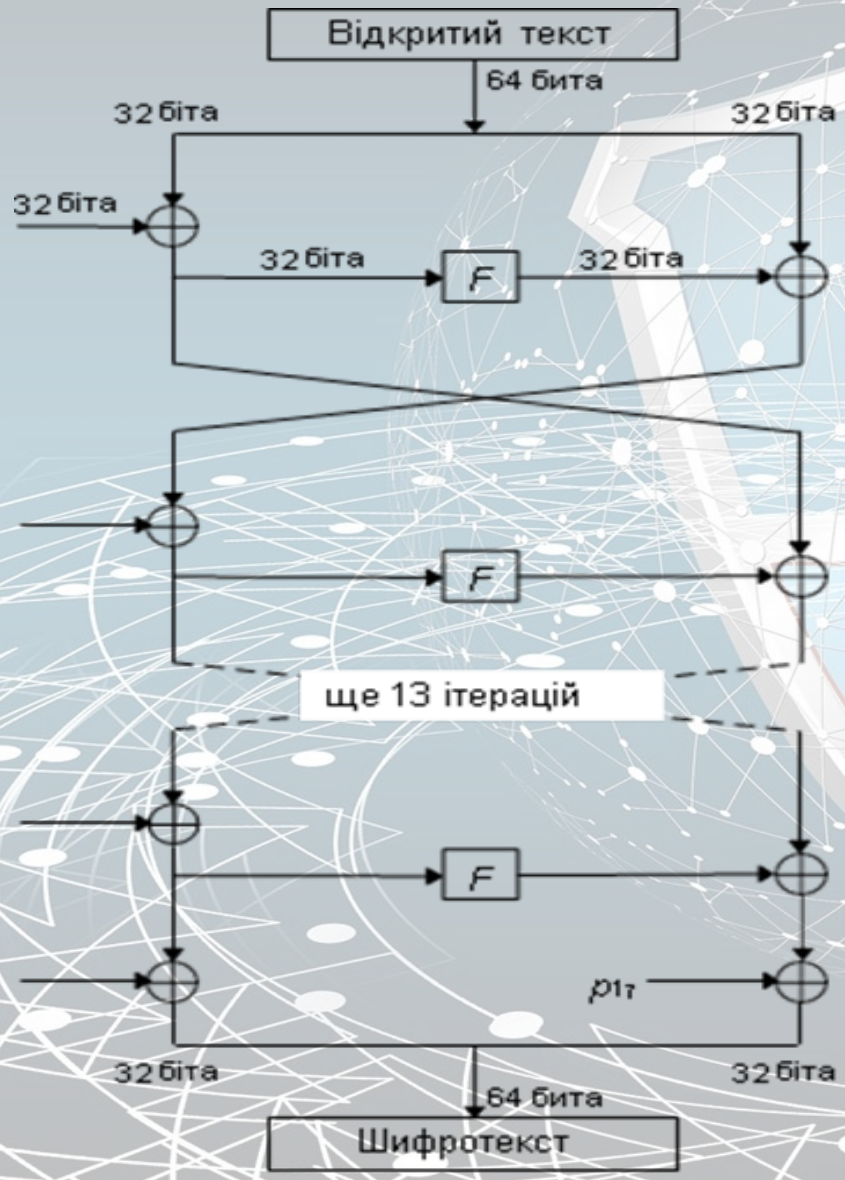


LOKI

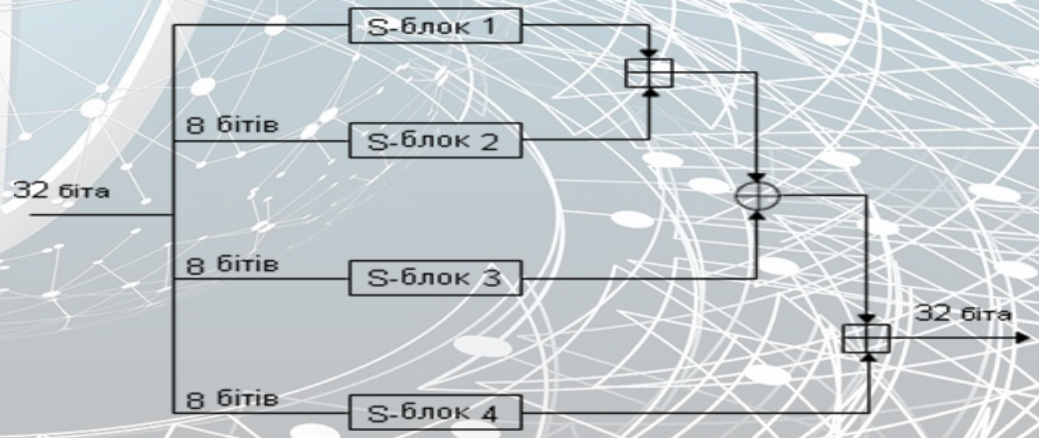
- Алгоритм генерації підз'єднань був змінений таким чином, що половинки переставляються після кожного другого кроку, а не кожного кроку.
- Алгоритм генерації підз'єднань змінено таким чином, що кількість позицій циклічного зсуву l-з'єднання становить або 12, або 13 біт.
- Початкові та кінцеві операції HOR блоку та ключа були усунені.
- Функція S-блоку була змінена для того, щоб згладити профілі CHOR S-блоків (щоб зробити їх більш чутливими до диференціального криптоаналізу) і запобігти використанню f(x) = O для значення, де f є комбінацією E-, S- і P-блоків.



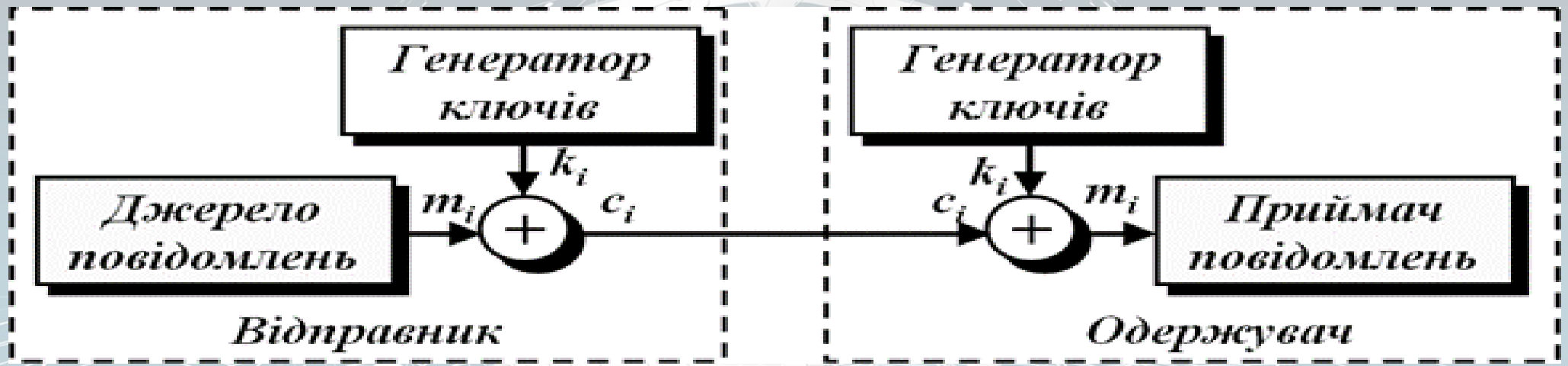
Blowfish



- Скорость. Blowfish шифрует данные на 32-битовых микропроцессорах со скоростью 26 тактов на байт.
- Компактность. Blowfish может работать менее, чем в 5 Кбайт памяти.
- Простота. Blowfish использует только простые операции: сложение, XOR и выборка из таблицы по 32- битовому операнду. Анализ его схемы несложен, что делает при реализации алгоритма уменьшает к о- личество ошибок [1391].
- Настраиваемая безопасность. Длина ключа Blowfish переменна и может достигать 448 битов



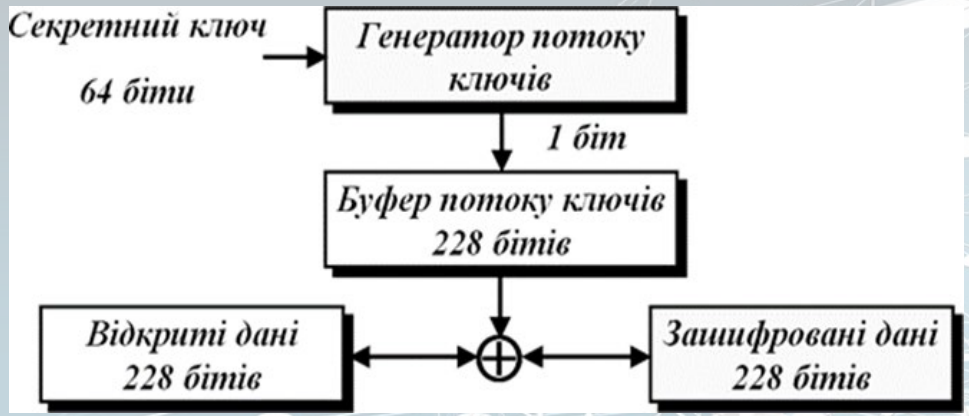
Потокові шифри



Для використання з криптографічною метою ГПВЧ повинен мати такі властивості:

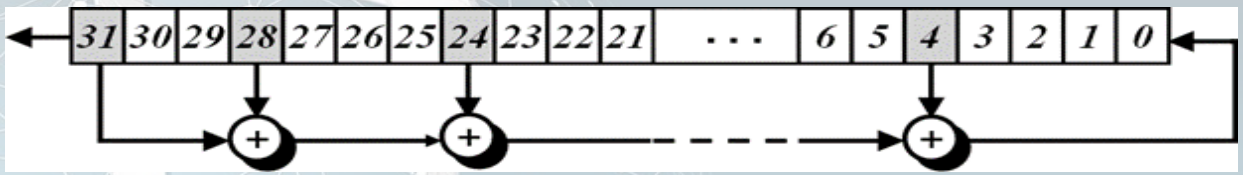
- період послідовності повинен бути дуже великим;
- породжувана послідовність не повинна відрізнятися від дійсно випадкової;
- ймовірності появи (породження) різних значень повинні бути точно рівні;
- для того, щоб тільки законний одержувач міг розшифрувати повідомлення, слід під час отримання потоку ключових бітів ki використовувати та враховувати певний секретний ключ, причому обчислення числа ki+1 за відомими попередніми елементами послідовності ki без знання ключа повинно бути важким завданням

Потоковий шифр А5

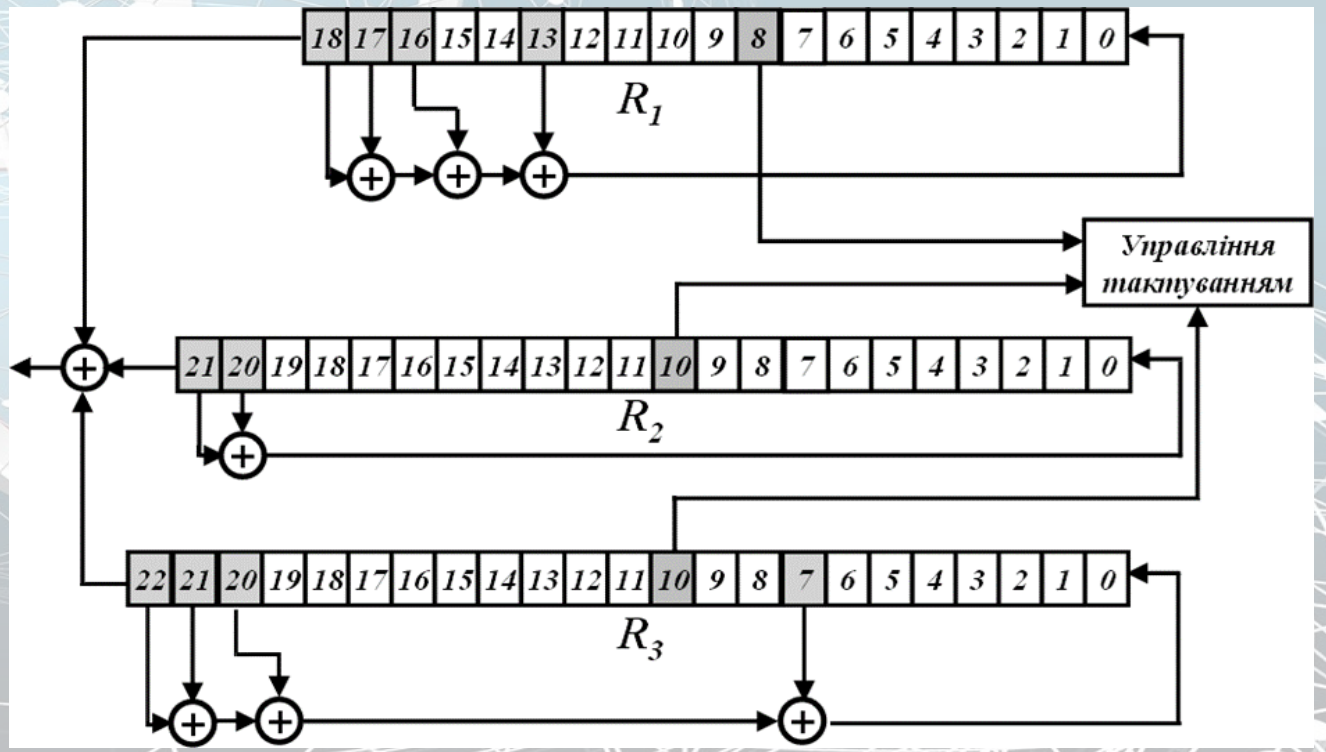


Принцип побудови алгоритму потокового зашифрування (розшифрування) даних А5

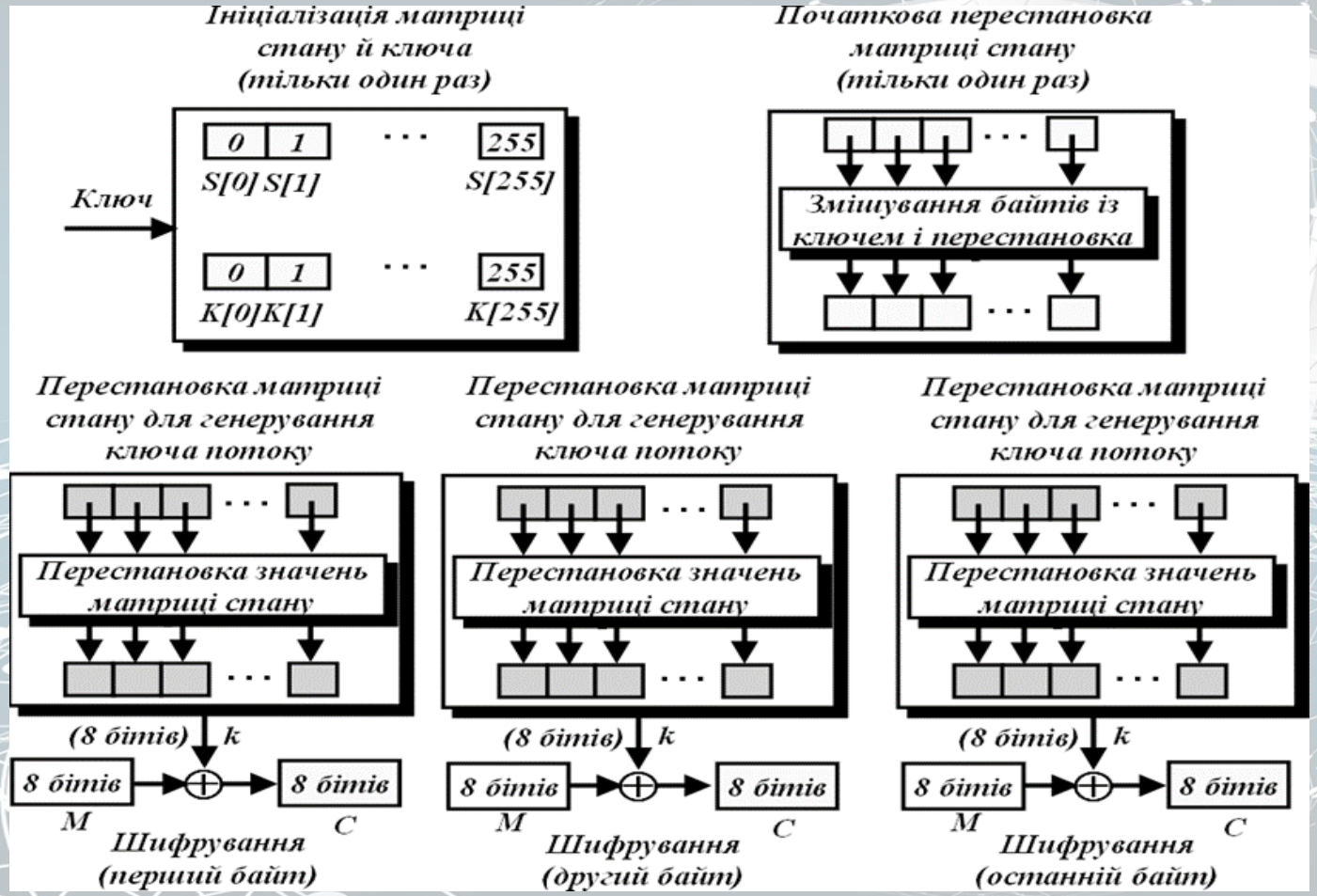
LFSR із багаточленом зворотного зв'язку



Структура система LFSR в алгоритмі А5



Потоковий шифр RC4



Принцип побудови шифру потоку RC4

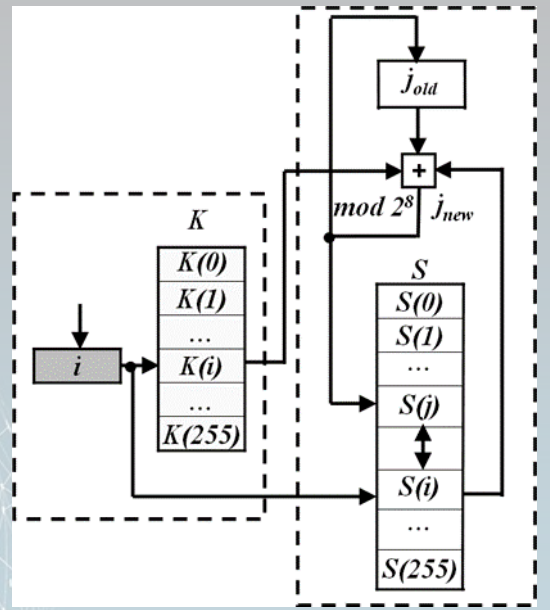
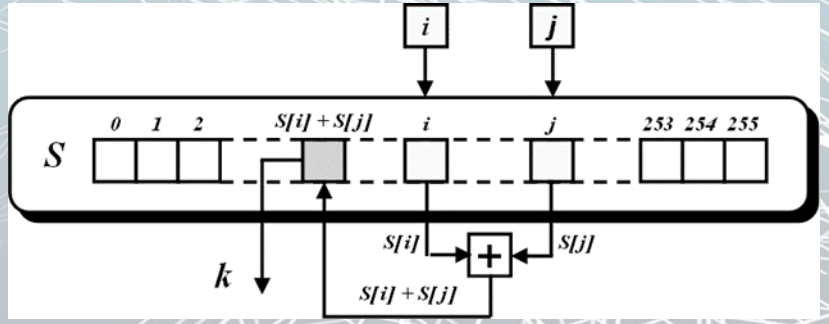


Схема ініціалізації таблиці замін S і масиву ключа K



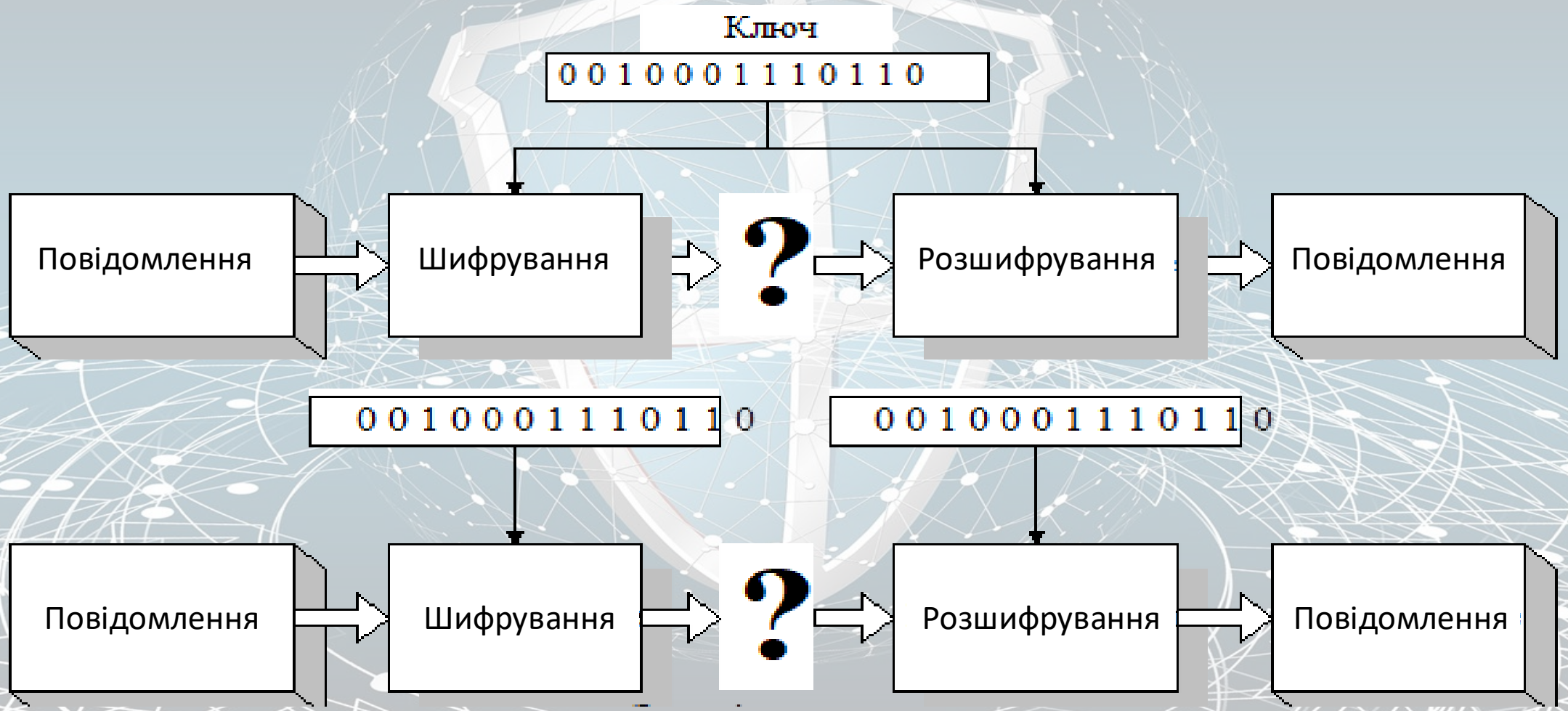
Ядро алгоритму RC4



Криптографія

Системи з відкритими ключима

Симетричне та асиметрічне шифрування



Основні положення

Шифрування-розшифровка інформації здійснюється за допомогою двох ключів:

- секретний ключ, який використовується для розшифровки отриманої інформації та здійснення електронного підпису при відправці інформації, секретний ключ зберігається на одній машині і закритий для використання сторонніми особами;
- відкритий ключ, який використовується для шифрування інформації, що відправляється і управління електронним підписом, відкритий ключ може вільно поширюватися по відкритих каналах.

Тому, щоб гарантувати надійний захист інформації, до систем з відкритим ключем (SOC) пред'являються дві важливі і очевидні вимоги:

- Перетворення вихідного тексту повинно бути незворотнім і виключати його відновлення на основі відкритого ключа.
- Визначення закритого ключа на основі відкритого ключа також має бути неможливим на сучасному технологічному рівні. При цьому бажана точна менша оцінка складності (кількості операцій) розкриття шифру.

Задіювання СВК

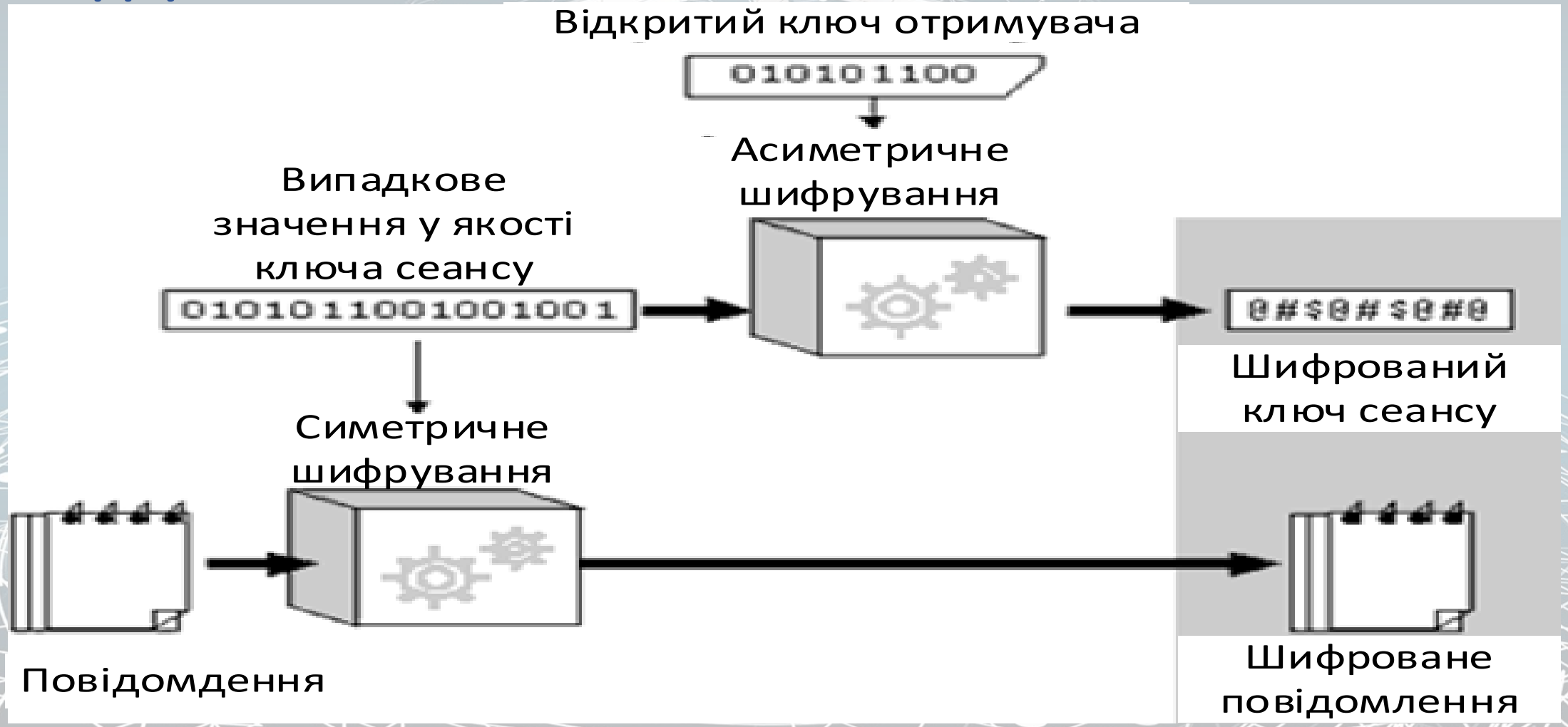
Криптосистеми з відкритим ключем, запропоновані сьогодні, покладаються на один з наступних типів незворотних перетворень:

- Розкладання великих чисел на простих множниках.
- Обчислення логарифма в кінцевому полі.
- Обчислення коренів алгебраїчних рівнянь

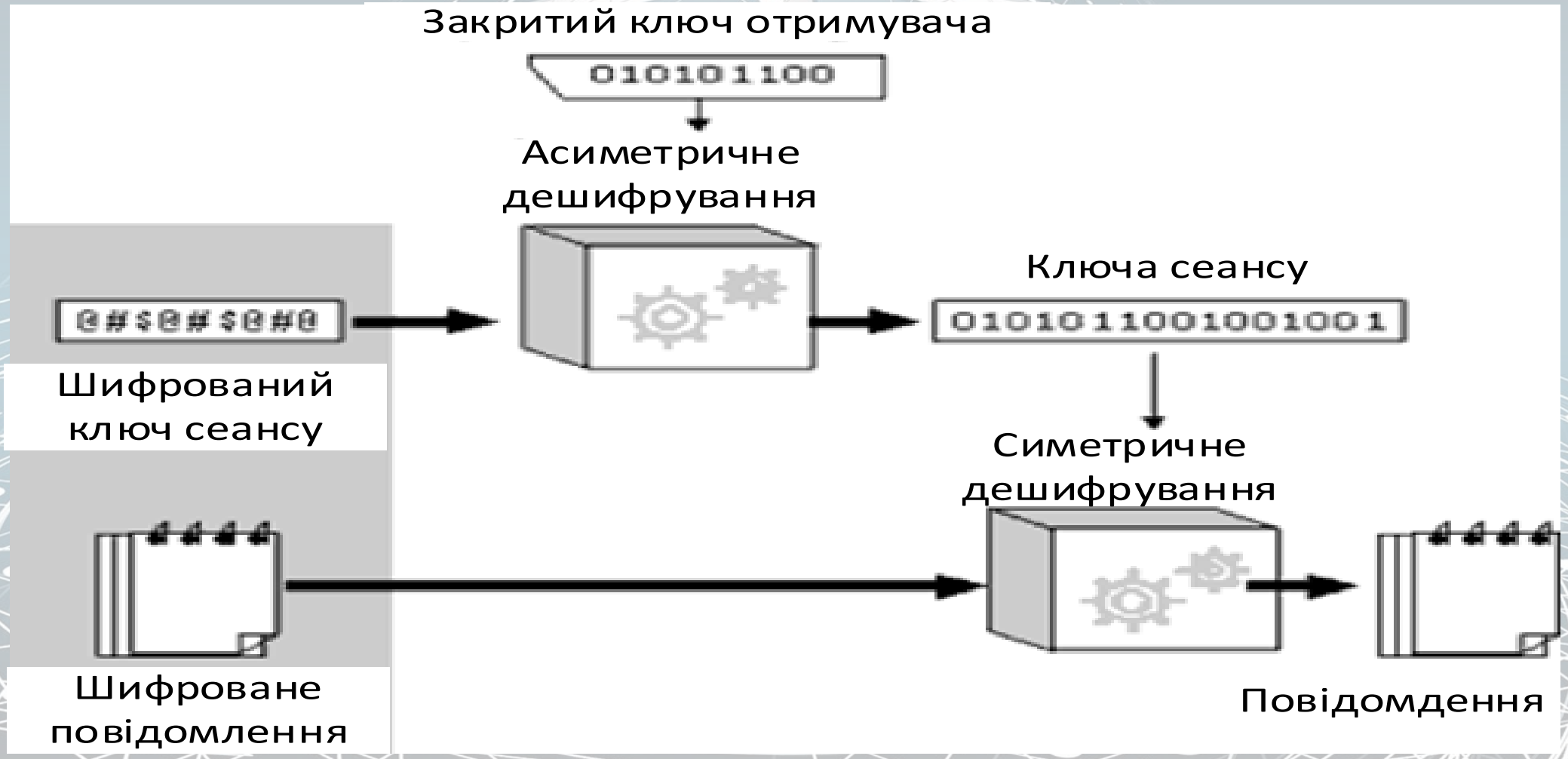
Алгоритми криптосистеми з відкритим ключем (СВК) можуть використовуватися для трьох цілей.

- Як самостійний засіб захисту переданих і збережених даних.
- Як засіб розподілу ключів. Алгоритми SOC більш трудомісткі, ніж традиційні криптосистеми. Тому часто на практиці раціонально розподіляти ключі за допомогою SOC, кількість яких в якості інформації незначно. А потім за допомогою звичайних алгоритмів обмінюються великими інформаційними потоками.
- Засоби аутентифікації користувачів. Електронний підпис.

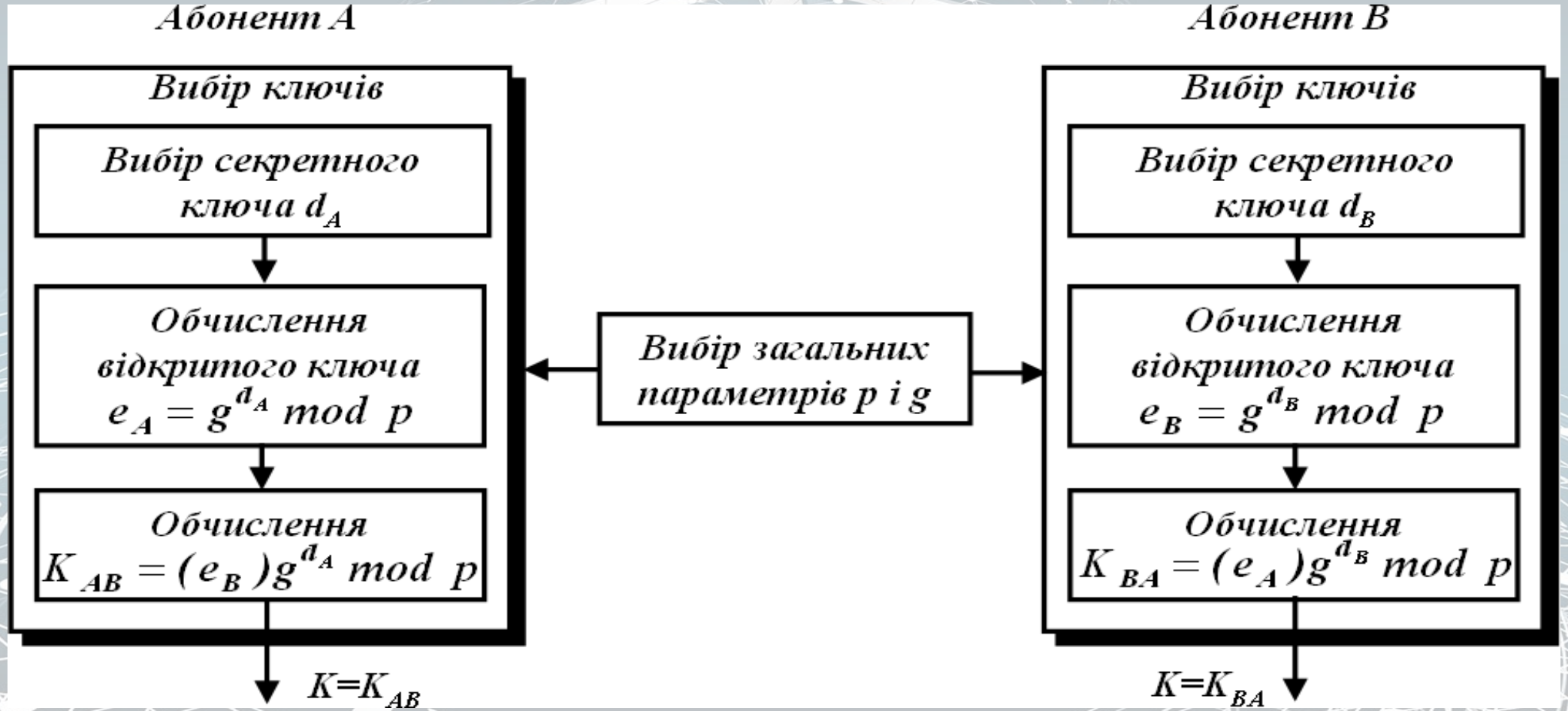
Використання СВК для симетричного шифрування



Використання СВК для симетричного дешифрування



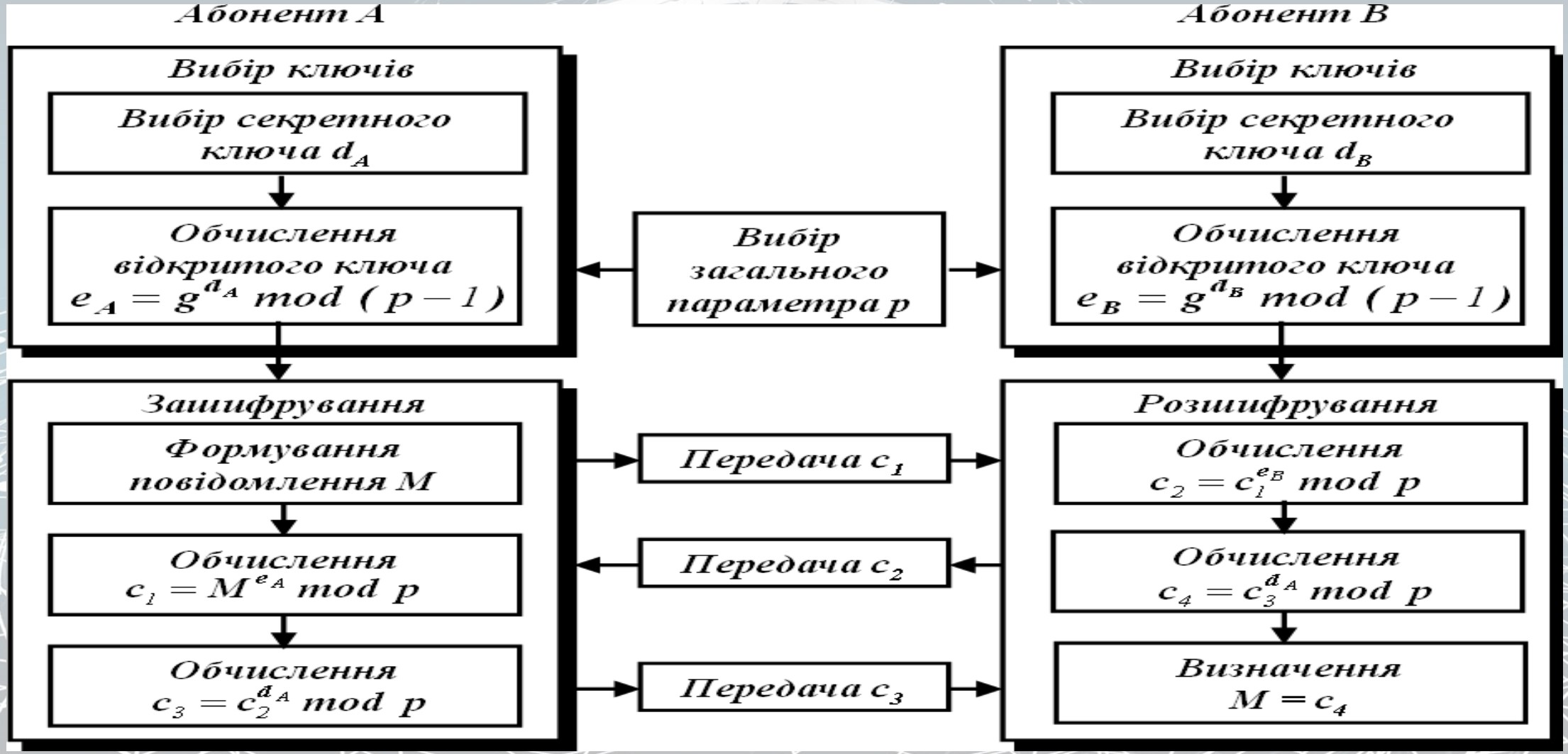
Алгоритм Діффі-Хеллмана



$Z_{AB} = (y_B)^A \bmod p$.

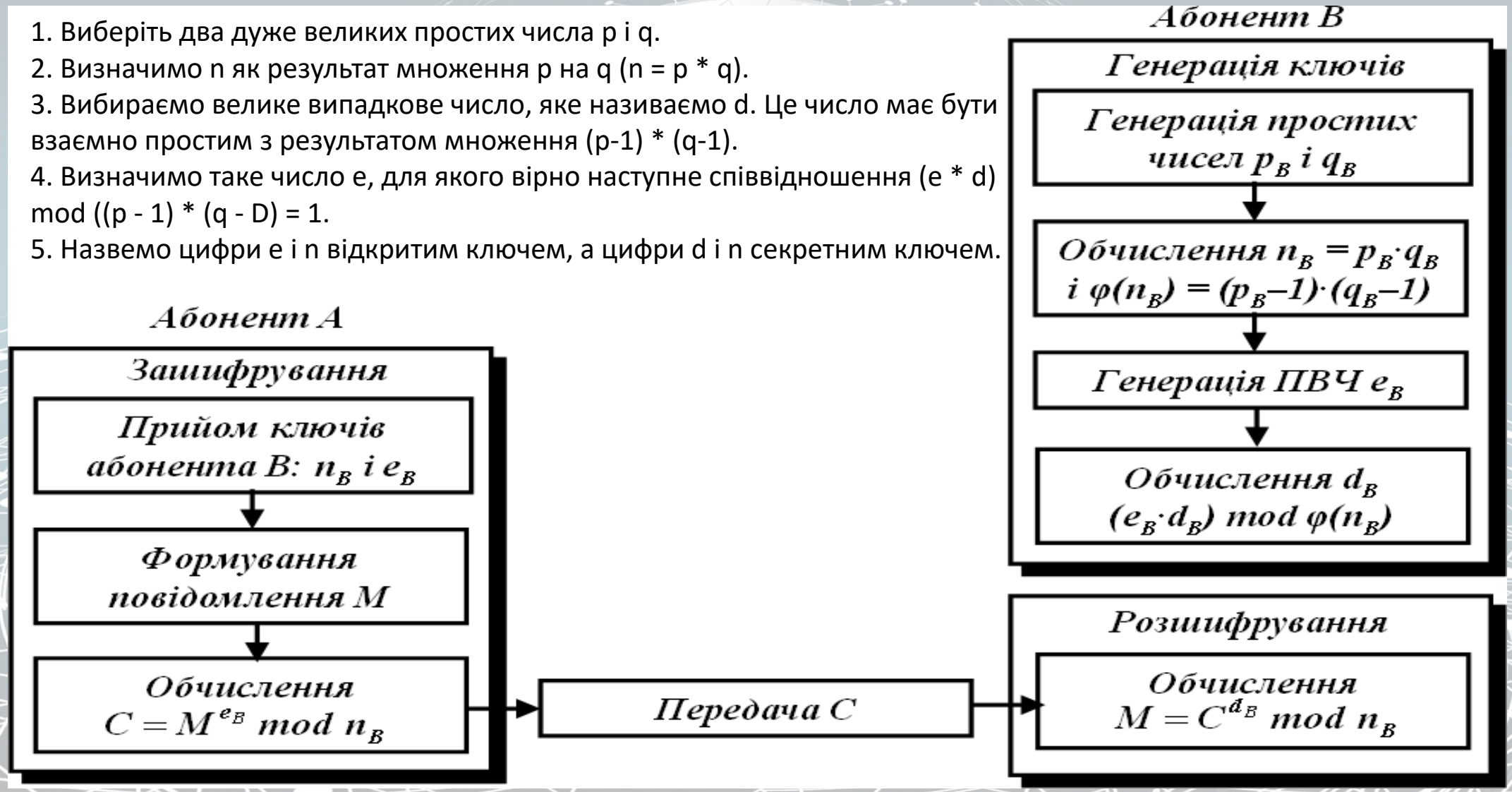
$Z_{BA} = (y_A)^B \bmod p$.

Криптографічна система ШАМІРА



Алгоритм RSA

1. Виберіть два дуже великих простих числа p і q.
2. Визначимо n як результат множення p на q (n = p * q).
3. Вибираємо велике випадкове число, яке називаємо d. Це число має бути взаємно простим з результатом множення (p-1) * (q-1).
4. Визначимо таке число e, для якого вірно наступне співвідношення (e * d) mod ((p - 1) * (q - D) = 1.
5. Назвемо цифри e і n відкритим ключем, а цифри d і n секретним ключем.



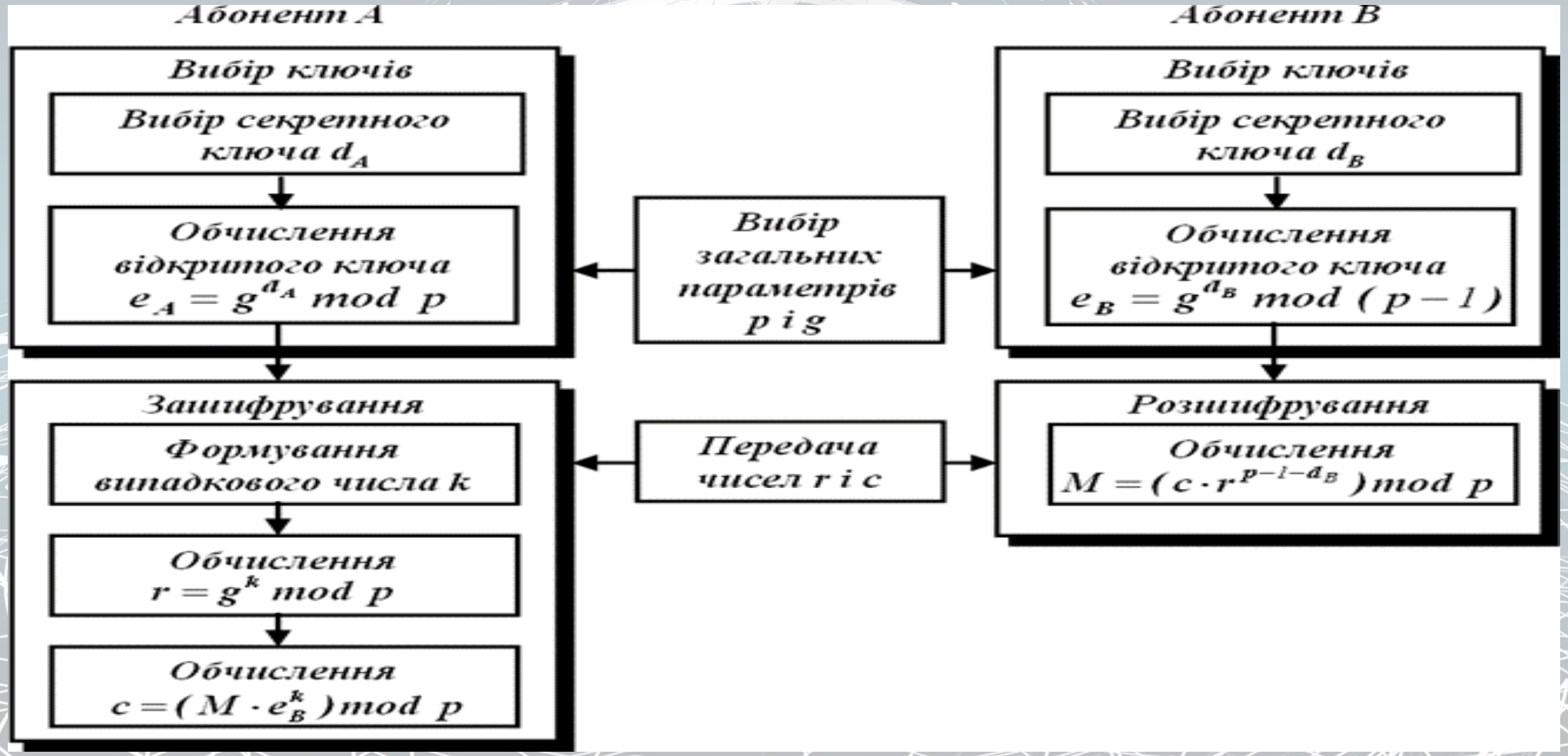
Приклад RSA

- 1. Виберіть p = 3 і q = 11.
- 2. Визначте n = 3 * 11 = 33.
- 3. Знайти (p-1) * (q-1) = 20. Тому в якості d вибираємо будь-яке число, взаємно просте з 20, наприклад, d = 3.
- 4. Виберемо число e. В якості такого числа можна взяти будь-яке число, для якого задовольняється співвідношення (e * 3) mod 20 = 1, наприклад 7.

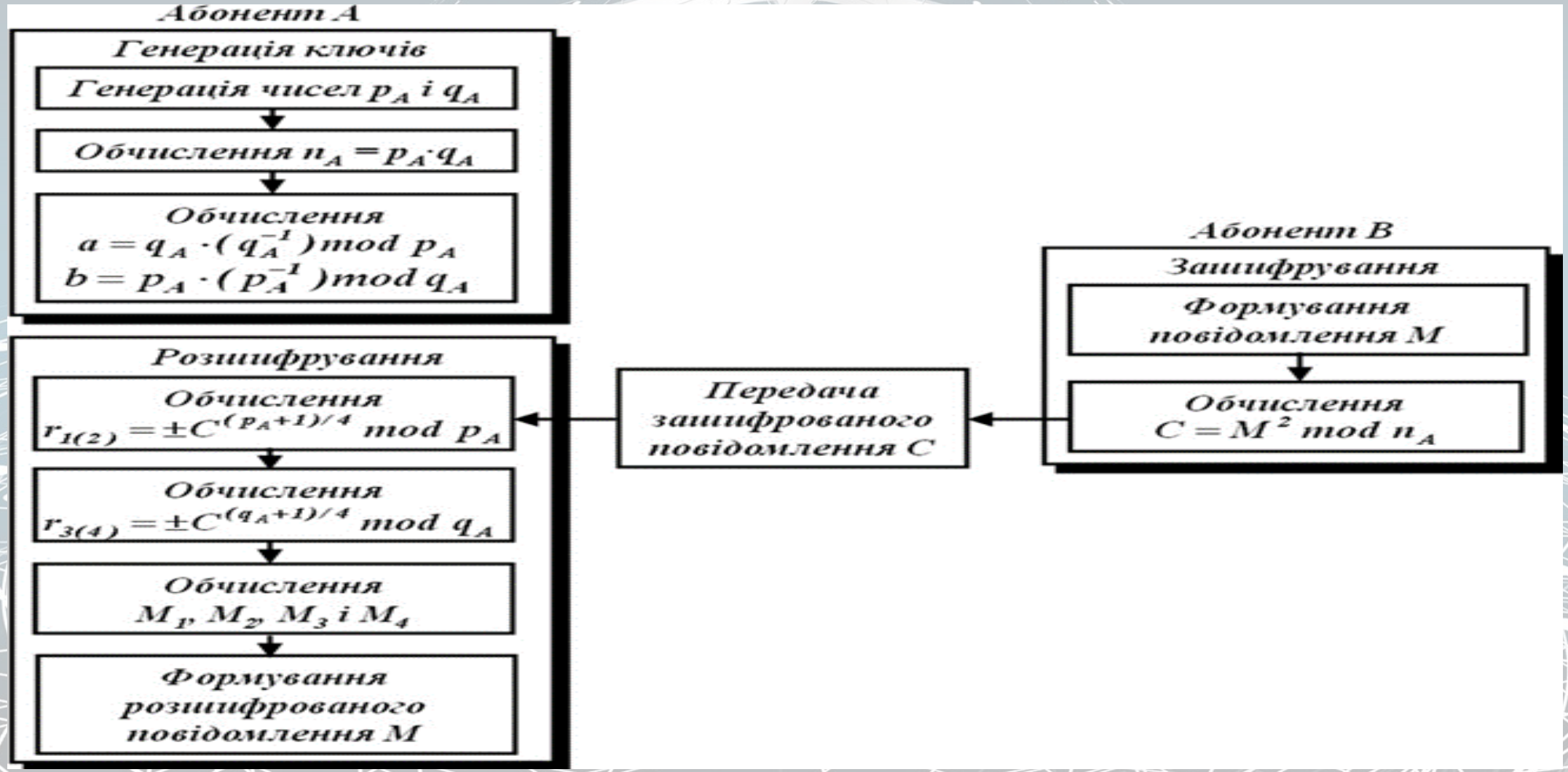
Уявімо зашифроване повідомлення у вигляді послідовності цілих чисел в діапазоні 0 ... 32. Нехай буква A представлена цифрою 1, буква B - цифрою 2, а буква C - цифрою 3. Тоді повідомлення можна представити у вигляді послідовності цифр 3, 1, 2. Зашифрувати повідомлення за допомогою ключа {7, 33}:

- Cl = (37) mod 33 = 2187 mod 33 = 9,
- C2 = (17) mod 33 = 1 mod 33 = 1,
- C3 = (27) мод 33 = 128 мод 33 = 29.
- 6. Спробуємо розшифрувати повідомлення {9, 1, 29}, отримане в результаті шифрування відомим ключем, на основі секретного ключа {3, 33}:
- M1 = (97) мод 33 = 729 мод 33 = 3,
- M2 = (17) mod 33 = 1 mod 33 = 1,
- M3 - (297) мод 33 = 24389 мод 33 = 2.

Криптосистема Ель-Гамаль



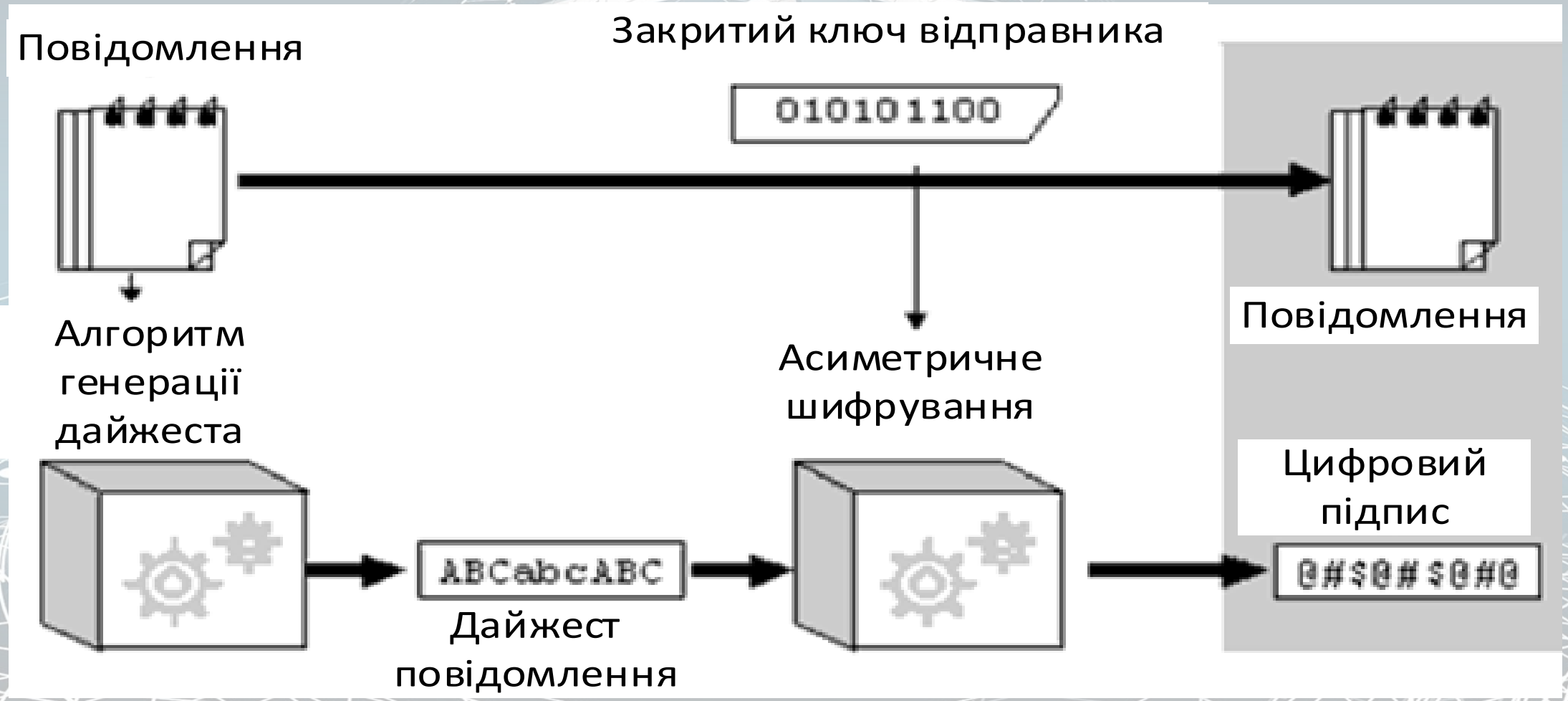
Криптографічна система РАБІНА



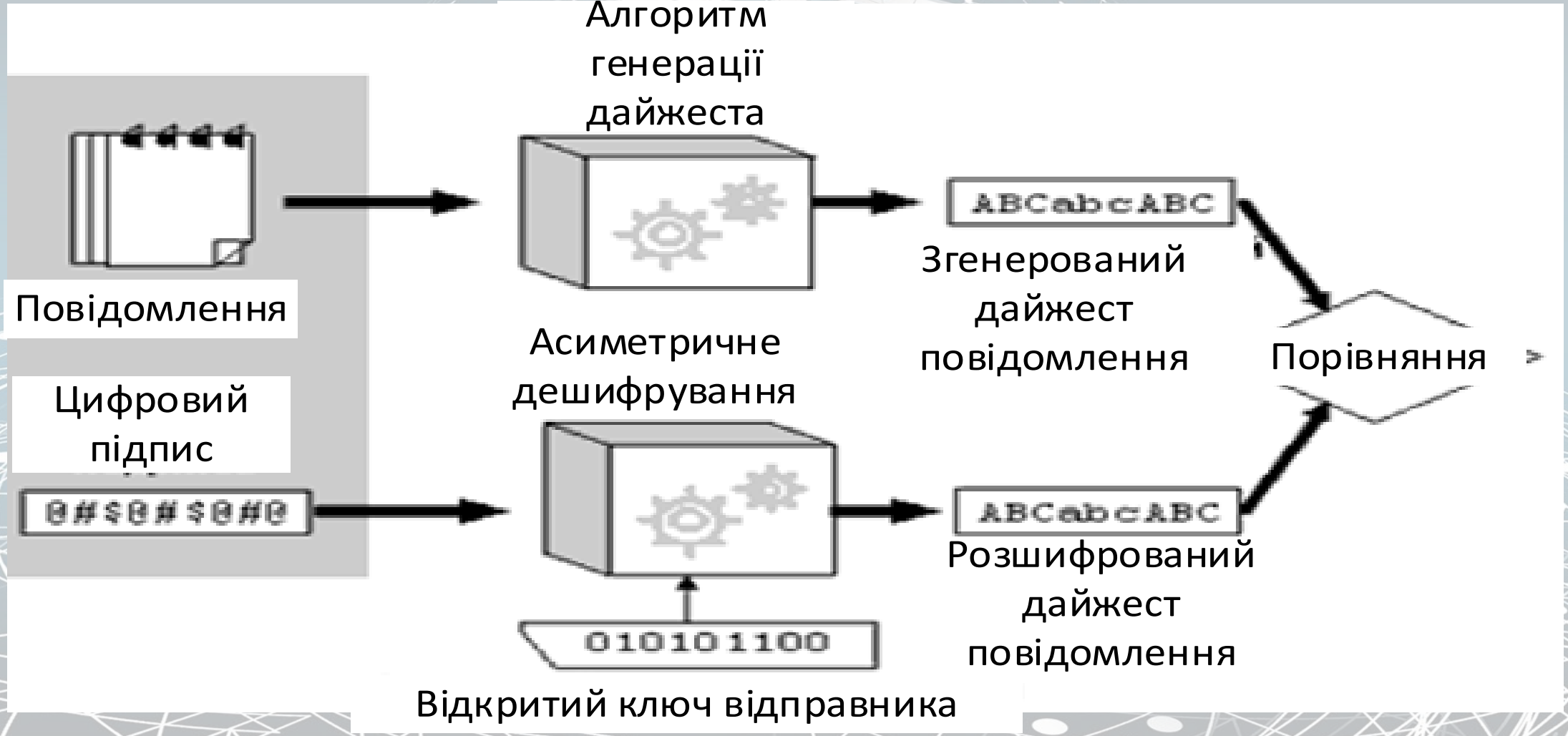
Які порушення і дії зловмисника повинна захищати система аутентифікації

- Відмова (ренегат).
- Модифікація (переробка).
- Підробки.
- Активне перехоплення.
- Маскування (імітація).
- Повторення.

Формування повідомлення з цифровим підписом



Перевірка цифрового підпису





Криптографія

Частина 3

Управління ключами

- генерація ключів;
- розподіл ключів;
- зберігання ключів;
- заміна ключів;
- депонування ключів;
- знищення ключів.

Розрядність ключа

- складність атаки грубою силою;
- необхідна продуктивність криптографічного алгоритму в тих випадках, коли збільшення розміру ключа збільшує час виконання операцій шифрування;
- термін служби інформації, що захищається, та її цінність;
- можливості противника.

Довжина ключа, біти

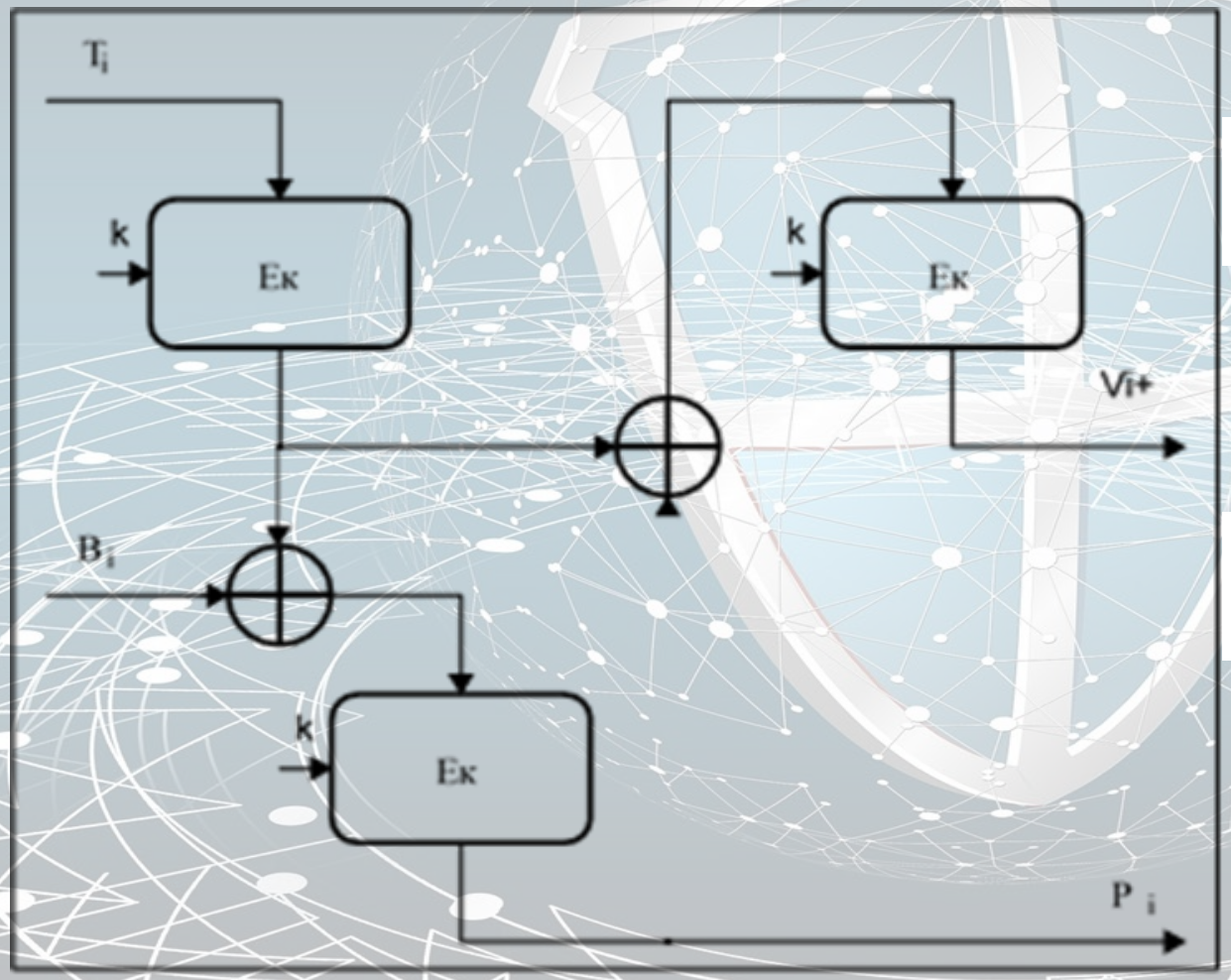
Криптосистема з закритим ключем	Криптосистема з відкритим ключем
56	384
64	512
80	768
112	1792
128	2304

Генерація ключів

Для генерації ключової інформації для використання в симетричній криптосистемі використовуються наступні методи (в порядку підвищення якості):

- генерація програмного забезпечення, яка передбачає обчислення чергового псевдовипадкового числа як функції поточного часу, послідовності символів, що вводяться користувачем, особливостей його клавіатурного почерку і т.д;
- генерація програмного забезпечення на основі моделювання якісного генератора PSP з єдиним законом розподілу;
- генерація обладнання за допомогою якісного генератора PSP;
- генерація обладнання з використанням генераторів випадкових послідовностей, побудованих на основі фізичних генераторів шуму та високоякісних генераторів PSP.

Схема генерації ключів ANSI X9.17



$$R_i = E_k\left(E_k\left(T_i\right) \oplus V_i\right).$$

$$V_{i+1} = E_k\left(E_k\left(T_i\right) \oplus R_i\right)$$

Неоднорідний ключовий простір

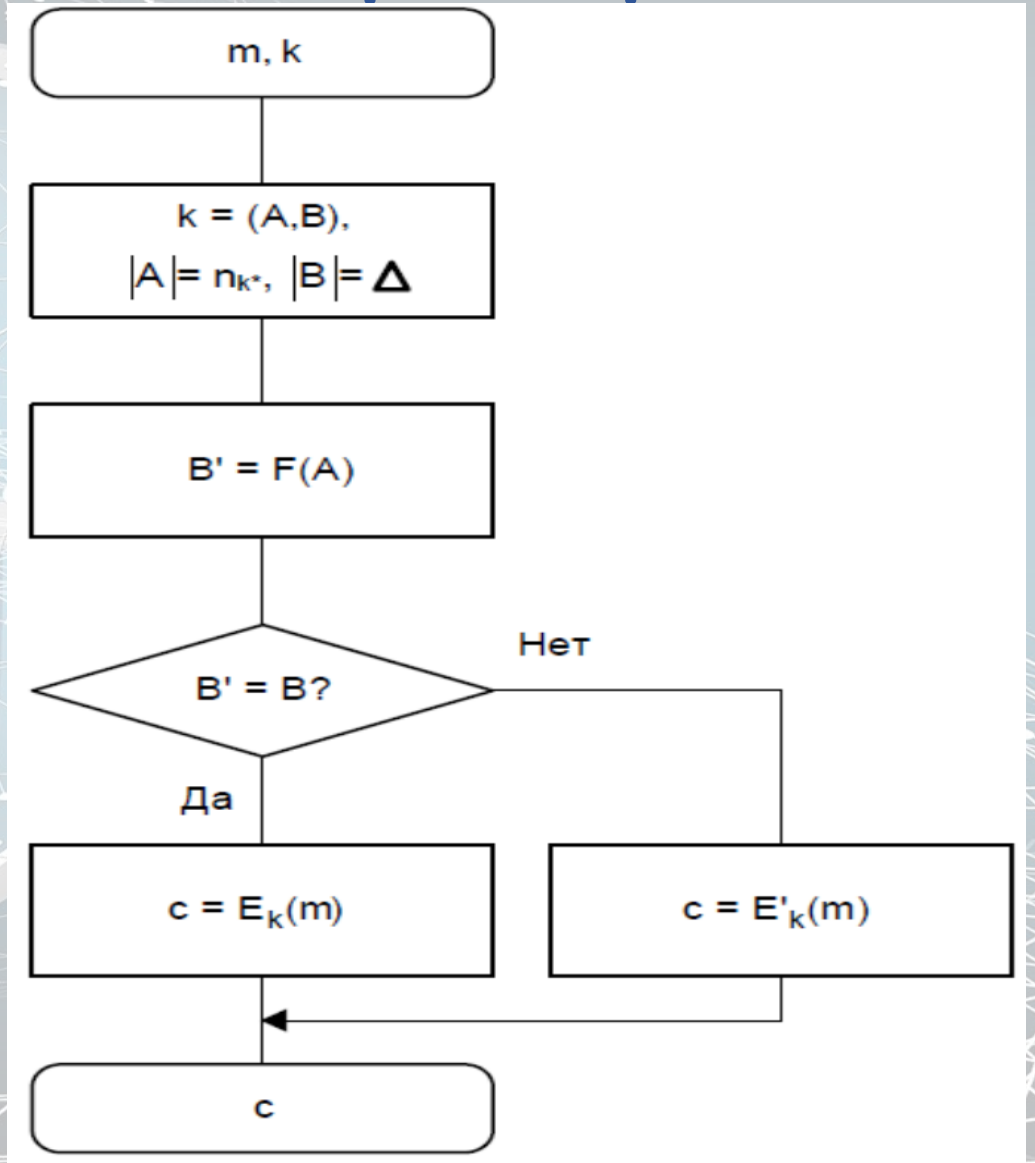
- Розкриття інформації за допомогою надійного криптографічного алгоритму Ек відбувається тільки при використанні ключів спеціального типу; $n_k \left(\left| k \right| = n_k \right)$
- «Правильна» (стійка) клавіша k Розрядність складається з двох $n_{k^*} \left(\left| k^* \right| = n_{k^*} \right)$
- Частини: ключ k* ширини та деякого коду фіксований довжини

$$\Delta = n_k - n_{k^*}$$

отриманого k* за допомогою деякої криптографічної функції F, тобто

$$k = (k^*, F(k^*)) \mid F(k^*) \mid = \Delta;$$

- Імовірність випадково отримати стабільний ключ мізерно мала і дорівнює 2Δ;
- Якщо ключ, отриманий на вході криптомодуля, не відповідає заданим умовам, для шифрування інформації використовується набагато менш стійкий алгоритмічний ритм E'k.

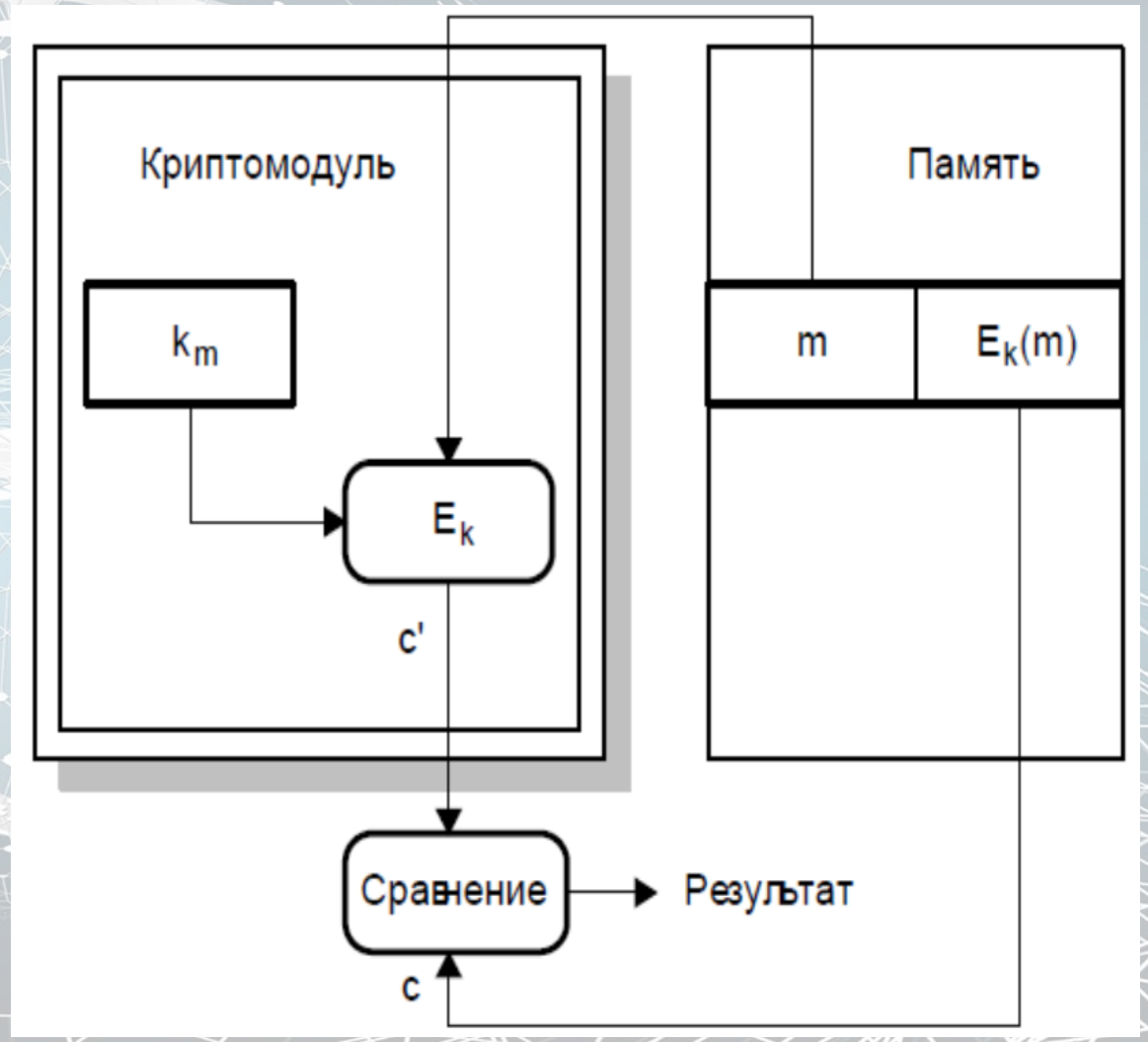


Накопичення ключів

Секретні ключі ніколи не повинні бути написані явно на носіях, які можна прочитати або скопіювати.

- ключ зберігається в захищеному від читання, запису і руйнівних впливів модуля захисту;
- ключ розповсюджується неелектронним способом, що виключає її перевірку;
- У системі обов'язково повинен бути спосіб перевірки справжності ключа.

Схема автентифікації майстер-ключа

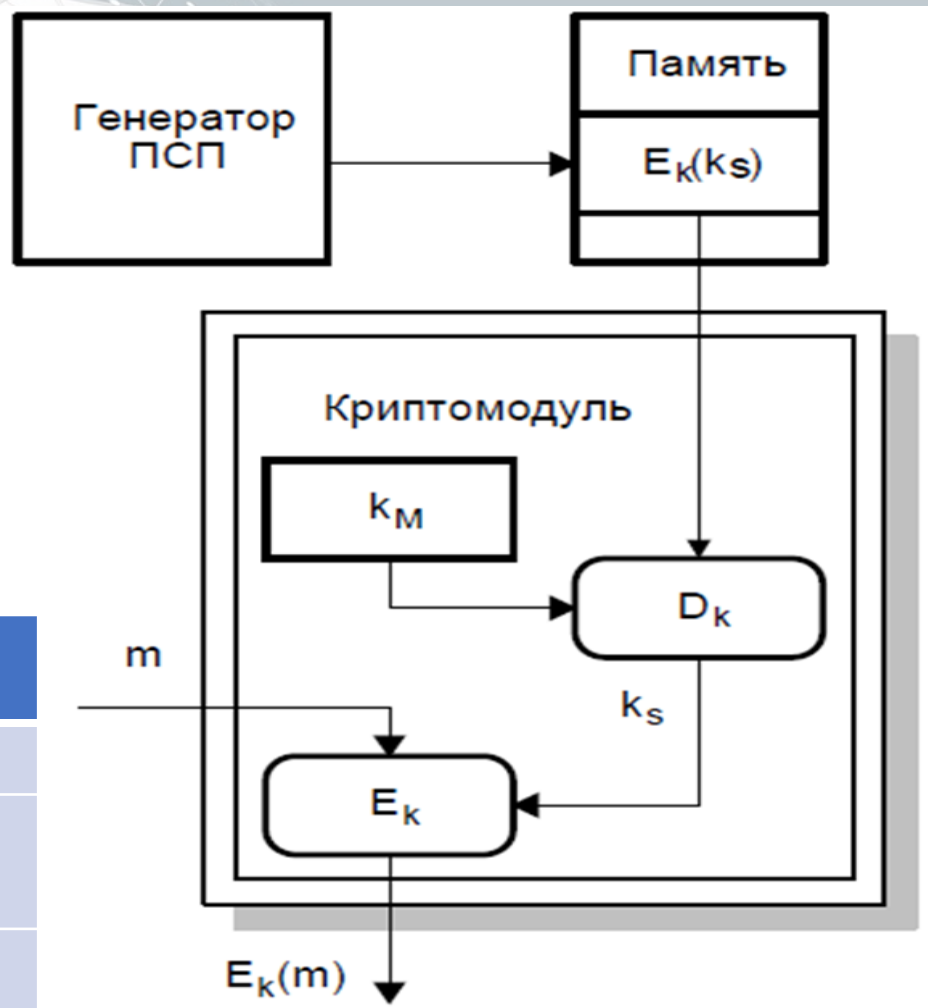


Зберігання сеансового ключа

- Запам'ятовування пароля pw і при необхідності автоматичне вилучення з нього ключа k за допомогою хеш-функції h(x) за формулою k = h(pw);
- запам'ятовування початкової начинки якісного генератора PSP, що формує ключ;
- використання пластикового ключа з розміщеним на ньому ПЗУ (ROM-ключем) або інтелектуальною карткою.

Ключові символи	Кількість символів	Кількість ожливих клавіш	Час перебору
Великі літери	32	1,1·1012	13 днів
Великі літери та цифри	42	9,7·1012	112 днів
Всі восьмибітні коди	256	1,9·1019	600 000 років

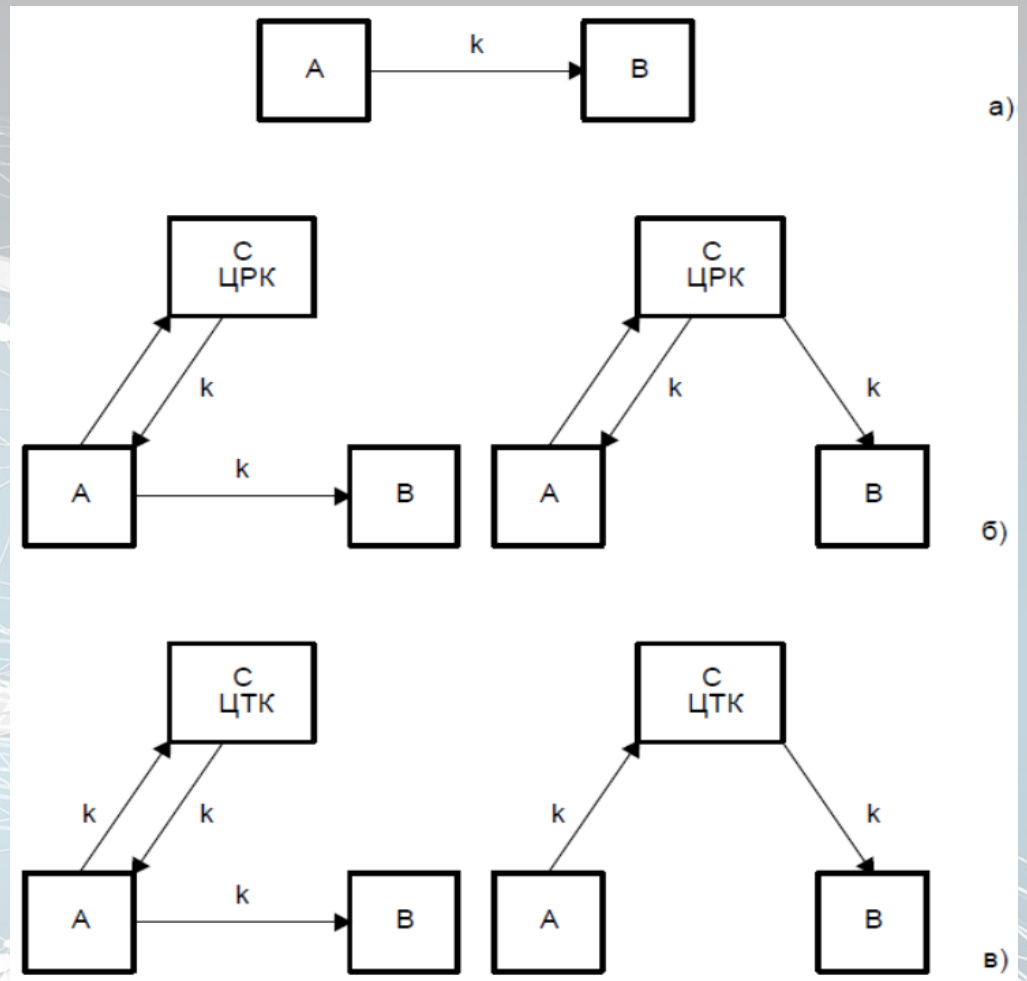
Схема захисту ключів сеансу



Розподіл ключів

1.Ву створення одного або декількох ключових розподільчих центрів. Недоліком такого підходу є те, що розподільчий центр знає, кому і які ключі призначені, а це дозволяє читати всі повідомлення, що циркулюють в IP. Можливі зловживання мають значний вплив на захист.

2. Прямий обмін ключами між користувачами інформаційної системи.



варіанти побудови схеми розподілу ключів: а – прямий обмін між користувачами в мережі (схема «точка-точка»); б – схеми Центру розподілу ключів (РКК); в – схеми Центру перекладу ключів (КК). а, в, с – учасники обміну інформацією, к – ключ

Функціями центру довіри можуть бути

- генерація, зберігання, розподіл та контроль терміну служби ключа;
- сертифікація ключів;
- аутентифікація учасників обміну інформацією;
- аудит;
- одночасова служба;
- послуги нотаріуса;
- послуга умовного депонування ключів.

Завдання управління ключами - знайти протокол розподілу ключів, який забезпечував би:

- можливість відмови від ключового розподільного центру;
- взаємне підтвердження автентичності учасників сесії;
- підтвердження валідності сесії механізмом запит-відповідь, використання для цього програмного або апаратного забезпечення;
- використання мінімальної кількості повідомлень при обміні ключами.

Термін служби ключа

- частота використання ключів (ключі екранування ключів, наприклад, використовуються набагато рідше, ніж ключі шифрування даних);
- величина шкоди, заподіяної компрометацією ключа, яка залежить, зокрема, від цінності інформації, що захищається;
- обсяг і характер інформації, що захищається (наприклад, при шифруванні випадково згенерованих ключів, інформація про вміст яких противнику заздалегідь нічого не відома, підлягає закриттю).

При визначенні терміну служби ключа враховуються такі міркування:

- Чим довше використовується ключ, тим більша ймовірність його компрометації.
- Чим довше використовується ключ, тим більше потенційної шкоди він може завдати в разі компрометації.
- Чим більше інформації, зашифрованої на одному ключі, перехоплює противник, тим простіше його атакувати;
- При тривалому використанні ключа у противника з'являється додатковий стимул витрачати значні ресурси на його відкриття, оскільки вигода в разі успіху виправдає всі витрати.

Криптографічни системи

- У потоковому шифруванні кожен символ у тексті шифру є функцією значення та положення відповідного відкритого текстового символу. Символи - це біти, байти і рідко більші одиниці тексту. Потокове шифрування - це шифрування заміщення символів.
- При блочному шифруванні вихідний текст спочатку розбивається на блоки бітів однакової довжини. До блоків застосовується залежна від ключа функція шифрування для перетворення їх у блоки шифрування однакової довжини. Зазвичай блоки шифруються за допомогою збивання.
- Основна відмінність систем з відкритим ключем полягає в тому, що знання ключа шифрування недостатньо для розшифровки і навпаки. Системи з відкритим ключем завжди блок-ключові.
- Якщо в потоковому і блочному шифрі функція шифрування залежить тільки від ключа, то в автошифрах вона залежить як від ключа, так і від одного або декількох попередніх символів або блоків шифрувального тексту.

види систем	Блокованість	Надточність	Транзитивність	Симетрія
Потокове	-	-	-	+
Блокувати	+	-	+	-
З відкритим ключем	+	-	+	+
Комбіновані	+	+	+	+

види систем	поширення помилок	Автентифікація	Алгоритм	Швидкість
Потокове	Ні	Ні	Типових немає	Великий
Блокувати	так	Ні	DES і аналоги	Великий
З відкритим ключем	так	так	RSA, ЕльГамаль	Дуже низький
Комбіновані	так	так	Вони виготовляються на основі блоку	Великий

Кодування, специфічне для пам'яті

Алгоритми стиснення даних дуже добре підходять для використання в поєднанні з криптографічними алгоритмами. На це є дві причини:

- При відкритті шифру криптоаналітик найбільше покладається на надмірність, властиву будь-якому відкритому тексту. Позбутися від цієї надмірності допомагає стиснення.
- Шифрування даних - дуже трудомістка операція. Стиснення зменшує довжину відкритого тексту, тим самим зменшуючи час, який він буде витрачати на його шифрування.

Причини

- Природні мови мають багато надмірності.
- Видалення повторюваних символів
- Посимвольне кодування.
- Використовуйте коди змінної довжини.

Шифрування в каналах зв'язку комп'ютерної мережі

- Шифрування каналів (1-фізичний)
- Шифрування на рівні контролю лінії даних (2)
- Шифрування транспортного рівня (4)
- Наскрізне шифрування (6)
- Шифрування рівня додатків (7)

Шифрування файлів

- Часто після шифрування файлу його незашифрована копія надійно забувається на іншому магнітному диску, на іншому комп'ютері або у вигляді роздруківки, зробленої на принтері;
- розмір блоку в алгоритмі блочного шифрування може значно перевищувати розмір окремого фрагмента даних в структурованому файлі, в результаті чого кінцева довжина зашифрованого файлу буде набагато більше, ніж довжина вихідного файлу;
- швидкість шифрування файлів за допомогою обраного для цієї мети криптографічного алгоритму повинна відповідати швидкості, з якою працюють пристрої вводу-виводу сучасних комп'ютерів;
- Працювати з ключами досить складно, так як різним користувачам зазвичай необхідно мати доступ не тільки до різних файлів, але і до окремих частин одного і того ж файлу.

Апаратне та програмне шифрування

- апаратне шифрування працює швидше
- обладнання легше фізично захистити від проникнення ззовні
- апаратне забезпечення шифрування простіше встановлювати

- бути реалізований у вигляді відповідної програми
- операційні системи мають вбудоване шифрування файлі

Проблеми шифрування

- Прозоре шифрування
- Шифрування великих повідомлень і потоків даних
- Використання блукаючих ключів
- Шифрування, кодування та стиснення інформації
- Приховування одного тексту у іншому
- Реалізації методів захисту інформації

Причини ненадійності криптографічних систем

- Неможливість використання сильних криптографічних алгоритмів (не стіки алгоритми);
  - Низька швидкість роботи сильних криптографічних алгоритмів.
  - Експортні обмеження
  - Використання власних криптографічних алгоритмів

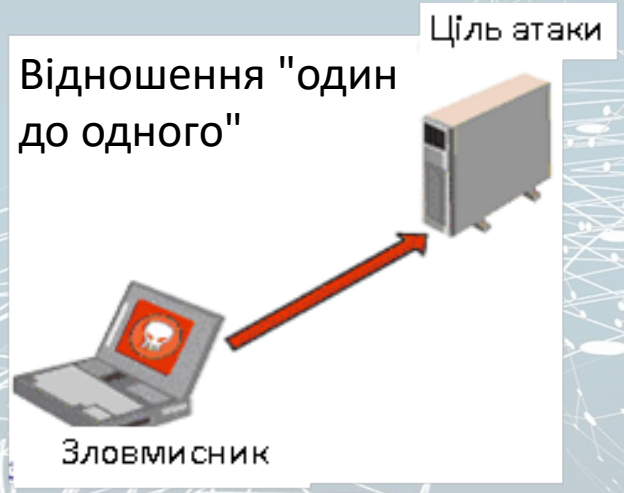
Стійки алгоритми

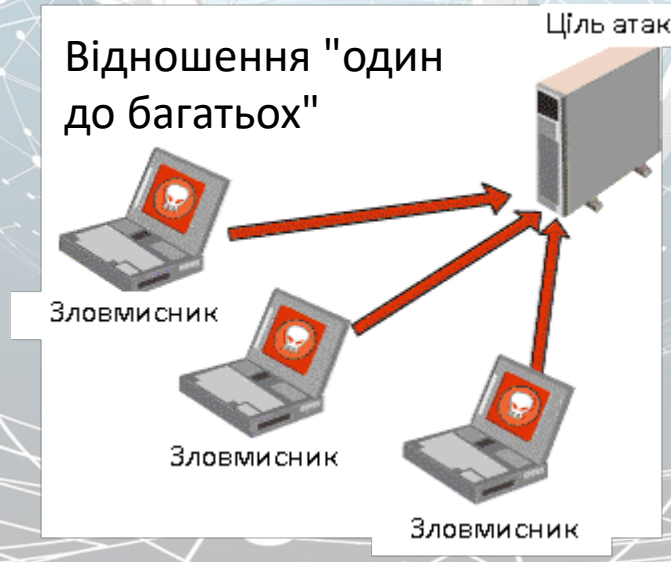
- Неправильне використання криптографічних алгоритмів;
  - Коротка довжина ключа
  - Повторне накладення шифру гами
  - Зберігання ключа разом з даними
- Помилки при реалізації криптографічних алгоритмів;
  - Зниження криптографічної стійкості при генерації ключа
  - Відсутність перевірки на наявність слабких клавіш
  - Наявність залежності в часі обробки ключа
  - Наявність люків.
  - Недоліки датчика випадкових чисел (ПВЧ).
  - Недостатній захист від РПС
- Людський фактор.

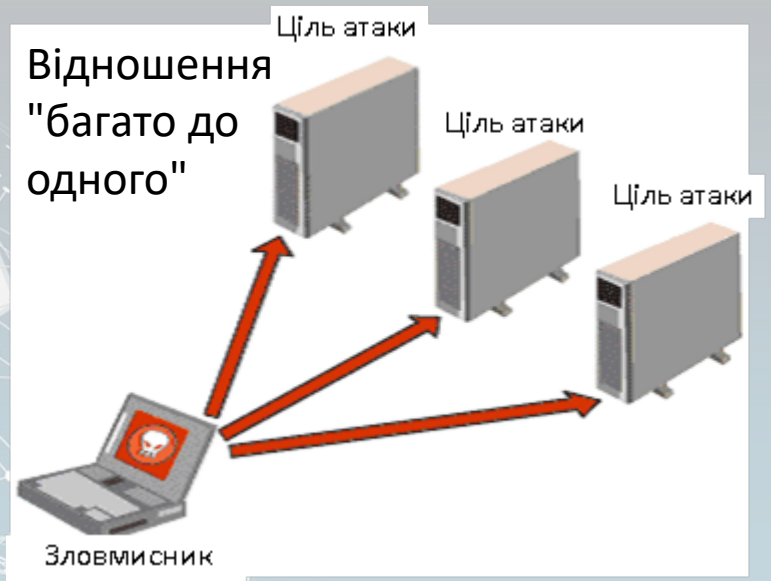
КОМП'ЮТЕРНІ АТАКИ Й ТЕХНОЛОГІЇ ЇХ ВИЯВЛЕННЯ

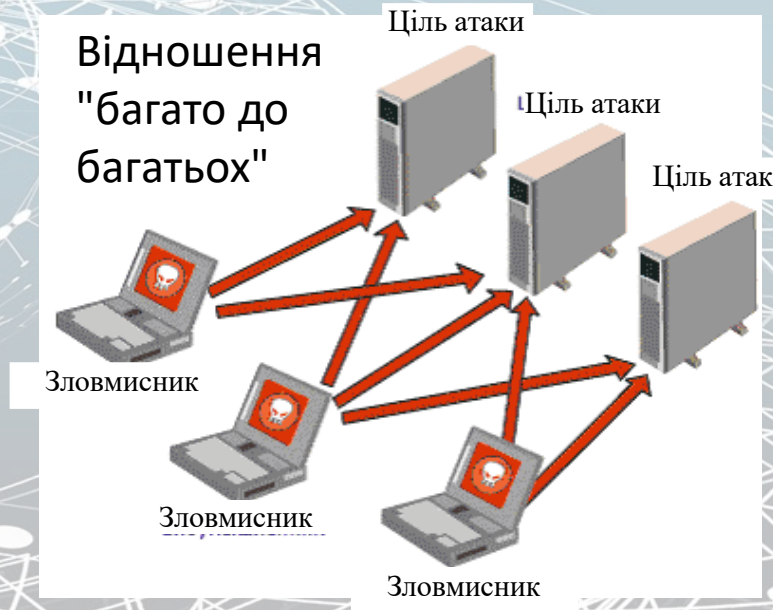
Моделі атак

Атакою на інформаційну систему називаються навмисні дії зловмисника, що використовують уразливості інформаційної системи й приводять до порушення доступності, цілісності й конфіденційності оброблюваної інформації.









Етапи реалізації атак

Можна виділити наступні етапи реалізації атаки:

- попередні дії перед атакою або "збір інформації";
- власно "реалізація атаки";
- завершення атаки.

Збір інформації – це основний етап реалізації атаки. Саме на даному етапі ефективність роботи зловмисника є запорукою "успішності" атаки. Спочатку вибирається ціль атаки й збирається інформація про неї (тип і версія операційної системи, відкриті порти й запущені мережні сервіси, установлене системне й прикладне програмне забезпечення і його конфігурація й т.д.). Потім ідентифікуються найбільш уразливі місця системи, яка атакується, вплив на які приводить до потрібного зловмисника результату. Зловмисник намагається виявити всі канали взаємодії (цілі) атаки з іншими вузлами.

Залежно від бажаного результату порушник концентрується на тім або іншому етапі реалізації атаки. Наприклад:

- для відмови в обслуговуванні докладно аналізується мережа, яка атакується, у ній вишукуються слабкі місця;
- для розкрадання інформації основна увага приділяється непомітному проникненню на вузли, які атакуються, за допомогою виявлених раніше уразливостей.

Збір інформації

Перший етап реалізації атак – це збір інформації про систему, яка атакується, або вузол. Він включає такі дії як визначення мережної топології, типу й версії операційної системи вузла, що атакується, а також доступних мережних і інших сервісів і т.п. Ці дії реалізуються різними методами

- Вивчення оточення
- Ідентифікація топології мережі
- Ідентифікація вузлів
- Ідентифікація сервісів або сканування портів
- Ідентифікація операційної системи
- Визначення ролі вузла
- Визначення уразливостей вузла

Реалізація атаки

- Проникнення. Проникнення має на увазі під собою подолання засобів захисту периметра (наприклад, міжмережного екрана).
- Встановлення контролю. Встановлення контролю над вузлом, який атакується.
- Цілі реалізації атак. По-перше, одержання несанкціонованого доступу до самого вузла й інформації, що втримується на ньому. По-друге, одержання несанкціонованого доступу до вузла для здійснення подальших атак на інші вузли.

Завершення атаки

- Етапом завершення атаки є "замітання слідів" з боку зловмисника.

Класифікація атак

- Віддалене проникнення (remote penetration). Атаки, які дозволяють реалізувати віддалене керування комп'ютером через мережу. Наприклад, NetBus або BackOrifice.
- Локальне проникнення (local penetration). Атака, що приводить до одержання несанкціонованого доступу до вузла, на якому вона запущена. Наприклад, GetAdmin.
- Віддалена відмова в обслуговуванні (remote denial of service). Атаки, які дозволяють порушити функціонування або перевантажити комп'ютер через Internet. Наприклад, Teardrop або trin00.
- Локальна відмова в обслуговуванні (local denial of service). Атаки, які дозволяють порушити функціонування або перевантажити комп'ютер, на якому вони реалізуються. Прикладом такої атаки є "ворожий" апплет, що завантажує центральний процесор нескінченним циклом, що приводить до неможливості обробки запитів інших застосунків.
- Мережні сканери (network scanners). Програми, які аналізують топологію мережі й виявляють сервіси, доступні для атаки. Наприклад, система nmap.
- Сканери уразливостей (vulnerability scanners). Програми, які шукають уразливості на вузлах мережі і які можуть бути використані для реалізації атак. Наприклад, система SATAN або ShadowSecurityScanner.
- Зломщики паролів (password crackers). Програми, які "підбирають" паролі користувачів. Наприклад, L0phtCrack для Windows або Crack для Unix.
- Аналізатори протоколів (sniffers). Програми, які "прослуховують" мережний трафік. За допомогою цих програм можна автоматично шукати таку інформацію, як ідентифікатори й паролі користувачів, інформацію про кредитні карти й т.д.

Типи і приклади атак. Пасивні і активні атаки

- Активні атаки включають явні впливи на систему, що змінюють її стан. Це можуть бути шкідливий програмний код-вірус, впроваджений в виконувану системою програму, спотворення даних на сторінках зламаного веб-сайту, блокування мережевого сервісу шляхом бомбардування його помилковими запитами або запроваджене в комунікаційний протокол неправдиве повідомлення. Головною відмінною рисою активних атак є те, що після свого завершення вони, як правило, залишають сліди.
- Пасивні атаки не порушують нормальну роботу ІС, вони пов’язані зі збором інформації про систему, наприклад прослуховуванням внутрішньомережевого трафіку або перехопленням повідомлень, що передаються по лініях зв’язку. У багатьох випадках пасивні атаки не залишають слідів, тому їх дуже складно виявити, часто вони так і проходять непоміченими.

Відмова в обслуговуванні - DoS

Відмова в обслуговуванні (Denial of Service, DoS) або DoS-атака – це атака на обчислювальну систему з метою виводу її з ладу, тобто створення таких умов, при яких легітимні користувачі системи не можуть дістати доступ до ресурсів, що надаються системою, або цей доступ ускладнений.

Існують різні причини, по яких може виникнути DoS-атака:

- Помилка в програмному коді, що призводить до звернення до невикористовуваного фрагменту адресного простору, виконання неприпустимої інструкції або іншої необроблюваної виняткової ситуації, коли відбувається аварійне завершення серверного додатку.
- Недостатня перевірка даних користувача, що призводить до нескінченного або тривалого циклу або підвищеного тривалого споживання процесорних ресурсів або використання великого об’єму оперативної пам’яті.
- Флуд (Flood) – атака, пов’язана з великою кількістю, зазвичай безглуздих або сформованих в неправильному форматі запитів до комп’ютерної системи або мережевого обладнання, яка має на меті відмову в роботі системи через вичерпання ресурсів системи – процесора, пам’яті або каналів зв’язку (полоси пропускання).
- Атака другого роду – атака, яка прагне викликати помилкове спрацьовування системи захисту і таким чином привести до недоступності ресурсу.

Розподілена атака відмови в обслуговуванні - DDoS

Якщо атака виконується одночасно з великого числа комп'ютерів, говорять про розподілену атаку відмови в обслуговуванні (Distributed Denial of Service, DDoS).

В деяких випадках до DDoS-атаки приводить легітимна дія, наприклад, слешдот-ефект.

- Слешдот-ефект (Slashdot) полягає в недоступності певного сайту (зазвичай, маловідомого) внаслідок розміщення посилання на нього на популярному сайті і, як наслідок, різкого збільшення кількості відвідувань даного сайту, що призводить до перевищення допустимого навантаження на сервер і відмови в обслуговуванні частини користувачів.

Поняття «DDoS-атака» практично рівносильно поняттю «флуд», і у вжитку те і інше часто взаємозамінно.

Для створення флуда можуть застосовуватися як звичайні мережеві утиліти, наприклад, ping, так і спеціальні програми. Є декілька варіантів організації DDoS атак:

- Ботнет – зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера.
- Флешмоб – домовленість великого числа користувачів інтернету почати здійснювати певні типи запитів до атакованого сервера.

Захист від DDoS-атак

Захист від розподілених DDoS-атак ґрунтується на аналізі трафіку, що надходить на вузлом, який захищається.

Ефективність захисту від DDoS-атак звичайно описується трьома основними параметрами:

- потужність атаки (Мбіт/с), що здатна витримати система;
- точність дій системи при виявленні й відбитті атаки;
- імовірність і кількість помилкових спрацьовувань (False Positive).

При виборі системи захисту від DDoS атак потрібно враховувати важливі фактори:

- потужність атаки (Мбіт/с), що здатна витримати система;
- точність дій системи при виявленні й відбитті атаки;
- імовірність і кількість помилкових спрацьовувань (False Positive);
- оперативна можливість перенаправлення трафіку (Зміна IP основного сервера);
- захист на вимогу – можливість включити захист від DDoS тільки на час атаки;
- пороги обмежень по трафіку/продуктивності системи.

Впровадження шкідливих програм

Численна група активних атак пов’язана з впровадженням в комп’ютери шкідливих програм (malware – скорочення від malicious software). До цього типу програм відносяться

- Троянська програма (Trojan Horses, Trojans) – різновид шкідливої програми, яка проникає в комп’ютер під виглядом легального програмного забезпечення, на відміну від вірусів і черв’яків, які поширюються самовільно.
- Руткіт (Root Kit – набір root-a) – програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі.
- Мережевий черв’як – шкідлива програма, яка самостійно розповсюджується через локальні і глобальні комп’ютерні мережі.
- Комп’ютерний вірус (Computer Virus) – шкідлива програма, яка має здатність до прихованого самопоширення.
- Спам (Spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати.

Соціальний інжиніринг

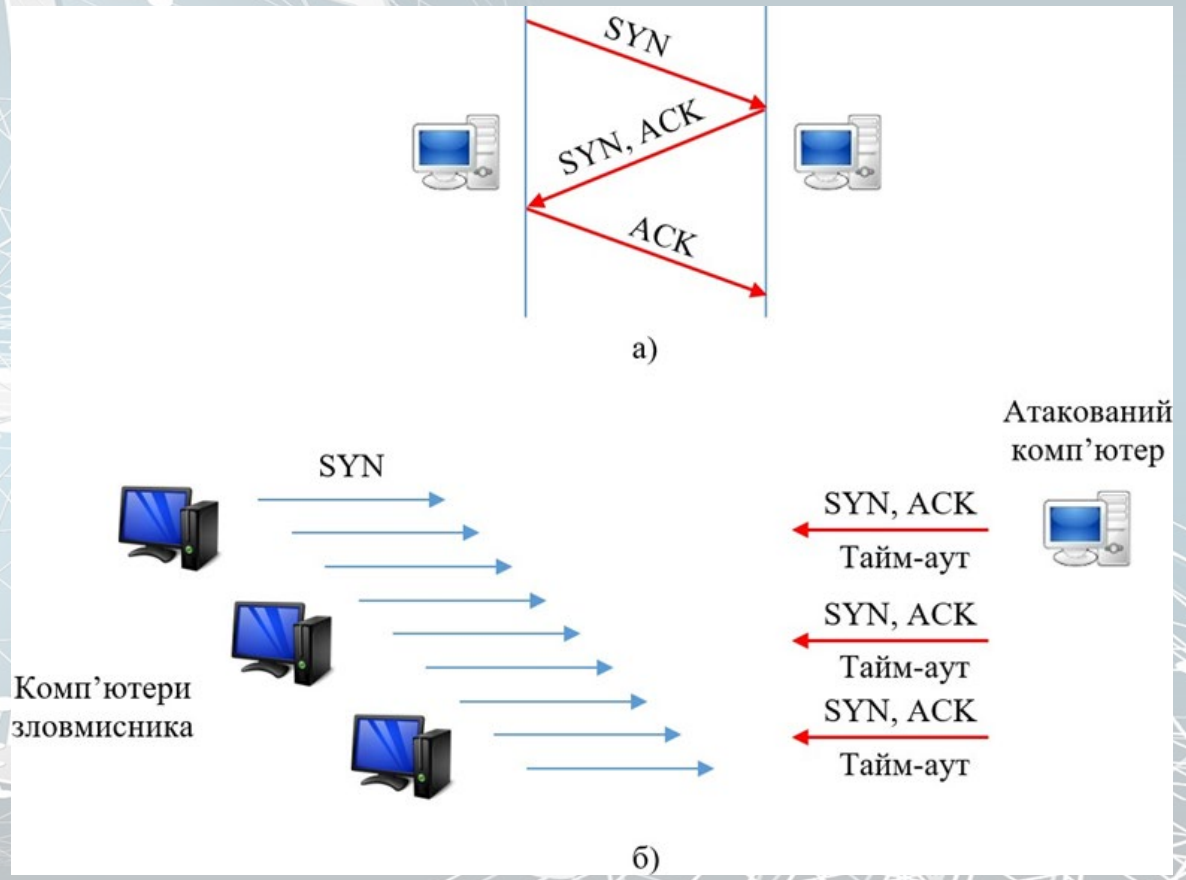
- Соціальний інжиніринг – це отримання несанкціонованого доступу до інформації або до системи без застосування технічних засобів.
- Фішинг (phishing спотворене fishing – рибалка) – один з різновидів соціального інжинірингу, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів.
- Більшість методів фішингу зводиться до того, щоб замаскувати підроблені посилання на фішингові сайти під посилання справжніх організацій. Адреси з помилками або субдомени часто використовуються зловмисниками.
- Соціальні мережі також представляють великий інтерес для фішерів, дозволяючи збирати особисті дані користувачів. За оцінками фахівців, понад 70% фішингових атак в соціальних мережах – успішні

Варіанти реакцій на виявлену атаку

- Повідомлення на консоль (включаючи резервну) системи виявлення атак або на консоль інтегрованої системи (наприклад, міжмережного екрана).
- Звукове оповіщення про атаку.
- Додаткові повідомлення на мобільний пристрій або факс.
- Обов'язкова реєстрація подій, що виявляються.
- Трасування подій (event trace), тобто запис їх у тій послідовності й з тією швидкістю, з якими їх реалізовував зловмисник.
- Переривання дій атакуючого, тобто завершення з'єднання.
- Реконфігурація мережного встаткування або міжмережевих екранів.
- Блокування мережевого трафіку так, як це реалізовано в міжмережевих екранах.

АТАКИ НА ТРАНСПОРТНУ ІНФРАСТРУКТУРУ МЕРЕЖІ. TCP-атаки. Затоплення SYN-пакетами (1)

- Атака затопленням SYN-пакетами (SYN Flood) використовує вразливість процедури встановлення логічного з’єднання протоколу TCP. Ця процедура базується на використанні прапорів SYN і ACK, які переносяться в заголовку кожного TCP-сегмента (рис.а). Для реалізації атаки зловмисник організовує передачу на сервер масованого потоку пакетів з прапором SYN, кожен з яких ініціює створення нового TCP-з’єднання (рис. б)
- Головним засобом боротьби з атакою затопленням SYN-пакетами є фільтрування трафіку, що надходить від джерела атаки. Для цього потрібно визначити адресу атакуючого вузла.



TCP-атаки. Затоплення SYN-пакетами (2)

- У деяких випадках атакуючий може поміщати SYN-сегменти в IP-пакети з «підробленою» адресою відправника. У цьому випадку говорять, що він використовує спуфінг.
- Спуфінг (Spoofing – підміна) – ситуація, в якій одна людина або програма успішно маскується під іншу шляхом фальсифікації даних і дозволяє отримати незаконні переваги.
- Подолання атаки шляхом фільтрації також ускладнюється, коли потік SYN- сегментів надходить на атакований сервер відразу від сотень заражених комп’ютерів з деякої мережі, тобто коли має місце розподілена атака затопленням SYN-пакетами (DDoS SYN Flood).
- Різновидом TCP-атаки затопленням SYN-пакетами є TCP-атака затопленням ACK-пакетами, що виконується шляхом відображення.

TCP-атаки. Підробка TCP-сегмента

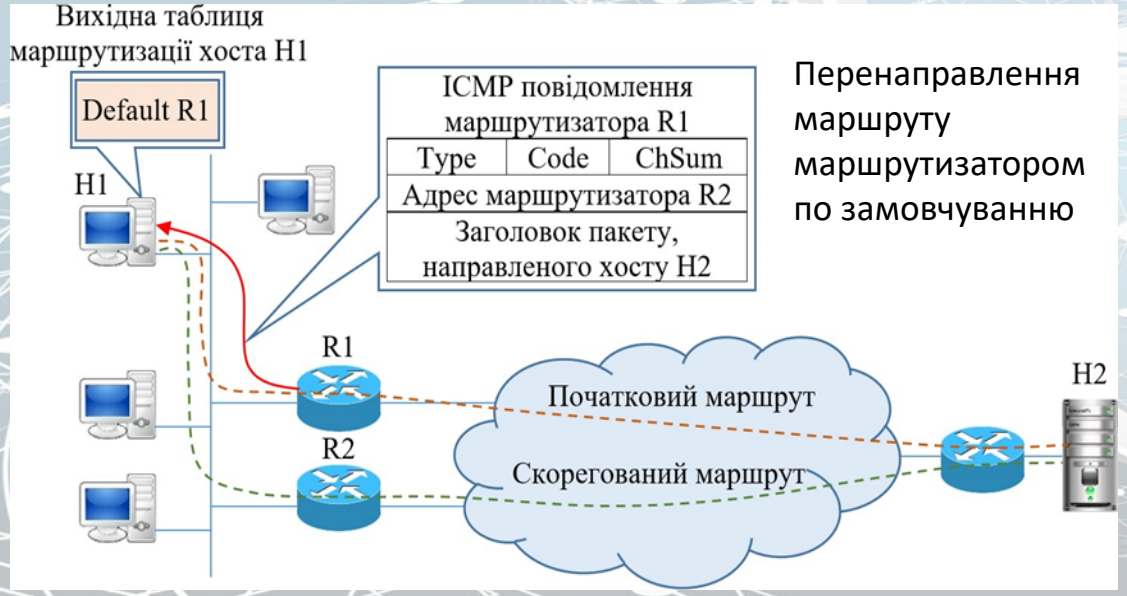
- Атака підробкою TCP-сегмента полягає в генерації TCP-сегментів, всі атрибути яких мають значення, що легітимні для деякого існуючого TCP-сеансу атакованого комп’ютера, тобто 1P-адреси, номера TCP-портів відправника і отримувача, а також порядкові номери з поточного діапазону вікна прийому.
- Різновидом підробки TCP-сегментів є їх повторне використання. Якщо зловмисник зміг якимось чином перехопити трафік між двома учасниками TCP- сеансу, то згодом він може просто надсилати учасникам сеансу дублікати перехоплених сегментів.

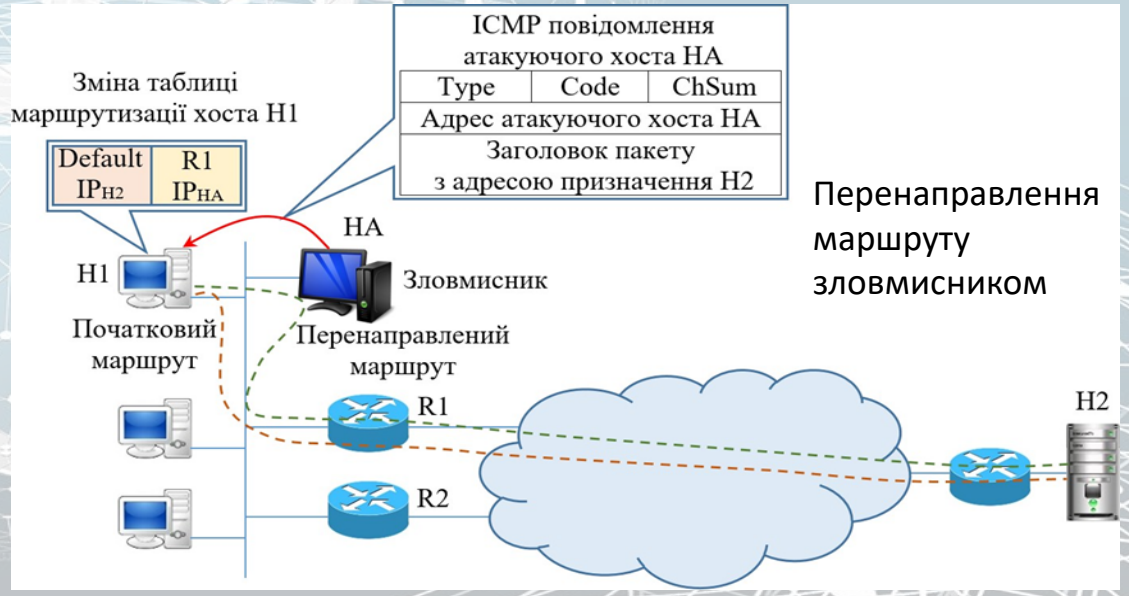
TCP-атаки. Скидання TCP-з’єднання

- Атака скиданням TCP-з’єднання використовується для розриву TCP-з’єднань легальних користувачів. Для проведення атаки зловмисник повинен підробити заголовок TCP- сегменту.
- Прийом скидання з’єднання використовується не лише зловмисниками, а й розробниками засобів захисту: наприклад, деякі фаєрволи застосовують його для припинення атаки.
- Боротьба а з атаками підробки TCP-сегмента і скиданням TCP-з’єднання може вестися по двох напрямах. Перший напрям пов’язаний із запобіганням прослуховування трафіку, другий базується на зміні поведінки самого протоколу TCP, наприклад шляхом включення додаткової процедури автентифікації кожного TCP-сегмента з використанням цифрового підпису. Цифровий підпис не забезпечує конфіденційності, тому що вміст полів не шифрується, але він гарантує, що TCP-сегмент не був змінений третьою стороною.

ICMP-атаки. Перенаправлення трафіку

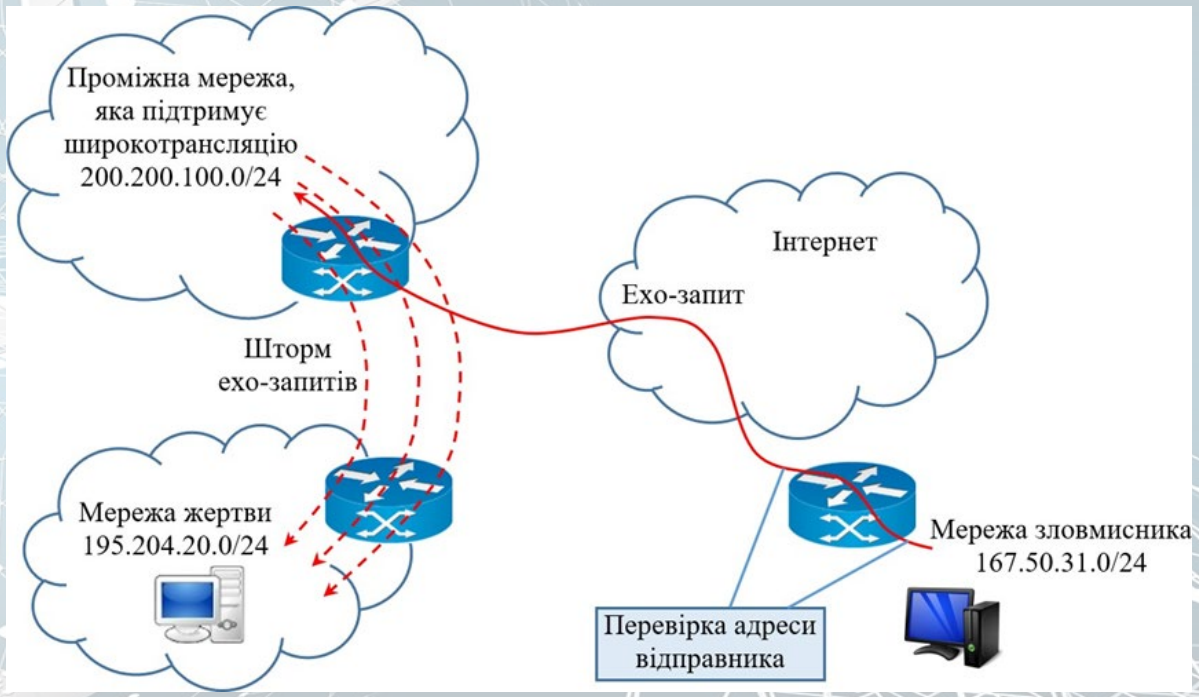
- Згідно протоколу ICMP маршрутизатор надсилає хосту безпосередньо приєднаної локальної мережі ICMP-повідомлення про перенаправлення маршруту у разі відмови цього маршруту або в тих випадках, коли виявляє, що для деякої адреси призначення хост використовує нераціональний маршрут.





ICMP-атаки. ICMP-атака Smurf

- ICMP-атака Smurf – це DDoS-атака, яка використовує функцію ехо-запиту протоколу ICMP.
- В атаці Smurf використовується той факт, що ехо-запит може бути надісланий не тільки по індивідуальній, а й по широкотрансляційній (broadcast) адресі деякої мережі.
- У ICMP-атаці Smurf використовується характерний прийом – посилення атаки за рахунок відображення надісланого пакета великою кількістю комп’ютерів.



Компоненти ICMP-атаки Smurf

ICMP-атаки. Пінг смерті і Ping-затоплення

- Атака Пінг смерті (Ping of Death) полягає у відправці на атакований комп’ютер ехо-запиту з довжиною IP-пакета, що перевищує його максимально можливий розмір, який відповідно до стандарту становить 65535 байт. Оскільки відповідний буфер ядра ОС не розрахований на такий розмір, ОС зазнає краху, звідси і така назва атаки. Так як дана атака заснована на перевищенні розміру буфера при складанні фрагментованого IP-пакету, то вона є окремим випадком атак, що використовують IP-фрагментацію.
- Інша атака, яка називається Ping-затопленням, також є досить простою: зловмисник використовує утиліту ping своєї операційної системи для відправки ехо-запитів на атакований комп’ютер з максимально можливою частотою. Якщо швидкодія мережевого інтерфейсу його комп’ютера вища, ніж у атакованого комп’ютера, то атака вдається, так як вся вхідна пропускна спроможність інтерфейсу атакованого комп’ютера виявляється вичерпаною.

UDP-атаки

- UDP-затоплення відноситься до DoS-атак і має на меті вичерпання пропускної спроможності інтерфейсу атакованого комп’ютера. Вона подібна до розглянутої атаки Ping-затоплення, коли зловмисник просто направляє інтенсивний потік датаграм на атакований комп’ютер.
- В атаці ICMP/UDP-затопленням використовується два протоколи. Зловмисник направляє інтенсивний потік UDP-пакетів, в яких в якості адреси відправника вказана адреса комп’ютера-жертви, на програмні порти комп’ютерів, що знаходяться в пасивному стані (тобто в даний момент з цими портами не пов’язані додатки, що прослуховують мережу).
- Атака UDP/echo/chargen-затопленням схожа на попередню, в ній також має місце відображення UDP-пакетів, але при цьому пакети відправляються з номером порту 7 або 19. Ці порти зазвичай активні, вони підтримують сервіси echo (порт 7) і Chargen (порт 19), використовуючи протокол UDP. Сервіс Chargen у відповідь на запит генерує рядок випадкових символів довільної довжини від 0 до 512 і надсилає його хосту, що звернувся.

IP-атаки. Атака на IP-опції

- Атака на IP-опції являє собою DoS-атаку на маршрутизатори, в якій використовується поле додаткових опцій протоколу IP.
- Атака заснована на тому факті, що у більшості IP-пакетів поле опцій відсутнє, тому для просування таких пакетів маршрутизатор задіює спеціалізовані процесори портів, які дуже швидко і економно виконують цю операцію.
- Звичайна практика боротьби з цією атакою – фільтрація (відкидання) всіх пакетів, в заголовку яких є опції. Можливо також ігнорування всіх або деяких опцій.

IP-атаки. IP-атака на фрагментацію

Атака на фрагментацію спрямована на кінцеві вузли IP-мереж, в обов’язок яких входить збірка фрагментованого IP-пакету в єдине ціле. Операція складання має декілька вразливостей, які можуть бути використані зловмисником:

- Перевищення максимальної довжини пакету (переповнення буфера збірки).
- Перекриття сегментів за рахунок спеціального підбору зсувів і довжин фрагментів.
- Заміщення фрагментів.
- Незавершені фрагменти.

Атаки на фрагментацію протоколу IPv6 в принципі аналогічні атакам на фрагментацію IPv4, але так як в новій версії протоколу IP був врахований досвід попередньої боротьби, у зловмисника залишається менше варіантів.

Мережева розвідка

- Будь-якій атаці передує мережева розвідка, при якій зловмисник намагається зібрати необхідні для атаки дані. Конкретний набір даних залежить від типу атаки, але частіше за все мережева розвідка включає збір таких даних: IP-адреси активних (тобто відповідають на мережевий трафік) хостів; номера активних TCP-портів; номера активних і пасивних UDP-портів хостів; тип і версії ОС і додатків.
- Виявлення IP-адрес активних хостів мережі називають скануванням мережі (Network Scanning), а активних і пасивних портів – скануванням портів (Port Scanning).
- Найбільш поширеними прийомами сканування мережі є: Пінг TCP SYN, Пінг TCP ACK, Пінг UDP, Пінг ICMP, Пінг IP.
- Схожі методи застосовуються і для сканування портів, тут перевага віддається SYN-скануванню протоколу TCP.
- Щоб уникнути розкриття, зловмисники часто використовують спуфінг IP-адреси при атаках.

Атаки на DNS. DNS-спуфінг

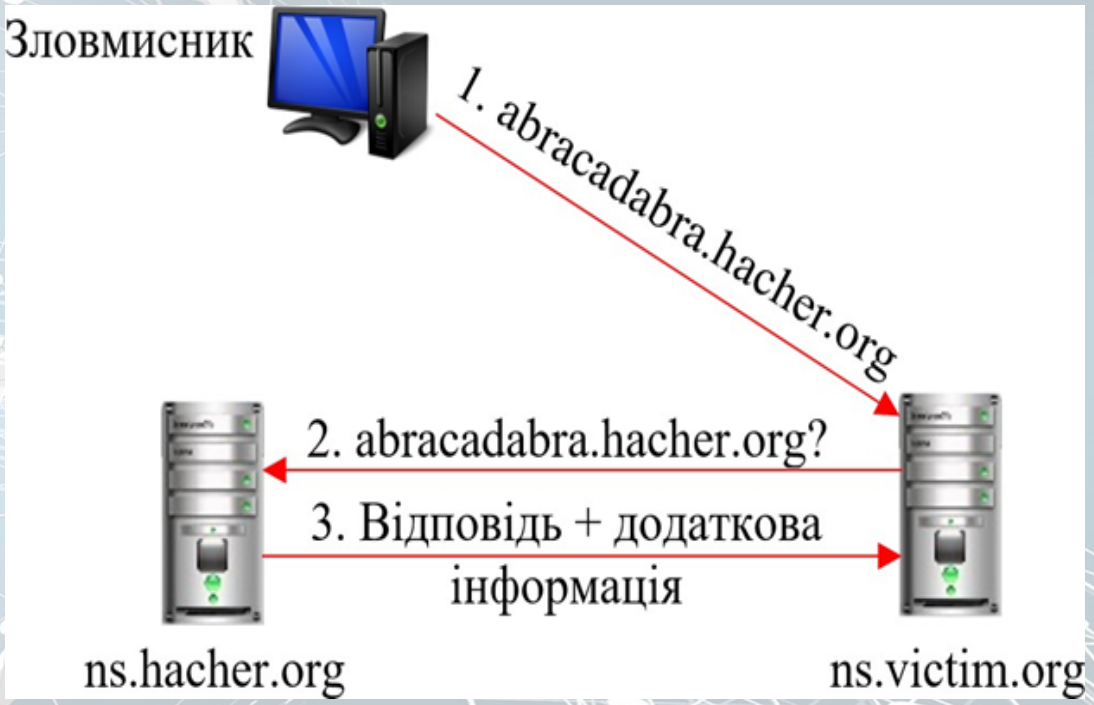
- Він вирішує перенаправити потік даних, які легальний корпоративний клієнт надсилає корпоративному серверу, на свій комп’ютер. Для цього потрібно випередити відповідь DNS-сервера клієнту і нав’язати йому свій варіант відповіді, в якому замість IP-адреси корпоративного сервера (в прикладі - 193.25.34.125) зловмисник вказує IP-адреса атакуючого хоста (203.13.1.123).



Схема перенаправлення трафіку з використанням неправдивих DNS-відповідей

Атаки на DNS. Отруєння кешу DNS

- Атака отруєнням кешу DNS спрямована на заміну коректного запису, що зберігається в кеші деякого DNS-сервера, підробленим записом, який направляє DNS-клієнта на неправдивий вузол.
- Першим кроком зловмисника є напрямлення на атакований DNS-сервер ns.victim.org запиту на неіснуюче ім’я, яке відноситься до домену зловмисника. Отримавши такий запит і не маючи на нього відповіді в кеші (так як даного імені не існує), DNS-сервер ns.victim.org пересилає запит серверу ns.hacker.org, який веде зону hacker.org (знайшовши цей сервер через звичайну процедуру пошуку, що починається з запиту до кореневого сервера).



Загальна схема отруєння кешу DNS

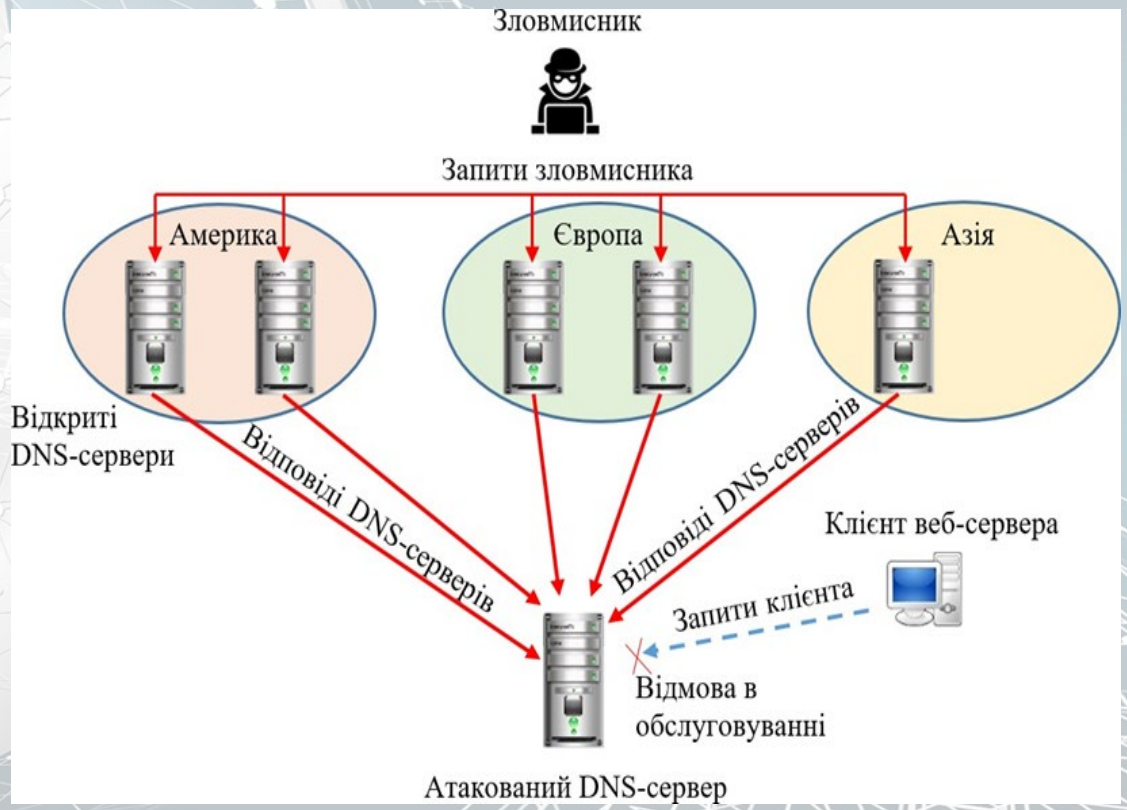
Атаки на DNS. Атаки на кореневі DNS-сервери

Найбільш потужними і відчутними за своїми наслідками була DDoS-атака 21 жовтня 2002 на кореневі сервери :

- Атака тривала трохи більше години і була спрямована на всі 13 адрес кореневих серверів.
- Атака була комбінованою, використовувалися ICMP-атака ping-затопленням, TCP- атака затопленням SYN-пакетами, атака фрагментованими IP-пакетами та атака UDP-затопленням.
- Інтенсивність атаки на сервер – 50-100 Мбіт/с; сумарна інтенсивність – 900 Мбіт/с.
- В атаці використовувався спуфінг Ip-адрес, визначити реальні джерела атаки не вдалось.

Атаки на DNS. DDoS-атаки відбиття від DNS-серверів

- Основна ідея атаки відбиття в тому, що в Інтернеті працюють мільйони DNS-серверів, основним обов’язком яких є відправка відповідей на запити клієнтів. При цьому відповідь може за обсягом набагато перевищувати запит.
- Загальна схема атаки зображена на рис. Для організації цієї тривалої атаки було використано близько 30000 DNS-серверів, що працювали у відкритому рекурсивному режимі, тобто відповідали на запити будь-яких користувачів і при цьому давали повні (рекурсивні) відповіді.



Атака відбиття від DNS-серверів

Атаки на DNS. Методи захисту служби DNS

Існує ряд запобіжних заходів, які підвищують захищеність DNS-серверів від атак або використання їх як інструмент атаки.

- Захист ОС хоста. Оскільки, DNS – це додаток ОС, то сама ОС повинна бути надійно захищена всіма можливими способами.
- Поділ користувачів на внутрішніх і зовнішніх. Рекурсивні неповноважні відповіді повинні надаватися лише внутрішнім користувачам, які викликають більшу довіру.
- Передача файлу зони з первинного сервера тільки вторинним серверів цієї зони з використанням для передачі захищених протоколів, наприклад SFTP або SCP.
- Використання DNSSEC. DNSSEC є набором стандартів, що забезпечують автентифікацію відповідей DNS-серверів за допомогою цифрового підпису та системи публічних ключів. DNSSEC-клієнт може перевірити, що отримана відповідь дійсно прийшла від уповноваженого сервера зони. DNSSEC ускладнює зловмисникам спуфінг-атаки і отруєння кешу, так як для цього потрібно підробляти цифровий підпис сервера. З 2010 року всі кореневі сервери, а також багато серверів верхнього рівня і великих провайдерів підтримують DNSSEC.

ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА ПРОТИДІЯ ВТОРГЕННЯМ

СИСТЕМИ ВИЯВЛЕННЯ АТАК

Системи виявлення атак (СВА) – це програмні або програмно-апаратні системи, які автоматизують процес аналізу подій в інформаційно-комунікаційній системі з міркувань безпеки – англ. – Intrusion Detection Systems (IDS).

Технологія виявлення атак базується на трьох складових:

- ознаках, що описують порушення політики безпеки;
- джерелах, у яких шукають ознаки порушень політики безпеки;
- методах аналізу інформації, яку одержують з різни джерел.

Архітектура СВА:

- сенсорна підсистема - збір подій, пов'язаних з безпекою системи, що захищається;
- підсистема аналізу - виявлення атак і підозрілих дій на основі даних сенсорів;
- сховище – забезпечує накопичення первинних подій і результатів аналізу;
- консоль управління - конфігурація СВА, спостерігання за станом системи, що захищається, і СВА, переглядання виявлених підсистемою аналізу інцидентів.

СИСТЕМИ ВИЯВЛЕННЯ АТАК

Для успішного функціонування СВА в мережі повинні бути створені такі канали зв'язку:

- канали, за допомогою яких СВА здійснює моніторинг хостів і мереж;
- канали між сенсорами і керуючим сервером, по яких передаються дані про виниклі події;
- канали, за якими виконуються відповідні дії СВА. Можливий способи управління СВА:
- централізоване управління і прийняття рішення керування усім моніторингом, виявленням й звітністю здійснюється безпосередньо з єдиного «поста»);
- частково розподілене управління (моніторинг і визначення керуються з локального вузла, а ієрархічна звітність спрямовується в одне або більше центральних розташувань);
- повністю розподілене управління (моніторинг і визначення виконуються з використанням підходу, заснованому на агентах, коли рішення про відповідь приймаються в точках аналізу).

Можливості СВА

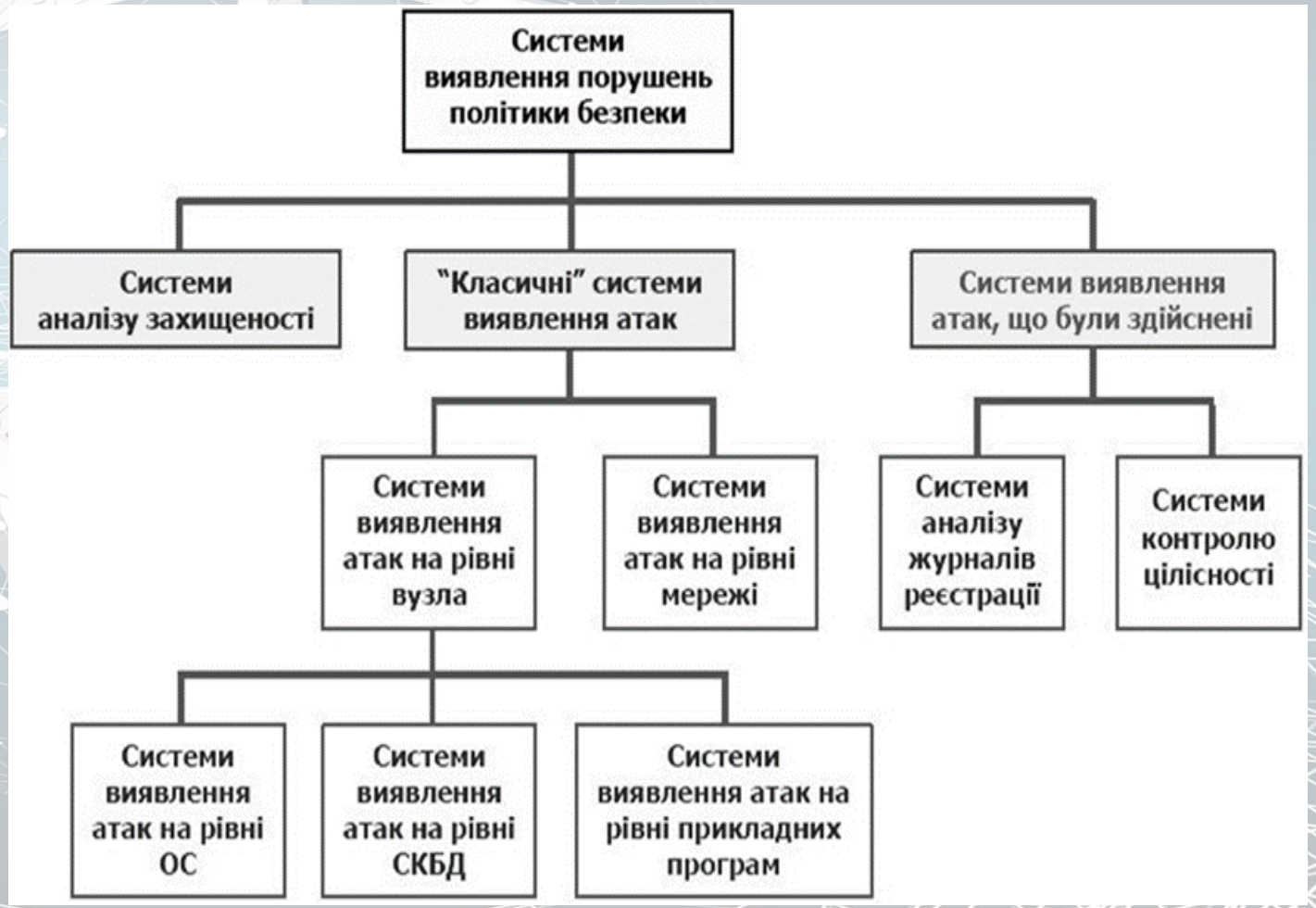
Найбільш ефективним є блокування атак у випадках, коли у системі є вже відомі, але ще не виправлені вразливості. Причини такої ситуації:

- у деяких системах не можуть бути виконані всі необхідні відновлення й модифікації;
- адміністратори іноді не мають досить часу або ресурсів для відстеження й встановлення всіх необхідних відновлень;
- користувачам можуть бути необхідні функціональність мережних сервісів і протоколів, які мають відомі уразливості;
- як користувачі, так і адміністратори роблять помилки при конфігуруванні й використанні систем.

Класифікації СВА за різними характеристиками

Відповідно етапу фіксації здійснення атаки:

- Типовим для СВА є виявлення атак у реальному часі, тобто в момент їх здійснення. Такі СВА є класичними.
- Існують системи, які здійснюють аналіз журналів реєстрації, і таким чином виявляють атаки, які були здійснені раніше.
- Іноді до СВА відносять засоби, які здійснюють аналіз системи і попереджають про потенційну можливість здійснення атаки. До таких засобів відносяться сканери вразливостей



Класифікації СВА за різними характеристиками

Відповідно до інформаційних джерел:

- СВА рівня мережі (network-based IDS);
- СВА рівня вузлів (host-based IDS) - СВА рівня ОС, СВА рівня СКБД, СВА рівня прикладних програм

Відповідно до методу аналізу:

- виявлення зловживань (misuse detection);
- виявлення аномалій (anomaly detection).

Відповідно до швидкості реакції (затримка в часі між одержанням інформації із джерела та її аналізом і реакцією на неї):

- СВА пакетного режиму (interval-based IDS). Багато ранніх СВА рівня вузлів використовували таку схему роботи, тому що вони цілком залежали від накопичення записів аудита в ОС. СВА пакетного режиму не виконують ніяких активних дій у відповідь на виявлені атаки.
- СВА реального часу (real-time IDS). СВА реального часу обробляють безперервний потік інформації від джерел. Це є переважною схемою роботи СВА рівня мережі, які одержують інформацію з потоку мережного трафіку. Виявлення проникнення, що здійснюється СВА реального часу, приводить до результатів досить швидко, і це дозволяє СВА виконувати певні дії у відповідь в автоматичному режимі.

Відповідно до характеру відповіді (набір дій, які система виконує після виявлення проникнень):

- Активні заходи. Автоматичне втручання в деяку іншу систему (наприклад, керування комутатором або мережним екраном)
- Пасивні заходи. Звіт СВА, зроблений для людей, які потім виконують деякі дії на основі даного звіту

СВА рівня мережі

СВА рівня мережі визначають атаки, захоплюючи й аналізуючи мережні пакети.

Переваги СВА рівня мережі:

- декілька оптимально розташованих СВА можуть переглядати велику мережу;
- розгортання СВА рівня мережі не впливає сильно на продуктивність мережі. Сенсори, як правило, є пасивними пристроями, які прослуховують мережний канал без впливу на нормальне функціонування мережі;
- СВА рівня мережі можуть бути зроблені практично невразливими до атак або навіть абсолютно невидимими для атакуючих.

Недоліки СВА рівня мережі:

- СВА рівня мережі, захоплюючи трафік, не гальмує роботу самої мережі, але може не встигати обробляти всі пакети у великій або зайнятій мережі.
- При підвищеному навантаженні в мережі СВА може пропустити атаку, не виявивши її.
- Необхідність швидко аналізувати пакети може призвести до того, що розробники СВА будуть обмежувати її можливості визначенням невеликої кількості атак або ж використовувати як можна менші обчислювальні ресурси, що знижує ефективність виявлення.
- У сучасних мережних технологіях намагаються уникати спільного середовища передачі даних, що ускладнює підключення сенсорів СВА рівня мережі.
- • СВА рівня мережі не можуть аналізувати зашифровану інформацію.
- • Більшість СВА рівня мережі не здатні зробити висновок про те, чи була атака успішною, вони можуть тільки визначити, що атака була розпочата. Після того як СВА виявить атаку, адміністратор повинен вручну досліджувати кожний атакований хост для визначення, чи відбулося реальне проникнення.

СВА рівня вузла

СВА рівня вузла мають справу з інформацією, зібраною усередині єдиного комп'ютера. Вони зазвичай використовують в якості інформаційних джерел журнали реєстрації подій, що створюються ОС та прикладними програмами.

Переваги СВА рівня вузла:

- СВА рівня вузла, з їхньою можливістю стежити за подіями локально по відношенню до хосту, можуть визначити атаки, які не можуть виявити СВА рівня мережі.
- На відміну від СВА рівня мережі, СВА рівня вузла можуть «бачити» наслідки початої атаки, тому що вони можуть мати безпосередній доступ до системної інформації, файлів даних і системних процесів, які є ціллю атаки
- СВА рівня вузла здатні аналізувати діяльність із великою вірогідністю й точністю, визначаючи тільки ті процеси й користувачів, які мають відношення до конкретної атаки.
- СВА рівня вузла часто можуть функціонувати в оточенні, у якому мережевий трафік зашифрований, коли джерела інформації рівня вузла створюються до того, як дані шифруються, і/або після того, як дані розшифровуються на хості призначення.
- На функціонування СВА рівня вузла не впливає топологія мережі.
- Коли СВА рівня вузла працюють із результатами аудита ОС, вони можуть надати допомогу у виявленні «троянських коней» або інших атак, які порушують цілісність ПЗ.

Недоліки СВА рівня вузла

- СВА рівня вузла більш складні у керуванні, тому що інформація повинна бути сконфігурована й повинна управлятися для кожного хоста, що переглядається.
- Джерела інформації (а іноді й частина засобів аналізу) для СВА рівня вузла розташовані на тому ж хості, що є метою атаки, тому, як складова частина атаки, СВА може бути атакована й відключена.
- СВА рівня вузла не завжди можуть визначити сканування мережі, або інші впливи, метою яких є вся мережа, тому що СВА спостерігає тільки за мережними пакетами, одержуваними конкретним хостом.
- СВА рівня вузла можуть бути блоковані деякими DoS-атаками.
- Коли СВА рівня вузла використовує результати аудита ОС як джерело інформації, об'єм інформації може бути величезним, що потребує додаткових ресурсів для зберігання в системі.
- СВА рівня вузла використовують обчислювальні ресурси хостів, за якими вони спостерігають, що впливає на продуктивність спостережуваної системи.

СВА рівня прикладних програм

СВА рівня прикладних програм (application-based IDS) є специфічною підмножиною СВА рівня вузла, які аналізують події, пов’язані з конкретним прикладним ПЗ.

Переваги СВА рівня прикладних програм:

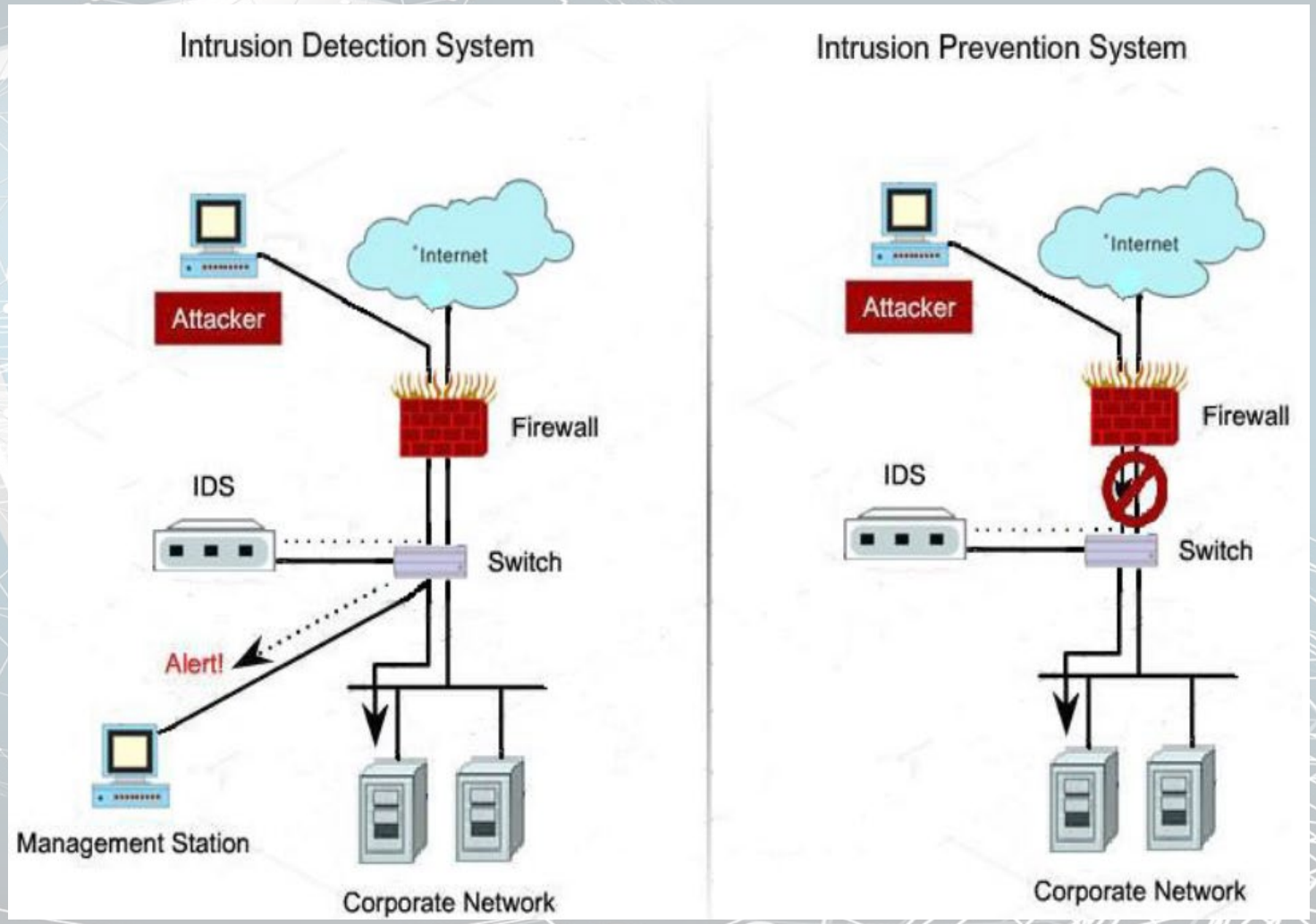
- СВА рівня прикладних програм можуть аналізувати взаємодію між користувачем і програмою, що часто дозволяє відстежити неавторизовану діяльність конкретного користувача.
- СВА рівня прикладних програм, як правило, можуть працювати в зашифрованих оточеннях, тому що вони отримують інформацію у кінцевій точці інформаційного обміну, де інформація представлена вже в незашифрованому вигляді.

Недоліки СВА рівня прикладних програм:

- СВА рівня прикладних програм можуть бути більш уразливі, ніж СВА рівня ОС, до атак на записи реєстрації подій. Тому що журнали реєстрації прикладного ПЗ можуть бути захищені менш надійно, ніж результати аудита ОС.
- СВА рівня прикладних програм часто переглядають події на користувальницькому рівні абстракції, на якому у більшості випадків неможливо визначити «троянських коней» або інші подібні атаки, пов’язані з порушенням цілісності ПЗ.
- Для компенсації зазначених недоліків СВА рівня прикладних програм доцільно використовувати у комбінації з СВА рівня ОС та/або рівня мережі.

Пасивні та активні СВА

- Пасивна СВА (Система виявлення вторгнень, IDS – Intrusion Detection System) при виявленні порушень безпеки записує інформацію про це порушення в додаток, а також надсилає інформацію про порушення на консоль та/або адміністратору системи за певним каналом зв'язку.
- Активна СВА (Система Запобігання Вторгнень, IPS – Intrusion Prevention System) веде відповідні дії на порушення, скидаючи з'єднання або перенастроюючи міжмережевий екран для блокування трафіку від зловмисника. Відповідні дії можуть проводитися автоматично або по команді оператора.



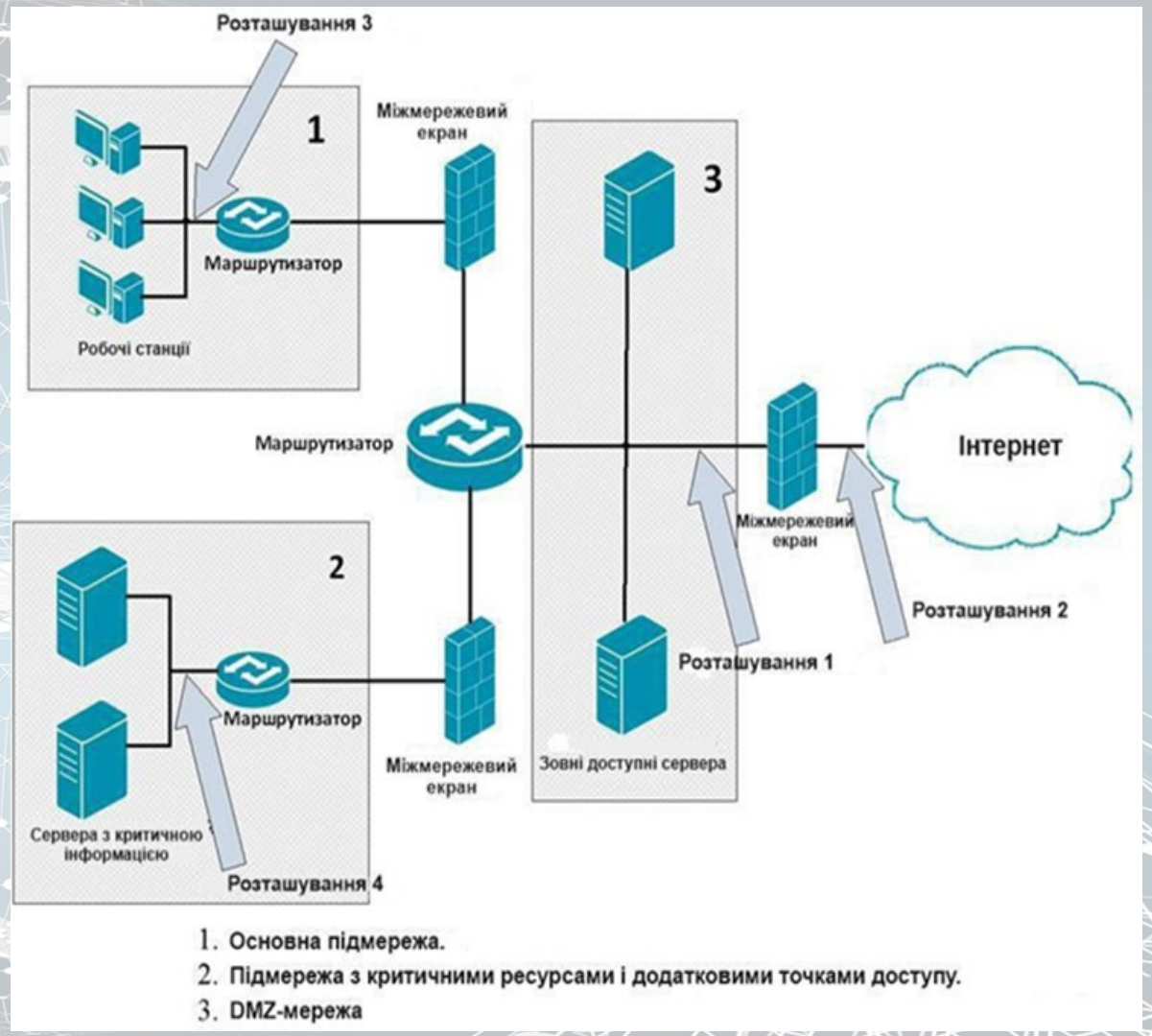
Дія пасивної (IDS) та активної (IPS) СВА

СВА і Брандмауер

Міжмережевий екран відрізняється від СВА тим, що обмежує надходження на хост або у підмережу певних видів трафіку для запобігання вторгнень і не відстежує вторгнення, що відбуваються всередині мережі.

Можливі варіанти розташування сенсорів СВА рівня мережі (рис.).

- Позаду зовнішнього брандмауера в DMZ-мережі (розташування 1).
- Перед зовнішнім фаєрволом (розташування 2).
- На основний магістральної мережі (розташування 3).
- У критичних підмережах (розташування 4).



Можливі варіанти розташування сенсорів СВА рівня мережі

Системи виявлення вторгнень (IDS-системи)

Система виявлення вторгнень (IDS) призначена для розмежування авторизованого входу й несанкціонованого проникнення, що реалізується набагато складніше.

Існують два основних типи IDS:

- вузлові (HIDS);
- мережеві (NIDS).

Система HIDS розташовується на окремому вузлі й відслідковує ознаки атак на даний вузол.

Система NIDS перебуває на окремій системі, що відслідковує мережевий трафік на наявність ознак атак, проведених у підконтрольному сегменті мережі.



Вузлові IDS (1)

Вузлові IDS (HIDS) являють собою систему датчиків, що завантажуються на різні сервера організації й керуються центральним диспетчером. Датчики відслідковують різні типи подій і вживають визначені дії на сервері або передають повідомлення. Датчики HIDS відслідковують події, пов'язані із сервером, на якому вони завантажені.

Сенсор HIDS дозволяє визначити, чи була атака успішною, якщо атака мала місце на тій же платформі, на якій встановлено датчик.

Існує п'ять основних типів датчиків HIDS:

- Аналізатори журналів.
- Датчики ознак.
- Аналізатори системних викликів.
- Аналізатори поводження застосунків.
- Контролери цілісності файлів.

Вузлові IDS (2)

- Аналізатор журналу являє собою саме те, що відбиває саму назву датчика. Процес виконується на сервері й відслідковує відповідні файли журналів у системі. Якщо зустрічається запис журналу, що відповідає деякому критерію в процесі датчика HIDS, застосовується встановлена дія.
- Датчики ознак являють собою набори визначених ознак подій безпеки, що зіставляються із вхідним трафіком або записами журналу. Розбіжність між датчиками ознак і аналізаторами журналів полягає в можливості аналізу вхідного трафіку.
- Аналізатори системних викликів здійснюють аналіз викликів між додатками й операційною системою для ідентифікації подій, пов'язаних з безпекою.
- В аналізаторах поводження датчик перевіряє виклик на предмет того, чи дозволено застосунку виконувати дану дію, замість визначення відповідності виклику ознакам атак.
- Контролери цілісності файлів відслідковують зміни у файлах. Це здійснюється за допомогою використання криптографічної контрольної суми або цифрового підпису файлу.

Мережеві IDS

NIDS являє собою програмний процес, що працює на спеціально виділеній системі.

Переваги використання NIDS:

- NIDS можна повністю сховати в мережі таким чином, що зловмисник не буде знати про те, що за ним ведеться спостереження.
- Одна система NIDS може використовуватися для моніторингу трафіку з більшим числом потенційних систем-цілей.
- NIDS може здійснювати перехоплення вмісту всіх пакетів, що направляються на систему-ціль.

Недолік системи необхідно:

- Система NIDS може тільки видавати сигнал тривоги, якщо трафік відповідає встановленим правилам або ознакам.
- NIDS може упустити потрібний трафік, який цікавить, через використання широкої смуги пропущення або альтернативних маршрутів.
- Система NIDS не може визначити, чи була атака успішною.
- Система NIDS не може переглядати зашифрований трафік.
- У мережах, які комутуються, (на відміну від мереж із загальними носіями) потрібні спеціальні конфігурації, без яких NIDS буде перевіряти не весь трафік.



Конфігурація NIDS із двома мережними картами

Установка IDS

При створенні політики IDS необхідно виконати наступні кроки:

- Цілі використання IDS визначають вимоги для політики IDS.
- Розпізнавання атак є однією з головних цілей використання IDS. Система IDS запрограмована на пошук визначених типів подій, які служать ознаками атак.
- Моніторинг політики – це менш помітний аспект діяльності по виявленню атак. Метою системи IDS, налаштованої на відстеження політики, є відстеження виконання або невиконання політики організації.
- Застосування системи IDS як засіб примусового використання політики виводить конфігурацію моніторингу політики на більш високий рівень.
- Система IDS може виявитися корисною після виявлення інциденту. У цьому випадку за допомогою IDS можна зібрати докази.

Вибір об'єкта моніторингу (1)

- Вибір об'єкта моніторингу залежить від цілей, поставлених перед системою IDS, і від середовища, у якій IDS буде функціонувати. У таблиці приводяться приклади об'єктів моніторингу при використанні конкретних політик
- Вибір об'єкта моніторингу визначає розташування датчиків. Датчики можуть бути розташовані поза міжмережевого екраном, усередині мережі, на системах із секретною інформацією або на системах, використовуваних спеціально для збору й обробки даних журналу.

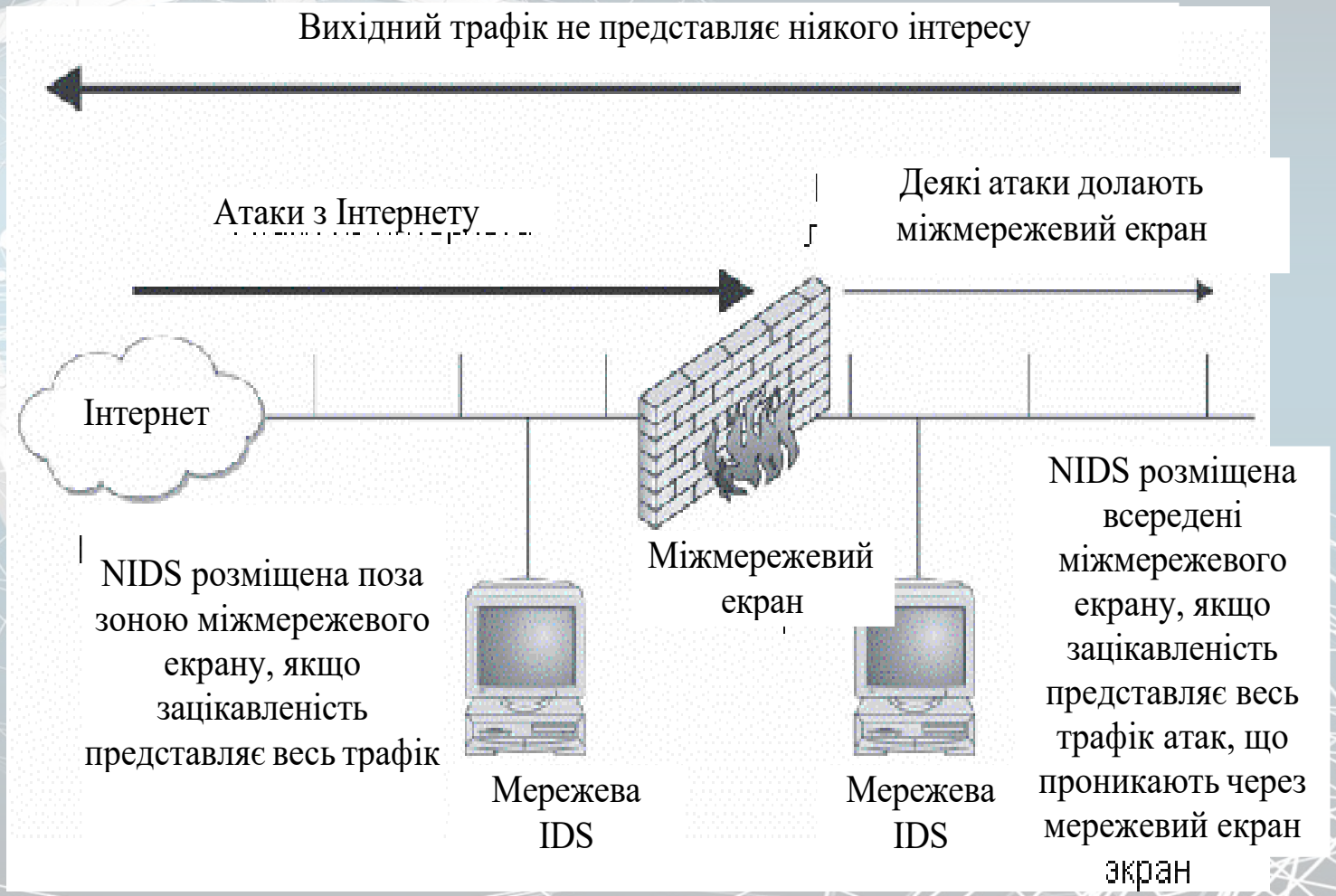
Політика	NIDS	HIDS
Виявлення атак	Весь трафік, що надходить на системи, що атакуються потенційно (мережні екрани, веб-сервери, сервери застосунків і т.д.)	Невдалі спроби входу. Спроби з'єднання. Вдалий вхід з віддалених систем.
Запобігання атак	Те ж, що й для виявлення атак	Те ж, що й для виявлення атак.
Виявлення порушень політики	Весь трафік HTTP, формований на системах клієнтах. Весь трафік FTP, формований на системах клієнтах	Успішні HTTP- з'єднання. Успішні FTP з'єднання. Файли, що завантажуються.
Примус до використання політик	Те ж, що й для виявлення порушень політики	Те ж, що й для виявлення порушення політики.
Примус до відповідності політикам з'єднань	Весь трафік, що порушує примусово використовувану політику з'єднання	Успішні з'єднання із заборонених адрес або по заборонених портах.
Збір доказів	Вміст усього трафіку, формованого на системі-цілі або атакуючій системі	Всі успішні підключення, що виходять із атакуючої системи. Всі невдалі з'єднання з атакуючих систем. Всі натискання клавіш із інтерактивних сеансів на атакуючих системах.

Вибір об'єкта моніторингу (2)

Приклад вибору об'єкта моніторингу на рис.

Якщо в мережі використовуються комутатори замість концентраторів, датчик NIDS не буде правильно працювати, якщо він просто підключений до порту комутатора.

Ключовим моментом, про який необхідно пам'ятати при винесенні рішення з приводу розміщення датчика IDS, є те, що датчик повинен мати можливість перегляду подій, які цікавлять, будь то мережний трафік або запис журналу.



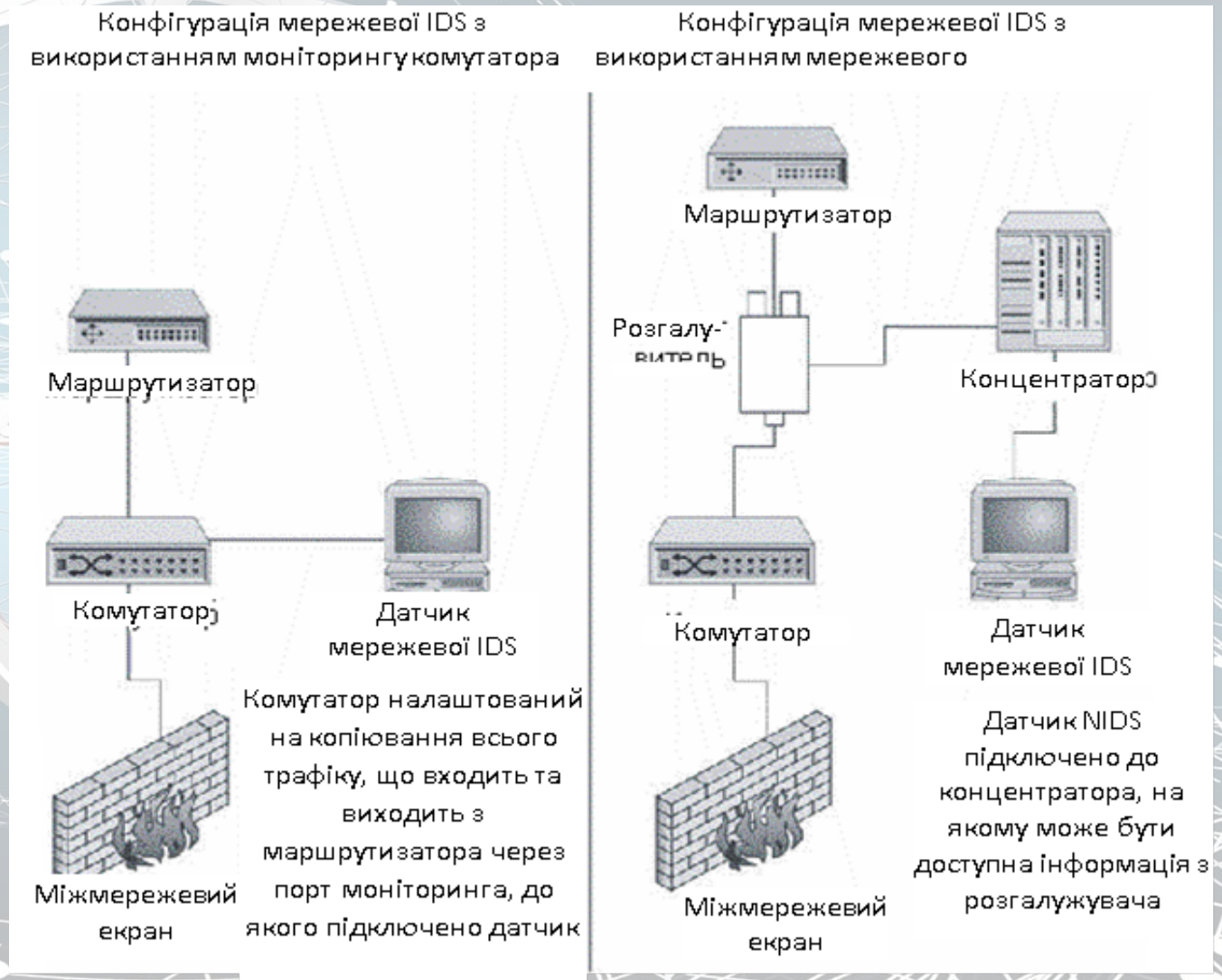
Вибір об'єкта моніторингу (3)

У випадку з мережею, яка комутується, існують два варіанти використання датчиків NIDS:

- застосування порту, що відслідковує комутатор
- застосування мережевого розгалужувача.

На рисунку показані конфігурації обох типів.

Розгалужувачі – це пасивні провідні з'єднання між двома пристроями (наприклад, між маршрутизатором і комутатором). Як правило, розгалужувач підключається до концентратора, до якого також приєднаний датчик NIDS. Це дозволяє датчику відслідковувати трафік.



Вибір об'єкта моніторингу (4)

- Аналогічно вибору об'єкта моніторингу, вибір відповідних дій залежить від цілей, для яких використовується система IDS.
- Пасивна обробка – це найпоширеніший тип дій, що вживаються при виявленні вторгнення. Причина цьому проста – пасивні відповідні дії забезпечують меншу ймовірність ушкодження легітимного трафіку, будучи, у той же час, найбільш простими для автоматичного застосування та вткористовують наступні заходи:
  - Запобігання
  - Ведення журналів
  - Ведення додаткових журналів.
  - Використання виділеного сервера журналів.
  - Повідомлення
- Активна обробка події дозволяє швидко вжити можливих заходів для зниження рівня шкідливої дії події.
  - Переривання з'єднань, сеансів або процесів.
  - Переналаштовування мережі.
  - Обманні дії.
  - Обманна дія "горщик з медом".

Автоматична й автоматизована відповідь

- Автоматична відповідь – це набір встановлених операцій, які виконуються при виникненні визначених подій.
- У таблиці наведені приклади відповідних пасивних і активних відповідних дій з використанням набору політик, що був визначений вище.

Політика	Пасивні відповідні дії	Активні відповідні дії
Виявлення атак	Ведення журналів Ведення додаткових журналів Повідомлення	Немає відповідної активної дії.
Запобігання атак	Ведення журналів Повідомлення	Закриття з'єднання. Завершення процесу. Можливе переналаштовування маршрутизатора або міжмережевого екрана.
Виявлення порушень політики	Ведення журналів Повідомлення	Немає відповідної активної дії.
Примусове використання політик	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштовування проксі.
Примусове використання політик з'єднання	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштовування маршрутизатора або міжмережевого екрана.
Збір доказів	Ведення журналів Ведення додаткових журналів Повідомлення	Обманні дії. Можливе закриття з'єднання.

Визначення порогів

Граничні значення забезпечують захист від помилкових спрацьовувань, що підвищує ефективність політики IDS.

Параметри, які необхідно взяти до уваги при налаштовуванні граничних значень

- Досвід користувача.
- Швидкісні характеристики мережі.
- Очікувані мережні з'єднання.
- Навантаження на співробітника з адміністрування або безпеки.
- Чутливість датчика.
- Ефективність програми безпеки.
- Наявні уразливості.
- Рівень таємності систем і інформації.
- Наслідки помилкових спрацьовувань.
- Наслідки неспрацьовування.

Застосування системи IDS (1)

Перед прийняттям в організації рішення про використання IDS (будь то комерційна система або некомерційна) керівництво організації повинно чітко визначити цілі застосування програми.

Система виявлення вторгнень може тільки видавати звіти про ті події, на виявлення яких вона налаштована. Конфігурація IDS складається із двох компонентів. Першою з них є ознаки атак, запрограмовані в системі. Другий компонент – будь-яким додаткові, визначені адміністратором, події, що також предствляють інтерес.

З умовою правильної конфігурації IDS можна привести чотири типи подій, про які буде повідомляти система IDS:

- Події дослідження.
- Атаки.
- Порушення політики.
- Підозрілі або непояснені події.

Застосування системи IDS (2)

- Події дослідження являють собою спроби атакуючого зібрати дані про систему перед безпосереднім проведенням атаки. Ці події можна розділити на п'ять категорій:
  - "Сховане" сканування.
  - Сканування портів.
  - Сканування "троянських коней".
  - Сканування уразливостей.
  - Відстеження файлів.
- Події атак вимагають найшвидшої відповідної реакції. В ідеальному випадку IDS повинна бути налаштована тільки на ідентифікацію подій високого пріоритету у випадку використання відомої внутрішньої уразливості.
- Більша частина систем IDS поставляється з ознаками наступних подій політики безпеки:
  - Загальний доступ до файлів (Gnutella, Kazaa і т.д.);
  - обмін миттєвими повідомленнями;
  - сеанси Telnet;
  - команди "r" (rlogin, rsh, rexec).
- Події, що не відповідають повністю ні одній з інших категорій, заносяться в категорію підозрілих подій. Підозрілою подією називається подія, що не вдалося розпізнати.

Дослідження підозрілих подій (1)

При виникненні підозрілих дій варто виконати процедуру, що складається з наступних кроків, щоб визначити, чи є дана дія вдалим вторгненням або спробою проникнення, або вона носить нешкідливий характер. Отже, потрібно виконати наступні кроки:

- ідентифікувати систему. Ця процедура може полягати в перетворенні IP-адрес в іменах вузлів;
- записувати в журнал відомості про додатковий трафік між джерелом і пунктом призначення. Одна-єдина окрема подія може не представляти повну інформацію про трафік між двома системами. ;
- записувати в журнал весь трафік, що виходить із джерела. Мається на увазі, що даних, фіксуємих за допомогою запису всього трафіку між двома системами, недостатньо для визначення того, чи є активність легітимною, можна почати збір іншого трафіку, що надходить із джерела.;
- записувати в журнал вміст пакетів із джерела. За допомогою занесення в журнал вмісту пакетів можна скласти повний запис сеансу, а також зафіксувати команди, призначення, що відправляються безпосередньо в пункт.

Дослідження підозрілих подій (2)

Приклад конфігурації IDS із записом у журнал усього трафіку між двома системами

Ім'я події	Дія	IP-адреса джерела	IP-адреса пункту призначен-ня	Протокол	Порт джерела	Кінцевий порт
SUS_ACT	Повідом-лення, занесен- ня в журнал	Джерело підозрілої активності	Пункт призначення підозрілої активності	TCP,UDP і/або ICMP, залежно від типу виявленої активності	Будь-який	Будь-який

Приклад конфігурації IDS, призначеної для занесення в журнал усього трафіку, що виходить із визначеної адреси джерела

Ім'я події	Дія	IP-адреса джерела	IP-адреса пункту призначення	Протокол	Порт джерела	Кінцевий порт
SUS_SRC	Повідом-лення, запис у журнал	Джерело підозрілих дій	Будь-який	TCP,UDP і/або ICMP, залежно від типу виявленої активності	Будь-який	Будь- який

Приклад конфігурації IDS, що здійснює перехоплення вмісту пакетів

Ім'я події	Дія	IP-адреса джерела	IP-адреса пункту призначення	Прото-кол	Порт джерела	Кінце-вий порт
SUS_ACT	Повідом-лення, запис у журнал умісту пакета	Джерело підозрілої активності	Пункт призначення підозрілої активності	TCP або UDP	Будь-який	Порт, на який спрямо-ваний підозрі-лий трафік
SUS_ACT	Повідом-лення, запис у журнал умісту пакета	Пункт призначення з підозрілої активності	Джерело підозрілої активності	TCP або UDP	Порт, на який спрямо-ваний підозрі-лий трафік	Будь-який

Розгортання мережної IDS

1. Визначте, які дії ви намагаєтеся здійснити за допомогою розгортання датчика IDS. Це допоможе чітко обрисувати цілі застосування IDS.
2. На основі цілей застосування IDS визначите, який мережний трафік потрібно відслідковувати.
3. Тепер вирішіть, яким чином будуть оброблятися різні події, що виявляються IDS. Спробуйте визначити, що буде розумніше – доручити виконання деякої дії системі IDS або операторові, що буде виконувати потрібну процедуру.
4. При відсутності досвіду роботи з датчиком IDS вам доведеться нелегко при першій установці граничних значень. Якщо у вашому огляді є вже функціонуюча система IDS, можете подивитися, які граничні значення встановлені на цій системі для різних ознак атак.
5. Складіть план розгортання IDS. Визначте, кого в організації потрібно задіяти для виконання цього завдання.
6. Якщо ви хочете спробувати здійснити розгортання датчика NIDS, виділіть для цього комп'ютер і встановіть на нього Linux, FreeBSD або іншу версію операційної системи сімейства Unix.
7. Завантажте останню версію програми Snort (безкоштовна IDS) із сайту http://www.snort.org/.
8. Додержуйтеся інструкцій по установці й виконаєте інсталяцію програми Snort. Можна також установити ряд додаткових програмних пакетів для спрощення процесу керування й конфігурації.
9. Підключіть датчик до мережі. Найкраще зробити це за допомогою концентратора. Проте, можна також використовувати порт розгалужувача на комутаторі.
10. Розмістивши датчик на потрібному місці, перегляньте файли журналів, щоб з'ясувати, які події в них фіксуються. Також можна використовувати програму Acid для перегляду файлів журналу через веб-інтерфейс. Acid – це веб-інтерфейс, використовуваний для аналізу даних програми Snort.

Системи протидії вторгненням (IPS-системи)

Система запобігання вторгнень (англ. Intrusion Prevention System) – програмна або апаратна система мережевої й комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки й автоматично захищає від них.

IDS/IPS-системи використовуються для виявлення аномальних дій у мережі, які можуть порушити безпеку й конфіденційність даних, наприклад: спроби використання уразливостей програмного забезпечення; спроби підвищення привілеїв; несанкціонований доступ до конфіденційних даних; активність шкідливих програм і т.д.

Використання IPS-систем переслідує кілька цілей:

- виявити вторгнення або мережну атаку й запобігти їм;
- спрогнозувати можливі майбутні атаки й виявити уразливості для запобігання їхнього подальшого розвитку;
- виконати документування існуючих погроз;
- забезпечити контроль якості адміністрування з погляду безпеки, особливо великих і складних мереж;
- одержати корисну інформацію про проникнення, які мали місце, для відновлення й коректування факторів, що викликали проникнення;
- визначити розташування джерела атаки стосовно локальної мережі (зовнішні або внутрішні атаки), що важливо при прийнятті рішень про розташування ресурсів у мережі.

IPS-системи (2)

У цілому, IPS аналогічні IDS. Головна ж відмінність полягає в тому, що вони функціонують у реальному часі й можуть в автоматичному режимі блокувати мережні атаки. Кожна IPS містить у собі модуль IDS.

IDS, у свою чергу, звичайно складається з:

- системи збору подій;
- системи аналізу зібраних подій;
- сховища, у якому накопичуються зібрані події й результати їхнього аналізу;
- бази даних про уразливості (цей параметр є ключовим, так як чим більше база у виробника, тим більше погроз здатна виявляти система);
- консолі керування, що дозволяє будувати всі системи, здійснювати моніторинг стану мережі, яка захищається, переглядати виявлені порушення й підозрілі дії.

IPS-системи (3)

Класифікація:

- Мережні IPS (Network-Based Intrusion Prevention, NIPS): відслідковують трафік у комп'ютерній мережі й блокують підозрілі потоки даних.
- IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS): перевіряє активність у бездротових мережах. Зокрема, виявляє невірно зконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфінг mac-адрес.
- Поведінковий аналіз мережі (Network Behavior Analysis, NBA): аналізує мережний трафік, ідентифікує нетипові потоки, наприклад DoS і DDoS-атаки.
- Система запобігання вторгнень для окремих комп'ютерів (Host- Based Intrusion Prevention, HIPS): резидентні програми, що виявляють підозрілу активність на комп'ютері.

За способами моніторингу IPS-системи можна розділити на дві великі групи: NIPS (Network Intrusion Prevention System) і HIPS (Host Intrusion Prevention System). Перша група орієнтована на мережевий рівень і корпоративний сектор, у той час як представники другої мають справу з інформацією, що зібрана всередині єдиного комп'ютера, а отже можуть використовуватися на персональних комп'ютерах.

Серед NIPS і HIPS також виділяють:

- Protocol-Based IPS, PIPS. Являє собою систему (або агент), що відслідковує й аналізує комунікаційні протоколи зі зв'язаними системами або користувачами.
- Application Protocol-Based IPS, APIPS. Являє собою систему (або агент), що веде спостереження й аналіз даних, переданих з використанням специфічних для визначених застосунків протоколів. Наприклад, відстеження вмісту SQL-команд.

HIPS (1)

HIPS (Host-Based Intrusion Prevention System, англ. система запобігання вторгнень) – проактивна технологія захисту, побудована на аналізі поводження. HIPS-продукти здійснюють аналіз активності програмного забезпечення й всіх модулів системи й блокування потенційно небезпечних дій у системі користувача. Аналіз активності здійснюється за рахунок використання перехоплювачів системних функцій або установці так званих міні-фільтрів.

Види HIPS:

- Класичні HIPS. Класичні HIPS-продукти надають користувачеві інформацію про активність того або іншого застосунку, однак рішення про дозвіл/заборону тої або іншої операції повинен приймати користувач, таким чином класичні HIPS-продукти дозволяють користувачеві тонко налаштувати ті або інші правила контролю, але створення правил вимагає високої кваліфікації користувача.
- Експертні HIPS. На відміну від класичних HIPS-продуктів, експертні HIPS можуть самостійно ухвалювати рішення щодо блокуванні тієї або іншої активності, виходячи з правил і алгоритмів, закладених розроблювачем продукту. Для використання експертних HIPS-продуктів користувачеві не обов'язково мати визначену кваліфікацію, однак експертні HIPS-продукти в ряді випадків можуть блокувати легітимну активність користувальницького програмного забезпечення, або можуть не визнати дану активність програми за шкідливу.

HIPS (2)

Механізми ухвалення рішення IPS

- По-перше, наскільки повні вихідні дані, з яких джерел вони зібрані?
- По-друге, скільки підходів використовуються при ухваленні рішення і які вони?
- По-третє, наскільки обмежений у ресурсах (часових, обчислювальних, пам'яті, базі даних) хост, відповідальний за прийняття рішення про вторгнення?
- По-четверте, чи передбачена можливість втручання оператора в процес ухвалення рішення?
- І, нарешті, чи існують недетерміновані ситуації, у яких системі потрібне втручання оператора?

Механізми видаленого керування IPS:

- Наскільки надійні використовувані в IPS механізми віддаленого керування й наскільки вони розвинені?
- Чи будуть канали керування успішно функціонувати у випадку проведення DDoS-атаки на мережу?
- Чи може внутрішній зловмисник одержати керування системою IPS і модифікувати логіку її роботи?

Механізми централізованого керування IPS:

- Чи передбачені в IPS механізми централізованого завдання нових правил реакції IPS з їх наступним вибірним впровадженням на окремі модулі IPS?
- Чи можливо об'єднання окремих IPS у групи й формування групових політик?

Запобігання вторгненням за допомогою системи IDS

Для запобігання за допомогою NIDS успішного проведення атак на систему рішення по пакету повинно прийматися до того, як пакет досягне системи-цілі. Це означає, що архітектуру системи NIDS потрібно змінити таким чином, щоб датчик NIDS був розташований на одному каналу зв'язку із трафіком (як міжмережевий екран), а не просто стежив за минаючим трафіком (рисунок).



Проблеми, пов'язані з виявленням вторгнень

Заміна реактивної природи IDS на превентивну створює деякі проблеми. Дійсно, після цієї зміни виникають два серйозних питання:

- Відмова в обслуговуванні
- Доступність
- Відповідальність
- Повнота контролю трафіку
- Гнучкість підходу: можливість модифікації списку погроз

Повнота бачення/структура IPS

- Рівень 1 – мережа
  При роботі в реальній мережі нерідко виникають ситуації, коли трафік, що направляється через кілька пристроїв мережних IPS паралельно, не задовольняє критеріям вторгнення, а при розгляді його в сукупності, є вторгненням.
- Рівень 2 – існуюча інфраструктура
  Можливість збору інформації не тільки від мережевих модулів IPS, але й від хостових модулів IPS, дозволяє визначати взаємозв'язки між трафіком, реєструємими мережевими модулями, і станом хостів, реєструємими хостовими модулями
- Рівень 3 – розвиток інфраструктури
  Паралельно з розвитком механізмів IPS інформаційна інфраструктура компаній також еволюціонує. Все більший розвиток мобільних інструментів мережевої взаємодії не може залишатися непоміченим виробниками IPS.

Ключові тенденції розвитку систем виявлення вторгнень

- На рівні виявлення вторгнень
  - розширення спектра підтримуваних прикладних протоколів, особливо з урахуванням розвитку індустрії IP-телефонії, технології VoIP і росту популярності сервісу Video-On-demand, практично скрізь використання систем миттєвого обміну повідомленнями й т.п.
  - додавання підтримки мобільних пристроїв і механізмів аналізу взаємодії з мобільними пристроями.
  - більш глибоке пророблення алгоритмів функціонування вже підтримуваних прикладних протоколів, включаючи механізми контролю стану сеансу; як наслідок; підвищення гнучкості визначення факту вторгнення.
  - використання систем запобігання вторгнень для запобігання витоку конфіденційної інформації з організації по різних каналах.
- На функціональному рівні.
  - Це, по-перше, додавання функцій профілювання трафіку й введення механізмів якості обслуговування на рівні систем запобігання вторгнень.
  - По-друге, розширення можливостей централізованого керування системами запобігання вторгнень.
  - По-третє, розвиток засобів перетворення елементарних подій безпеки в "макро"-події, зручні для оператора.
- На рівні інфраструктури IPS.
  - По-перше, розширення інтеграції хостових і мережевих систем запобігання вторгнень для поліпшення точності виявлення вторгнень.
  - І, по-друге, розширення можливостей для інтеграції продуктів різних виробників, уніфікація форматів передачі даних і керуючих впливів.
  - структура системи запобігання вторгнень буде прагнути до розподіленої системи з модулями різних типів (і, можливо, що є розробками різних виробників) і єдиним центром прийняття рішень, що одержують інформацію про події й передає керуючу інформацію з використанням стандартизованих протоколів обміну інформацією.



Протоколи захищених каналів

Модель взаємодії ISO/OSI та стек протоколів TCP/IP

Стек TCP/IP отримав широке поширення завдяки наступним властивостям:

- найповніший стандартний і водночас популярний стек мережевих протоколів з багаторічною історією;
- практично всі великі мережі передають основну частину свого трафіку за допомогою TCP/IP.
- всі сучасні операційні системи підтримують стек TCP/IP;
- спосіб отримання доступу до мережі Інтернет;
- гнучка технологія підключення різнорідних систем на рівні як транспортних підсистем, так і прикладних сервісів;
- основа для створення корпоративної інтранету з використанням транспортних послуг Інтернет і розробленої в мережі Інтернет технології гіпертексту WWW;
- Стабільне, масштабоване, кросплатформне середовище для клієнт-серверних додатків

Способи утворення захищеного каналу

Технологія захищеного каналу забезпечує захист трафіку між двома точками в відкритій транспортній мережі, наприклад в Інтернеті. Захищений канал має на увазі виконання трьох основних функцій:

- взаємна автентифікація абонентів при встановленні з'єднання, яка може бути виконана, наприклад, шляхом обміну паролями;
- захист переданих по каналу повідомлень від несанкціонованого доступу, наприклад шляхом шифрування;
- підтвердження цілісності вступників по каналу повідомлень, наприклад шляхом передачі одночасно з повідомленням його дайджесту.

Залежно від місця розташування програмного забезпечення захищеного каналу розрізняють дві схеми його утворення:

- схема з кінцевими вузлами, взаємодіючими через публічну мережу (рис. а);
- схема з обладнанням постачальника послуг публічної мережі, розташованим на межі між приватною і публічною мережами (рис. б).



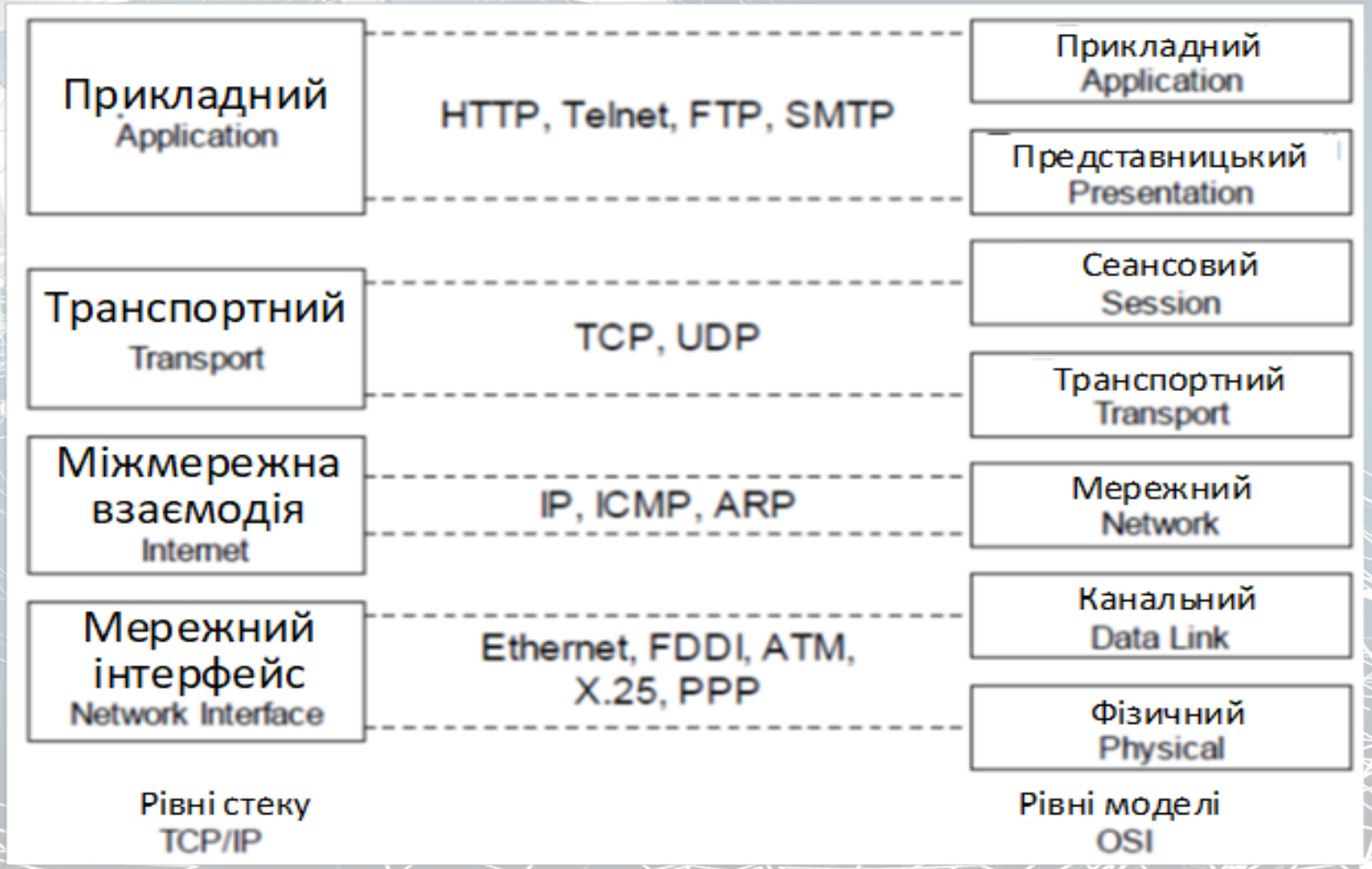
Ієрархія технологій захищеного каналу

- Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі OSI (табл.)
- Якщо захист даних здійснюється засобами верхніх рівнів (прикладного, відображення або сеансового), то такий спосіб захисту не залежить від технологій транспортування даних (IP або IPX, Ethernet Або ATM), що можна вважати перевагою.
- Захищений канал, реалізований на найвищому (прикладному) рівні, захищає тільки певну мережеву службу, наприклад файлову, гіпертекстову або поштову. Так, протокол S/MIME захищає виключно повідомлення електронної пошти.
- Засоби захищеного каналу стають прозорими для додатків в тих випадках, коли безпека забезпечується на мережевому і канальному рівнях. Однак тут виникає інша проблема – залежність сервісу захищеного каналу від протоколу нижнього рівня. Наприклад, протокол PPTP, не будучи протоколом канального рівня захищає кадри протоколу PPP канального рівня, упаковуючи їх в IP-пакети
- Протокол IPSec, який працює на мережевому рівні є компромісним варіантом. З одного боку, він прозорий для додатків, з іншого – може працювати практично у всіх мережах, так як базується на широко поширеному протоколі IP і використовує будь-яку технологію канального рівня (PPP, Ethernet, ATM і т. д.).

Рівні моделі OSI	Протоколи захищеного каналу	Властивості протоколів захищеного каналу
Прикладний рівень	S/MIME	Непрозорість для додатків, незалежність від транспортної інфраструктури
Рівень відображення	SSL, TLS	
Сеансовий рівень		
Транспортний рівень		
Мережевий рівень	IPSec	Прозорість для додатків, залежність від транспортної інфраструктури
Канальний рівень	PPTP	
Фізичний рівень		

Структура та функціональність стека протоколів TCP/IP

- Стек протоколів TCP/IP складається з чотирьох рівнів: додаток, транспорт, Інтернет і мережа. Для порівняння на рис. На малюнку також показані сім шарів моделі OSI.



Логічні та фізичні зв'язки між рівнями стека TCP/IP

Багаторівневі протоколи стека TCP/IP розроблені таким чином, що певний рівень хоста призначення отримує точно такий самий об'єкт, який був надісланий еквівалентним рівнем вихідного хоста. Кожен шар стека одного хоста утворює логічний зв'язок з рівнем стека з такою ж назвою іншого хоста. Коли фізичне з'єднання реалізується, шар передає свої дані інтерфейсу рівня, який знаходиться вище або нижче в тому ж хості. Рис. показано, як здійснюється фізичний і логічний зв'язок рівнів. Вертикальні стрілки показують фізичне з'єднання в межах одного хоста, а горизонтальні стрілки показують логічний зв'язок між тими ж шарами в різних хостах.

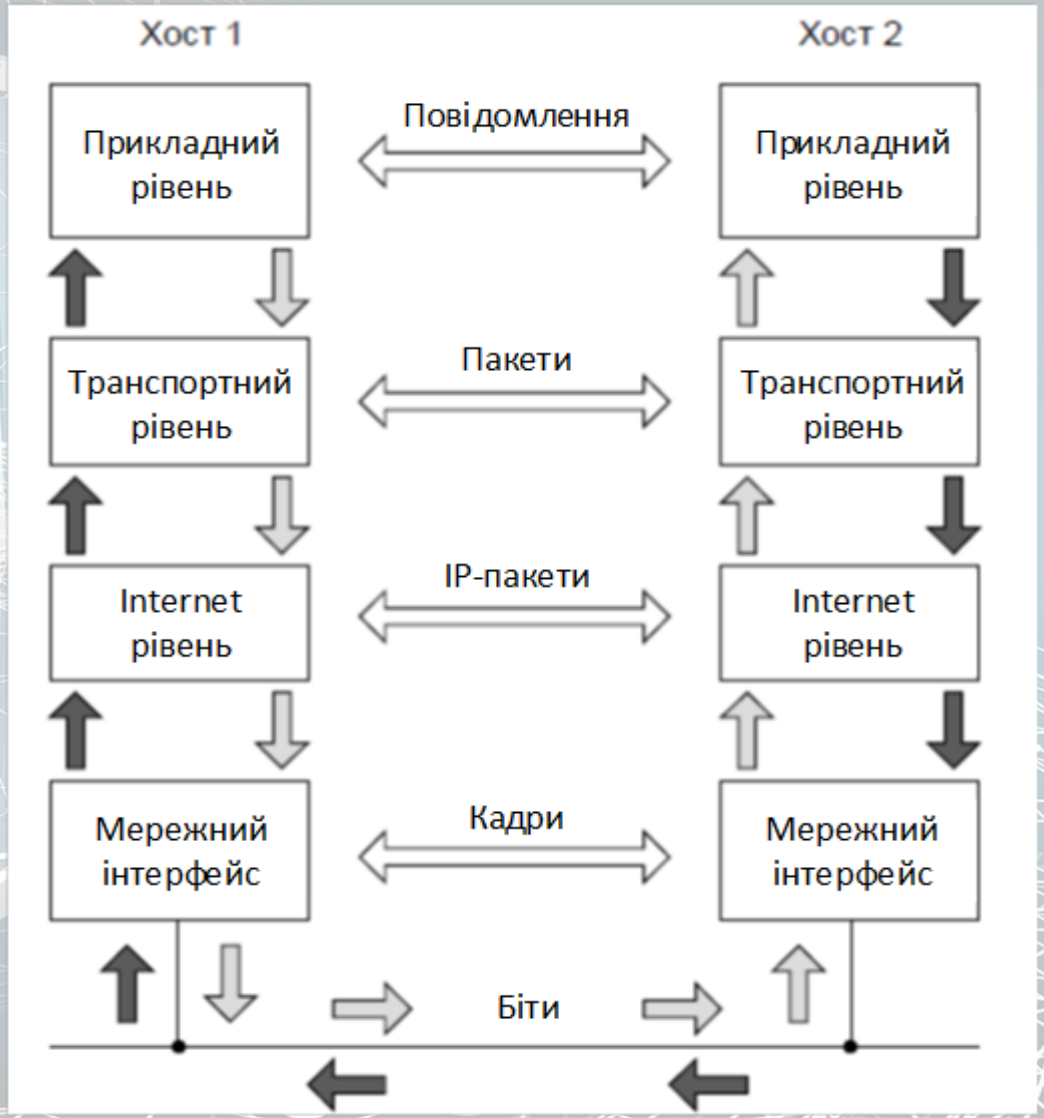
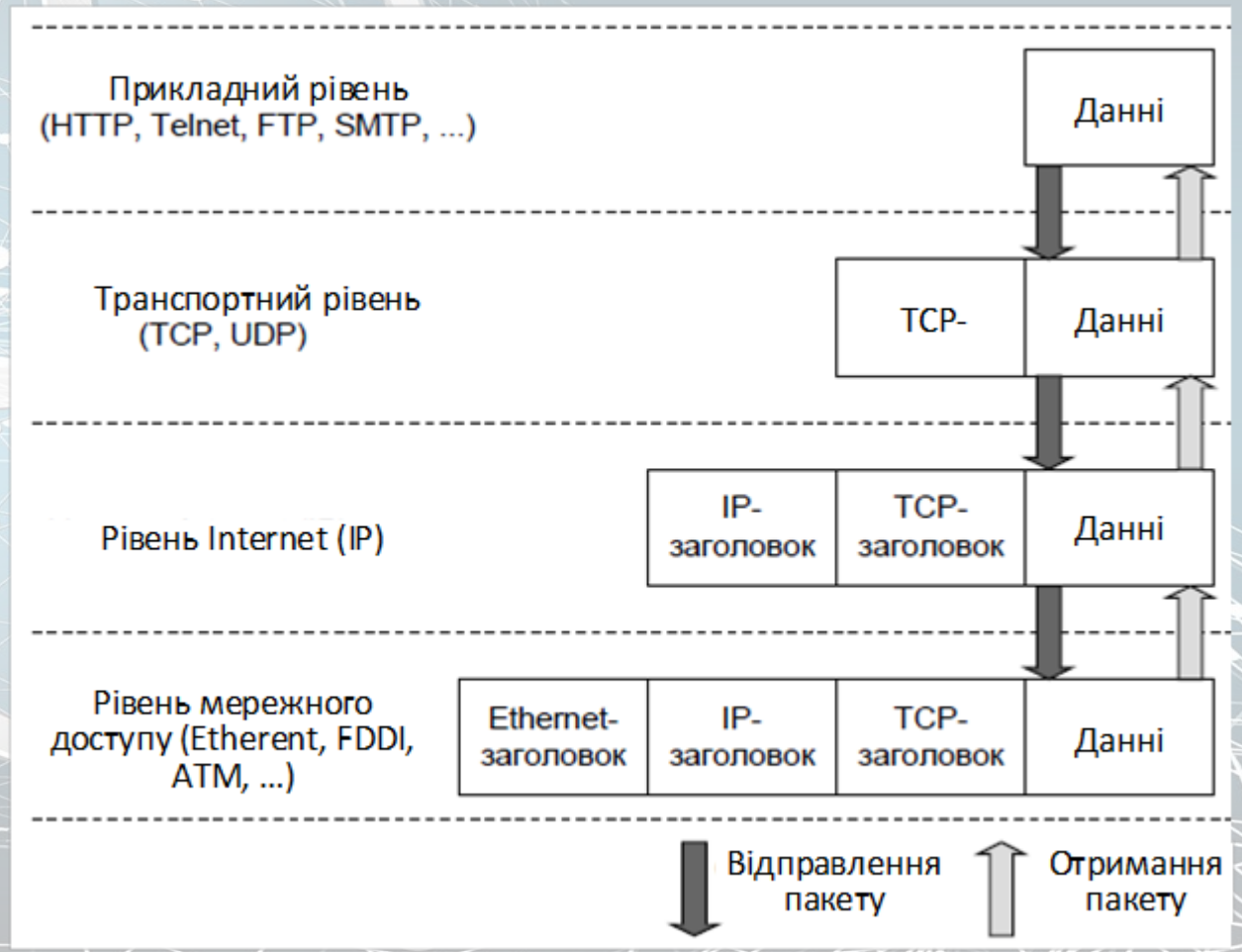


Схема інкапсуляції даних стека TCP/IP

- На рис. показана схема процесу інкапсуляції переданих даних і генерації пакетних заголовків в стеку TCP/IP.
- У системі, яка отримує цей потік інформації, заголовки послідовно видаляються в міру обробки даних і передачі їх вгору по стеку. Такий підхід забезпечує необхідну гнучкість в обробці переданих даних, так як до верхніх шарів не потрібно торкатися технології, що використовується на нижніх рівнях.



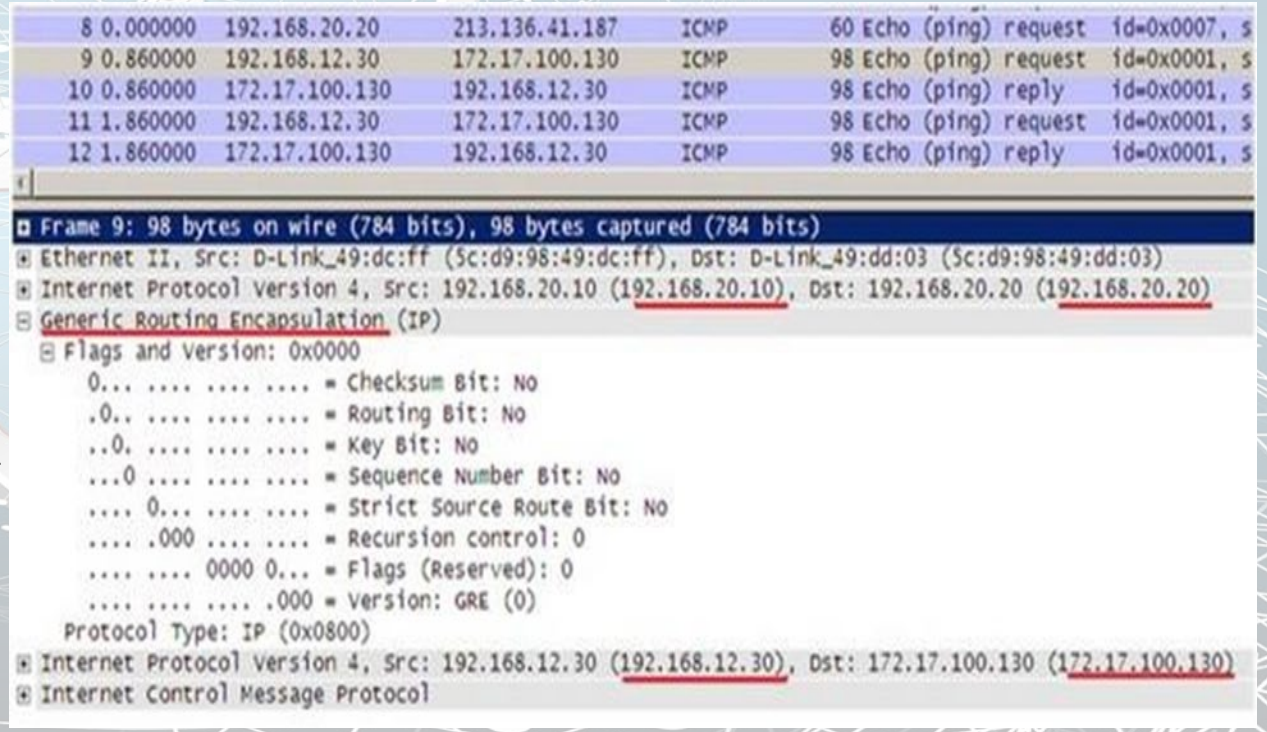
Протокол GRE

Протокол GRE (Generic Routing Encapsulation) дозволяє інкапсулювати будь-який протокол. Це може бути використане для будь-яких цілей, наприклад:

- Використовується в поєднанні з PPTP для створення віртуальних приватних мереж (VPN);
- застосовується в технології WDS для координації дій точок доступу і контролера WDS.
- використовується в технологіях мобільного IP.

Формат GRE-пакета

Заголовок протоколу доставки
Заголовок GRE
Вміст пакету GRE



Віртуальні приватні мережі

VPN використовуються у двох основних сценаріях:

- Для з'єднання двох віддалених локальних мереж, використовуючи як транспорт мережу з іншими параметрами безпеки.
- Для входу віддаленого користувача в локальну мережу, використовуючи як транспорт мережу з іншими параметрами безпеки.

Основні протоколи створення VPN та їхні характеристики з погляду безпеки створюваних з'єднань, можливостей масштабування й наявності яких-небудь додаткових можливостей (табл.).

Назва протоколу	Конфіден-ційність з'днання	Цілісність з'днання	Способи автентифікації учасників	Захист від можливості на майбутнє підлаштову-ватися під одну зі сторін
PPP	Є	Немає	CHAP	Немає
PPPoE	Є	Немає	CHAP	Немає
PPTP	Є	Немає	CHAP	Немає
L2TP	Є	Немає	CHAP	Немає
IPSec	Є	Є	Загальний секрет, сертифікат	Є
L2TP/IPSec	Є	Є	CHAP, загальний секрет, сертифікат	Є
GRE/IPSec	Є	Є	Загальний секрет, сертифікат	Є
SSL	Є	Є	Сертифікат	Є

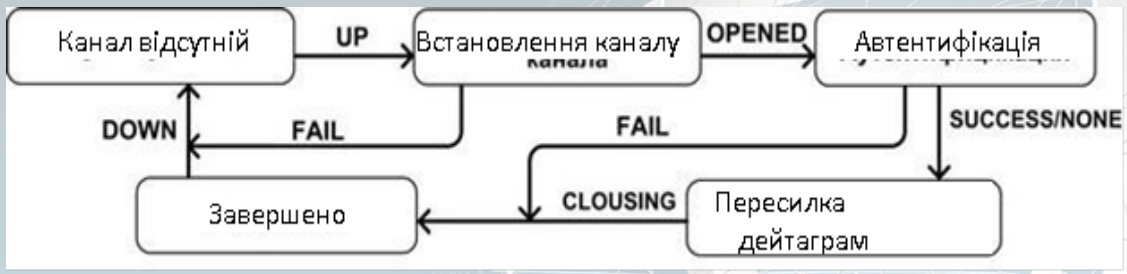
Протоколи канального рівня PPP (1)

Протокол Point-to-Point Protocol (PPP) – двоточковий протокол канального рівня (Data Link) мережевої моделі OSI. Зазвичай використовується для встановлення прямого зв'язку між двома вузлами мережі, причому він може забезпечити автентифікацію з'єднання, шифрування (з використанням ECP, RFC 1968) і стиснення даних. Використовується на багатьох типах фізичних мереж: нуль-модемний кабель, телефонна лінія, стільниковий зв'язок і т. д.

L2TP концентратор доступу (L2TP Access Concentrator – LAC)	Вузол, що є однією з кінцевих точок L2TP-тунелю. LAC є протилежною стороною L2TP мережного серверу (LNS). LAC розташований між LNS і віддаленою системою й перенаправляє пакети до кожної з них. Пакети, що посилаються від LAC до LNS, тунелюються за протоколом L2TP. З'єднання між LAC і віддаленою системою є або локальним, або виконується за протоколом PPP. Якщо замість L2TP використовується протокол PPTP, то аналогічний вузол називається PPTP концентратор доступу – PAC.
L2TP мережний сервер (L2TP Network Server – LNS)	Вузол, що є однієї з кінцевих точок L2TP-тунелі. LNS є протилежною стороною LAC. LNS є логічною кінцевою точкою PPP-сесії, що тунелюється від віддаленої системи за допомогою LAC. LNS також є кінцевою точкою тунелю між LNS і LAC. Якщо замість L2TP використовується протокол PPTP, то аналогічний вузол називається PPTP мережний сервер – PNS.
Сервер мережного доступу (NAS)	Пристрій, що надає користувачам мережний доступ на вимогу. Цей доступ є доступом типу точка-точка, що використовує PSTN або ISDN канали. Функції NAS може виконувати й LAC, і LNS.
L2TP/ PPTP-тунель	Тунель між LAC і LNS. Тунель складається з керуючого з'єднання й нуля або більше L2TP-сесій. L2TP/ PPTP- тунель передає інкапсульовані дейтаграми PPP і керуючі повідомлення між LAC і LNS.
L2TP/ PPTP-сесія	У протоколах PPTP і L2TP визначене поняття сесії. LNS і LAC підтримують стан для кожного виклику, що ініційований LAC або на який відповів LAC. L2TP-сесія створюється між LAC і LNS, коли PPP-з'єднання встановлене між віддаленою системою й LNS. Дейтаграми, що відносяться до PPP-з'єднання, посилають по тунелі між LAC і LNS. Між установленими сесіями й відповідними викликами існує взаємооднозначна відповідність.
Керуюче з'єднання L2TP/PPTP	Керуюче з'єднання використовується для встановлення й підтримки як для сесій, так і самого L2TP/ PPTP- тунелю й створюється для кожної пари LAC, LNS. Керуюче з'єднання визначає всі характеристики тунелю й пов'язаних з ним сесій.

Протоколи канального рівня PPP (2)

Діаграма станів



Приклад LCP-запиту

Приклад запиту на автентифікацію

CHAP-автентифікація в протоколі PPP

```
16 13.430000  192.168.20.10   192.168.20.20   PPP LCP    68 Configuration Request
17 13.430000  192.168.20.20   192.168.20.10   L2TP       60 Control Message - ZLB      (tunnel i
18 13.430000  192.168.20.20   192.168.20.10   PPP LCP    73 Configuration Request
19 13.430000  192.168.20.10   192.168.20.20   PPP LCP    73 Configuration Ack

Frame 16: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
Ethernet II, Src: D-Link_49:dc:ff (5c:d9:98:49:dc:ff), Dst: D-Link_49:dd:03 (5c:d9:98:49:dd:03)
Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
User Datagram Protocol, Src Port: l2f (1701), Dst Port: l2f (1701)
Layer 2 Tunneling Protocol
Point-to-Point Protocol
    Address: 0xff
    Control: 0x03
    Protocol: Link Control Protocol (0xc021)
PPP Link Control Protocol
    Code: Configuration Request (0x01)
    Identifier: 0x00
    Length: 14
  Options: (10 bytes)
      Maximum Receive Unit: 1456
      Magic number: 0x9c933d03
```

```
17 13.430000  192.168.20.20   192.168.20.10   L2TP       60 Control Message - ZLB      (tunnel i
18 13.430000  192.168.20.20   192.168.20.10   PPP LCP    73 Configuration Request
19 13.430000  192.168.20.10   192.168.20.20   PPP LCP    73 Configuration Ack

Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: D-Link_49:dd:03 (5c:d9:98:49:dd:03), Dst: D-Link_49:dc:ff (5c:d9:98:49:dc:ff)
Internet Protocol Version 4, Src: 192.168.20.20 (192.168.20.20), Dst: 192.168.20.10 (192.168.20.10)
User Datagram Protocol, Src Port: l2f (1701), Dst Port: l2f (1701)
Layer 2 Tunneling Protocol
Point-to-Point Protocol
    Address: 0xff
    Control: 0x03
    Protocol: Link Control Protocol (0xc021)
PPP Link Control Protocol
    Code: Configuration Request (0x01)
    Identifier: 0x00
    Length: 19
  Options: (15 bytes)
      Maximum Receive Unit: 1456
    Authentication protocol: 5 bytes
      Authentication protocol: Challenge Handshake Authentication Protocol (0xc223)
      Algorithm: MS-CHAP-2 (0x81)
    Magic number: 0xb146249a
```

```
20 13.430000  192.168.20.20   192.168.20.10   PPP LCP    68 Configuration Ack
21 13.430000  192.168.20.20   192.168.20.10   PPP CHAP   75 Challenge (NAME='', VALUE=0x1ae39f3
22 13.430000  192.168.20.10   192.168.20.20   PPP CHAP   112 Response (NAME='olga', VALUE=0xfa29
23 13.430000  192.168.20.20   192.168.20.10   PPP CHAP   100 Success (MESSAGE='S=4AD4E6F6B4226AB
24 13.430000  192.168.20.10   192.168.20.20   PPP CCP    64 Configuration Request
25 13.430000  192.168.20.10   192.168.20.20   PPP IPCP   88 Configuration Request

Frame 21: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
Ethernet II, Src: D-Link_49:dd:03 (5c:d9:98:49:dd:03), Dst: D-Link_49:dc:ff (5c:d9:98:49:dc:ff)
Internet Protocol Version 4, Src: 192.168.20.20 (192.168.20.20), Dst: 192.168.20.10 (192.168.20.10)
User Datagram Protocol, Src Port: l2f (1701), Dst Port: l2f (1701)
Layer 2 Tunneling Protocol
Point-to-Point Protocol
    Address: 0xff
    Control: 0x03
    Protocol: Challenge Handshake Authentication Protocol (0xc223)
PPP Challenge Handshake Authentication Protocol
    Code: Challenge (1)
    Identifier: 147
    Length: 21
  Data
      Value Size: 16
      Value: 1ae39f3a13f606e057299a39e5451224
```

Захист канального рівня – протокол PPTP

PPTP (Point-to-Point Tunneling Protocol) і L2TP (Layer-2 Tunneling Protocol) є протоколами тунелювання канального рівня моделі OSI. Спільною особливістю цих протоколів є те, що вони використовуються для забезпечення безпечного, багатопротокольного віддаленого доступу до ресурсів корпоративної мережі через відкриту мережу, наприклад Інтернет.

Структура пакетів пересилання тунелю PPTP

Заголовок рамки трансмісії	ІП Заголовок	ГРЕ Заголовок	ДПП Заголовок	Зашифровані дані ДПП	Кінець рами трансмісії

Архітектура протоколу PPTP

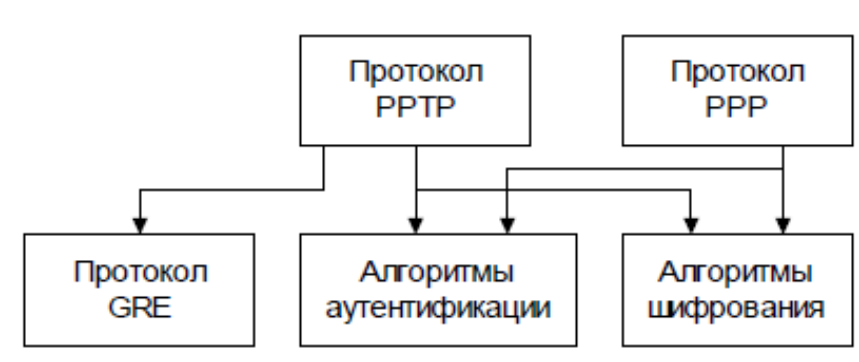


Схема тунелювання для прямого підключення віддаленого комп'ютера користувача до мережі Інтернет



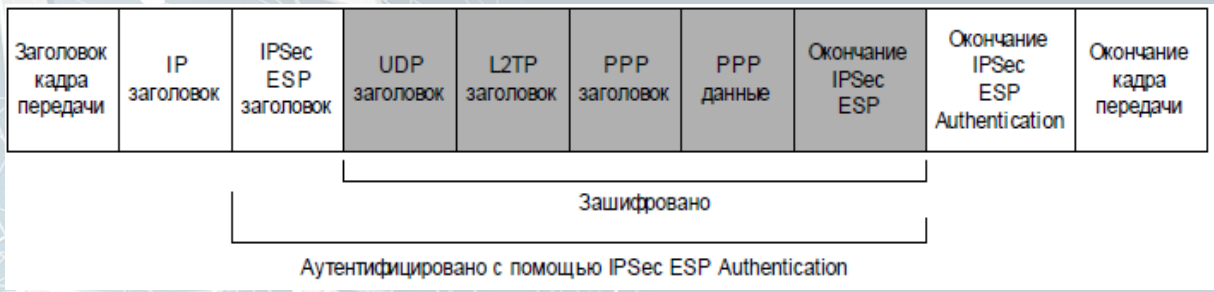
Захист канального рівня – протокол L2TP

Протокол L2TP був розроблений як протокол для безпечного тунелювання PPP-трафіку через мережі загального призначення з довільним середовищем.

На відміну від PPTR, L2TP не прив'язаний до IP, тому може використовуватися в мережах з комутацією пакетів, таких як ATM (Asynchronous Transfer Mode) або мережі Frame Relay. Крім того, в протокол L2TP додана важлива функція управління потоками даних.

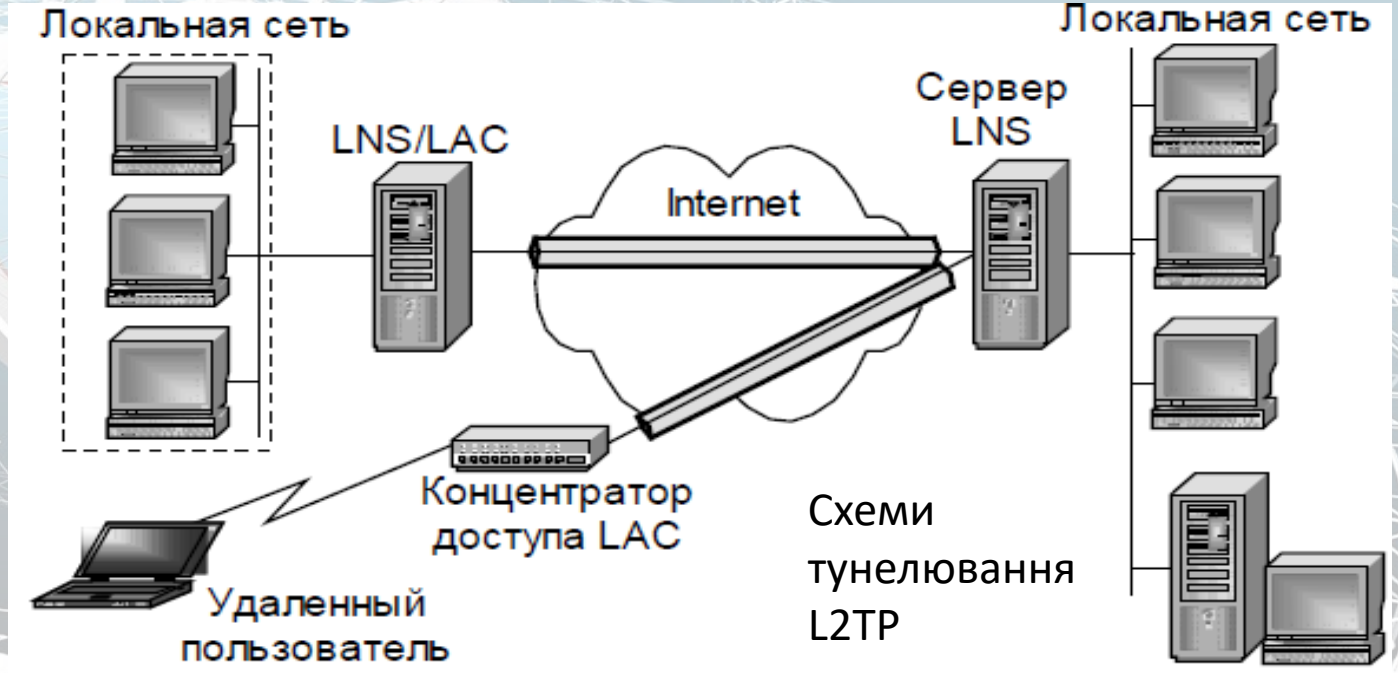
Протокол L2TP також додає ряд функцій безпеки, які не входять в специфікацію протоколу PPTP, зокрема, можливість роботи з протоколами AN і ESP стека протоколів IPSec. Архітектура протоколу L2TP показана на рис. праворуч

Структура пакетів для пересилання тунелів L2TP





Архітектура протоколу L2TP

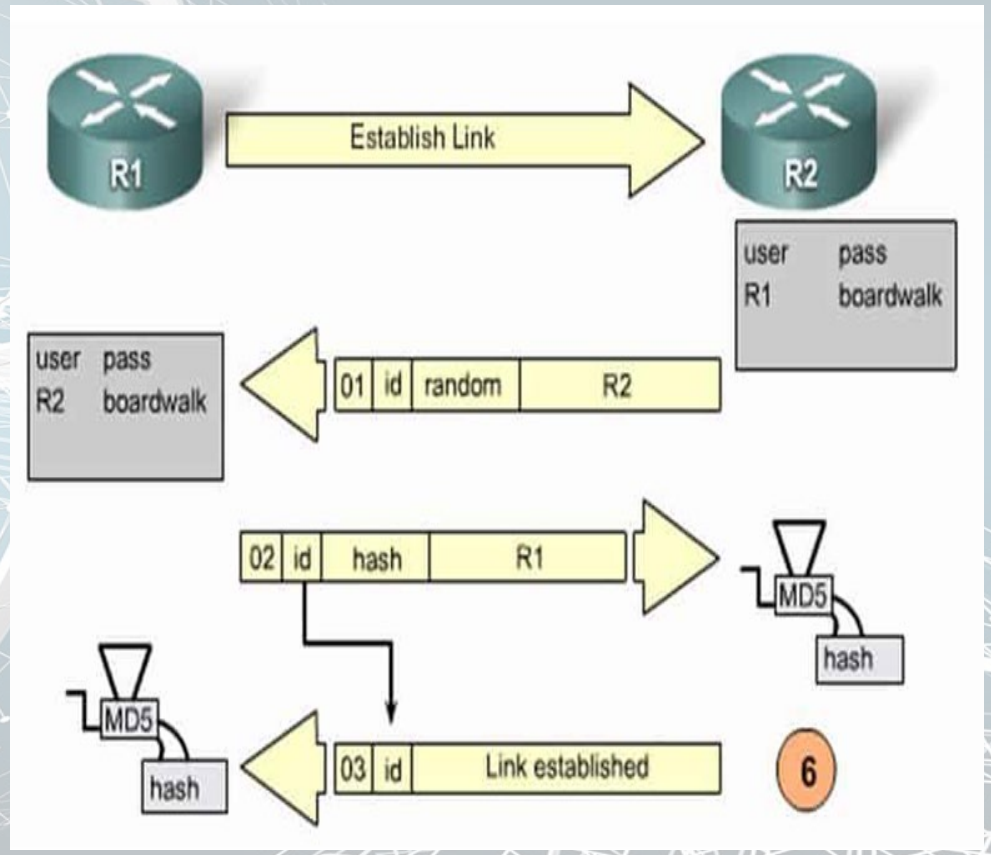


Схеми тунелювання L2TP

Протокол автентифікації Challenge-Handshake (CHAP)

Протокол CHAP використовується для періодичної перевірки автентифікації протилежної сторони за допомогою трикрокового рукостискання. Протокол виконується при початковому встановленні каналу й може повторюватися в будь-який час після того, як канал установлений.

1. Після завершення фази встановлення каналу та сторона, що запитує автентифікацію протилежної сторони, посилає їй повідомлення "challenge".
2. Протилежна сторона відповідає значенням, обчисленим за допомогою однобічної геш-функції.
3. Сторона, що запросила автентифікацію, порівнює відповідь із власним обчисленим значенням. Якщо значення збіглися, автентифікація вважається виконаною, у противному випадку з'єднання скидається.
4. Через довільні інтервали часу сторона, що запросила автентифікацію, надсилає новий запит протилежній стороні, і повторюються кроки 1 – 3.



Розширення Microsoft PPP CHAP версії 1

Microsoft розробив протокол MS-CHAP для автентифікації віддалених робочих станцій, що з однієї сторони мав би звичну для локальних користувачів функціональність, а з іншої сторони використовував би алгоритми шифрування й хешування.

MS-CHAP заснований на протоколі CHAP. Розходження між цими протоколами наступні:

- Пакет Response у протоколі MS-CHAP має формат, сумісний з Windows NT 3.5, 3.51 і 4.0. Формат MS-CHAP не вимагає, щоб автентифікатор зберігався в явному виді або у вигляді результату однобічного перетворення.
- MS-CHAP надає механізми запиту автентифікуючою стороною повторної автентифікації й зміни пароля.
- MS-CHAP визначена множина значень кодів, які вертаються клієнтові при невдалій автентифікації.

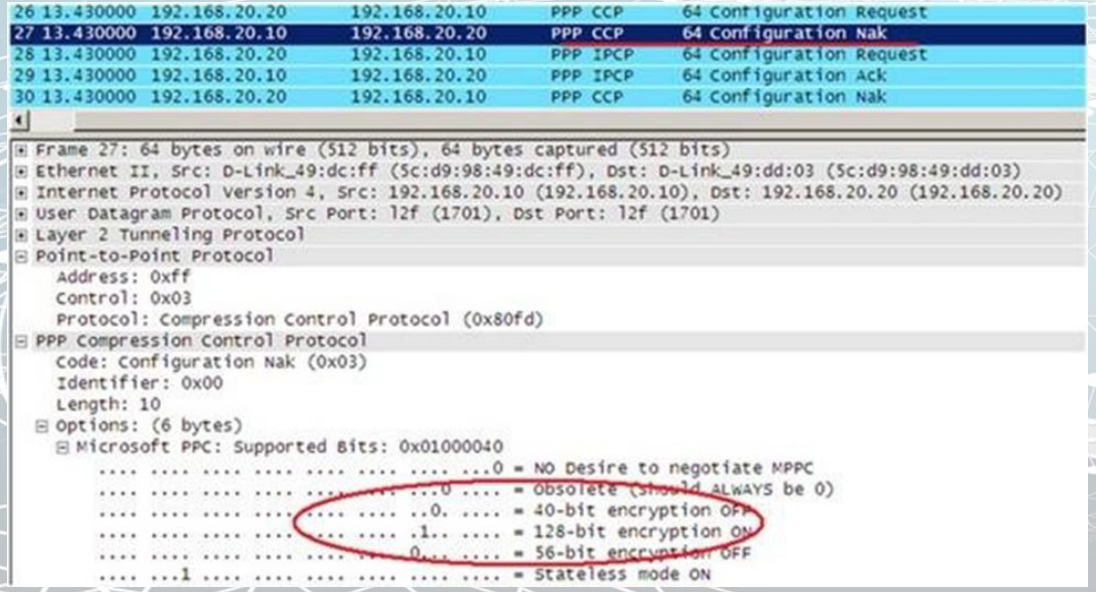
Розширення Microsoft PPP CHAP версії 2

Протокол MS-CHAP-V2 максимально відповідає як протоколу MS- CHAP-V1, так і стандартному протоколу CHAP. Розходження між протоколами MS-CHAP-V1 і MS-CHAP-V2 наступні:

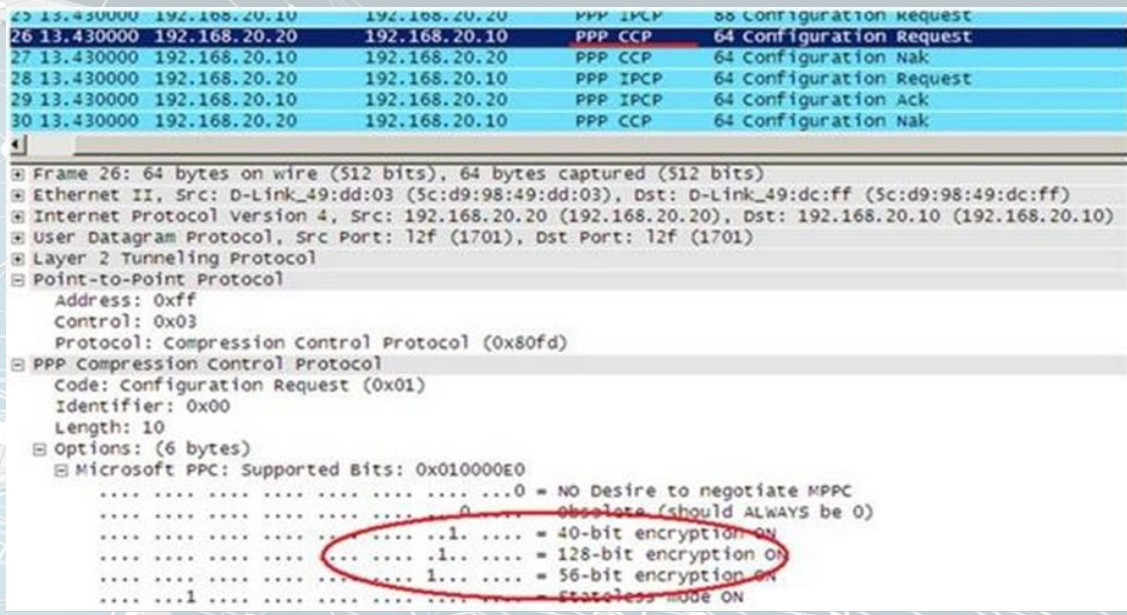
- Протокол MS-CHAP-V2 надає можливість вести перемовини про алгоритм при автентифікації в протоколі LCP.
- Протокол MS-CHAP-V2 забезпечує можливість взаємної автентифікації учасників, додаючи виклик у пакет Response, на який протилежна сторона відповідає в пакеті Success.
- Обчислення поля "Windows NT compatible challenge response" змінено в пакеті Response включенням виклику протилежної сторони й ім'ям користувача.
- В MS-CHAP-V1 поле "LAN Manager compatible challenge re- sponse" завжди посилало в пакеті Response. В MS-CHAP-V2 дане поле замінене на поле Peer-Challenge.
- Змінено формат поля Message у пакеті Failure.
- Пакети Change Password версій 1 і 2 більше не підтримуються. Вони замінені єдиним пакетом Change-Password.

Протокол шифрування MPPE Microsoft

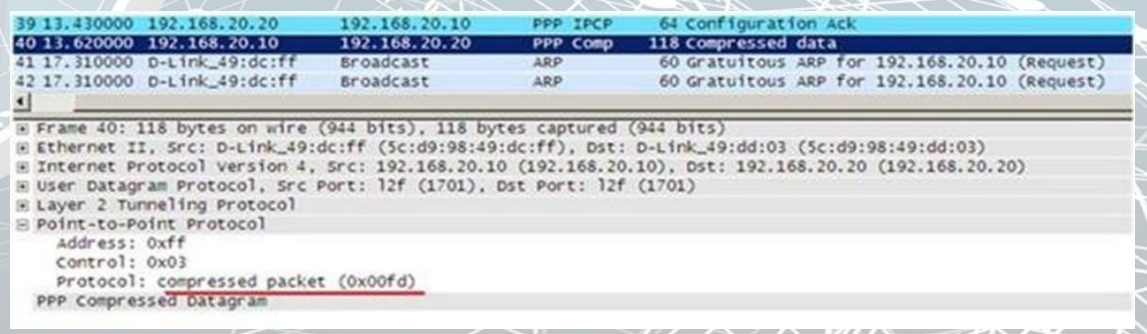
Протокол призначений для шифрування PPP-пакетів. У протоколі використовується потоковий алгоритм шифрування RC4. Про довжину ключа ведуться перемовини. MPPE (Microsoft Point-to-Point Encryption) підтримує 40-бітні, 56-бітні й 128-бітні ключі. Ключі сесії міняються часто, частота зміни ключів залежить від установлених опцій.



Перемовини про використовувану довжину ключа



Завершення переговорів про використовувану довжину ключа



Обмін зашифрованими дейтаграмами в протоколі PPP

Захист мережевого рівня – протокол конфігурування IPSec

Стек протоколів IPSec (Internet Protocol Security) використовується для аутентифікації учасників обміну, тунельного трафіку та шифрування IP-пакетів. Основним призначенням протоколу IPSec є забезпечення безпечної передачі даних по IP-мережах. Оскільки IPSec сумісний з IPv4, достатньо підтримувати його на обох кінцях з'єднання; Вузли мережі середнього рівня можуть взагалі нічого не «знати» про IPSec. Протокол IPs може захищати трафік як від поточної версії протоколу IPv4, що використовується сьогодні в Інтернеті, так і від версії IPv6, яка поступово впроваджується в Інтернет.

Ядро IPSec складають три протоколи:

- AH (Authentication Header – заголовок автентифікації) гарантує цілісність і автентичність даних;
- ESP (Encapsulating Security Payload – інкапсуляція зашифрованих даних) шифрує дані, що передаються, забезпечуючи конфіденційність, може також підтримувати автентифікацію і цілісність даних;
- IKE (Internet Key Exchange – обмін ключами Інтернету) вирішує допоміжну задачу автоматичного надання кінцевим точкам захищеного каналу секретних ключів, необхідних для роботи протоколів автентифікації і шифрування даних.

Розподіл функцій між протоколами IPSec

<table>
<tr><th>Виконувані функції</th><th colspan="2">Протокол</th></tr>
<tr><td>Забезпечення цілісності</td><td rowspan="3">AH</td><td rowspan="3">ESP</td></tr>
<tr><td>Забезпечення автентичності</td></tr>
<tr><td>Забезпечення конфіденційності</td></tr>
<tr><td>Розподіл секретних ключів</td><td colspan="2">IKE</td></tr>
</table>

Протокол IPSec

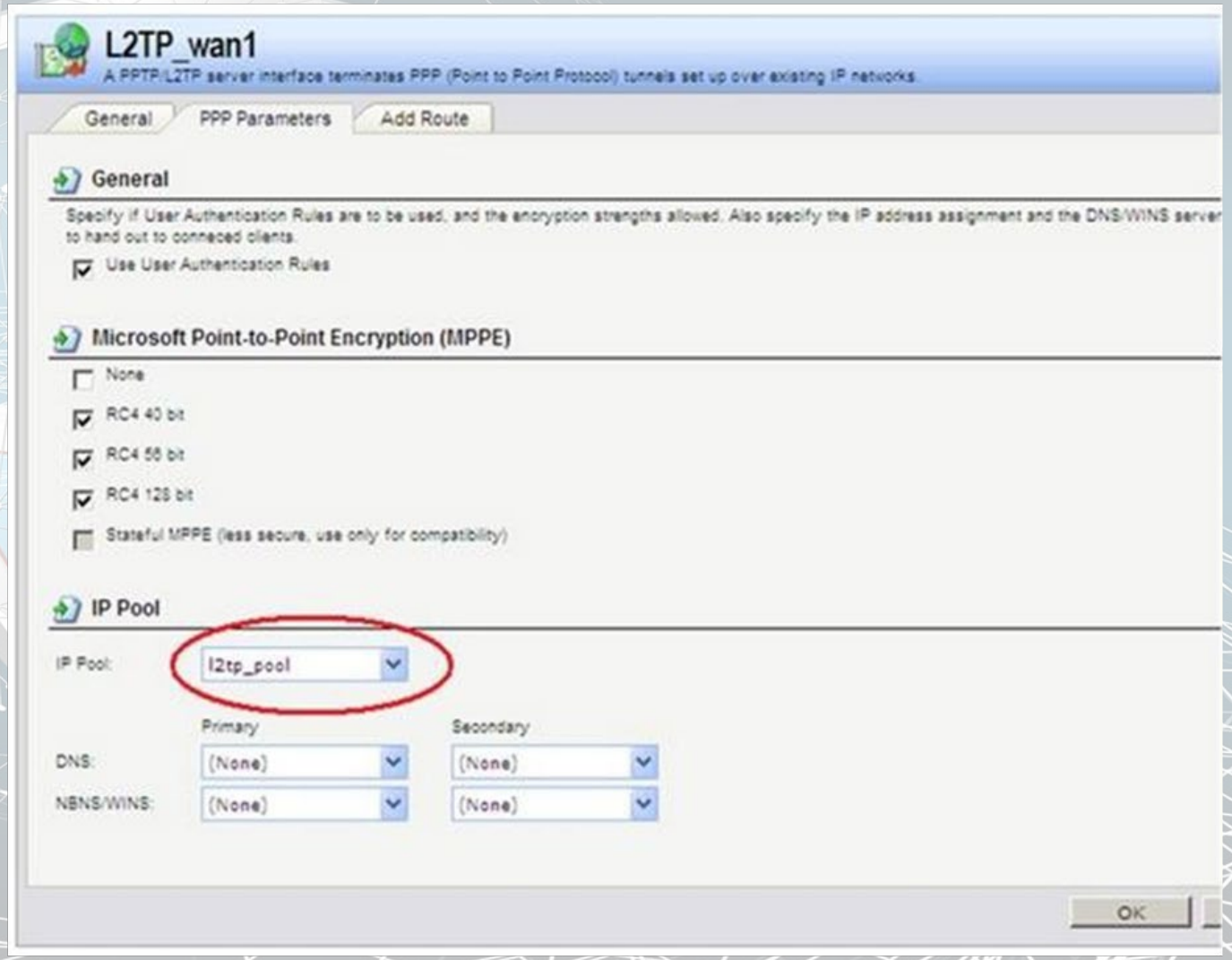
Поле протоколу даних канального рівня. Єдиний пакет інкапсульований в інформаційне поле PPP-даних канального рівня.

Поле кодів. Використовуються наступні коди:

- Configure-Request – запит конфігурації.
- Configure-Ack – підтвердження на запит конфігурації.
- Configure-Nak – негативне підтвердження.
- Configure-Reject – відхилення конфігурацію.
- Terminate-Request – завершення запиту.
- Terminate-Ack – підтвердження завершення.
- Code-Reject – код відхилення.

Конфігураційні опції IPCP дозволяють вести перемовини про необхідні параметри IP. IPCP використовує той же самий формат конфігураційних опцій, що й LCP.

- Протокол стискування IP. Даний параметр дозволяє домовитися про використання конкретного протоколу стискування. За замовчуванням стискування не потрібене.
- IP-адреса. Даний параметр надає спосіб ведення переговорів про IP-адресу, що буде призначена локальній стороні каналу. Він дозволяє відправникові Configure-Request вказати бажану IP-адресу або запросити протилежну сторону видати йому IP-адресу



Архітектура безпеки IPSec (1)

Основним призначенням протоколів IPSec є забезпечення безпечної передачі даних по IP-мережах. Використання IPSec гарантує:

- цілісність даних, що передаються, тобто дані при передачі не спотворюються, не втрачаються і не дублюються;
- автентичність відправника, тобто дані були передані відправником, який довів, що він є тим, за кого себе видає;
- конфіденційність переданих даних, тобто дані передаються у формі, що запобігає їх несанкціонованому перегляду.

Перелічимо основні завдання протоколів IPSec:

- Забезпечення криптографічного захисту на рівні IP для протоколів IPv4 і IPv6, а саме забезпечення конфіденційності й цілісності даних і цілісності деякої послідовності дейтаграм.
- Забезпечення прозорості для IP-трафіку, для якого не потрібне використання протоколів IPSec.
- Забезпечення розширюваності, тобто можливості додавати нові набори алгоритмів без зміни самого протоколу.

З метою забезпечення аутентифікації, конфіденційності та цілісності даних, що передаються, стек протоколів IPSec побудований на основі ряду стандартизованих криптографічних технологій:

- обмін ключами за алгоритмом Діффі-Хеллмана для розподілу секретних ключів серед користувачів у відкритій мережі;
- криптографія з відкритим ключем для підписання обмінів Діффі-Хеллмана для забезпечення автентичності двох сторін та уникнення атак типу "людина посередині";
- цифрові сертифікати для підтвердження автентичності відкритих ключів;
- блочні симетричні алгоритми шифрування даних;
- Алгоритми аутентифікації повідомлень на основі хешування.

Архітектура безпеки IPSec (2)

Основні завдання по створенню і підтримці захищеного каналу зв'язку полягають в наступному:

- аутентифікувати користувачів або комп'ютери під час ініціації захищеного каналу;
- шифрування та аутентифікація даних, що передаються між кінцевими точками захищеного каналу;
- Надання кінцевим точкам каналу секретних ключів, необхідних для роботи протоколів автентифікації та шифрування даних.

Більшість реалізацій IPSec мають такі компоненти:

- основний протокол IPSec. Цей компонент реалізує ESP і AH. Він обробляє заголовки, взаємодіє з базами даних SPD і SAD для визначення політики безпеки, що застосовується до пакета;
- Протокол управління обміном ключовою інформацією IKE (Internet Key Exchange). IKE зазвичай розглядається як процес на рівні користувача, за винятком реалізацій, вбудованих в операційну систему;
- База даних політик безпеки (SPD). Це один з найважливіших компонентів, оскільки він визначає політику безпеки, яка застосовується до пакета. SPD використовується основним протоколом IPSec при обробці вхідних і вихідних пакетів;
- База даних Асоціації безпеки (SAD). У базі даних SAD зберігається список захищених асоціацій SA (Security Association) для обробки вхідної та вихідної інформації. Вихідні SA використовуються для захисту вихідних пакетів, а вхідні SA використовуються для обробки пакетів із заголовками IPSec. База даних SA заповнюється SA вручну або за допомогою протоколу керування ключами IKE;
- управління політикою безпеки та безпечними асоціаціями CA. Це програми, які керують політикою безпеки і SA.

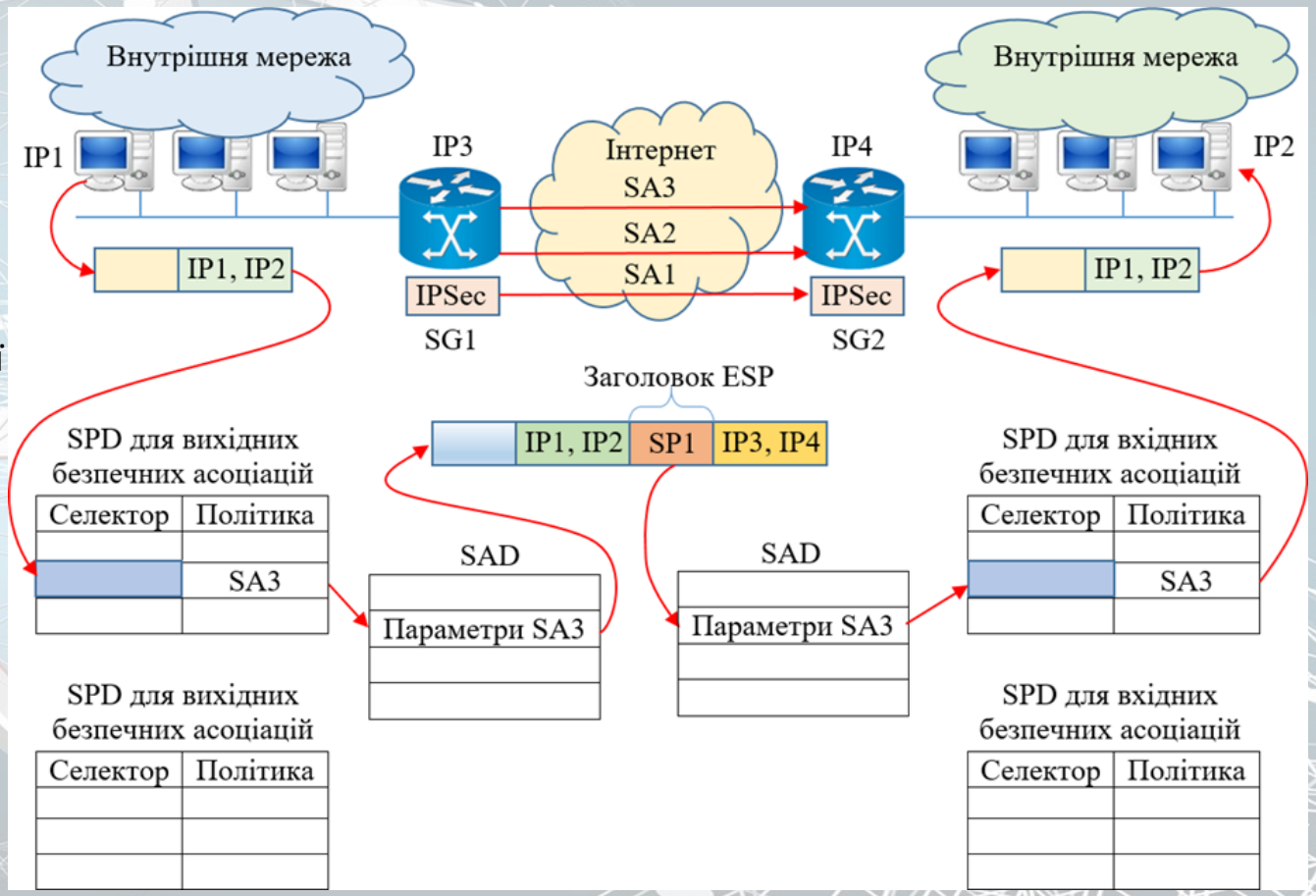
Архітектура безпеки IPSec (3)

Протокол IPSec, що працює на хості або на шлюзі, визначає метод захисту, який він повинен застосувати до трафіку, на основі двох типів баз даних, які підтримує IPSec в кожному вузлі:

- безпечних асоціацій (Security Associations Database, SAD);
- політики безпеки (Security Policy Database, SPD).

Селектор в SPD включає наступний набір ознак, на підставі яких можна з великим ступенем деталізації виділити захищений потік:

- IP-адреси відправника і отримувача можуть бути представлені як у вигляді окремих адрес (індивідуальних, групових або широкотрансляційних), так і діапазонами адрес, заданими за допомогою верхньої і нижньої меж або за допомогою маски;
- порти відправника і отримувача (тобто TCP- або UDP-порти);
- тип протоколу транспортного рівня (TCP, UDP);
- ім'я користувача в форматі DNS або X.500;
- ім'я системи (хоста, шлюзу безпеки і т. п.) в форматі DNS або X.500.



Використання баз даних SAD і SPD

Архітектура безпеки IPSec (4)

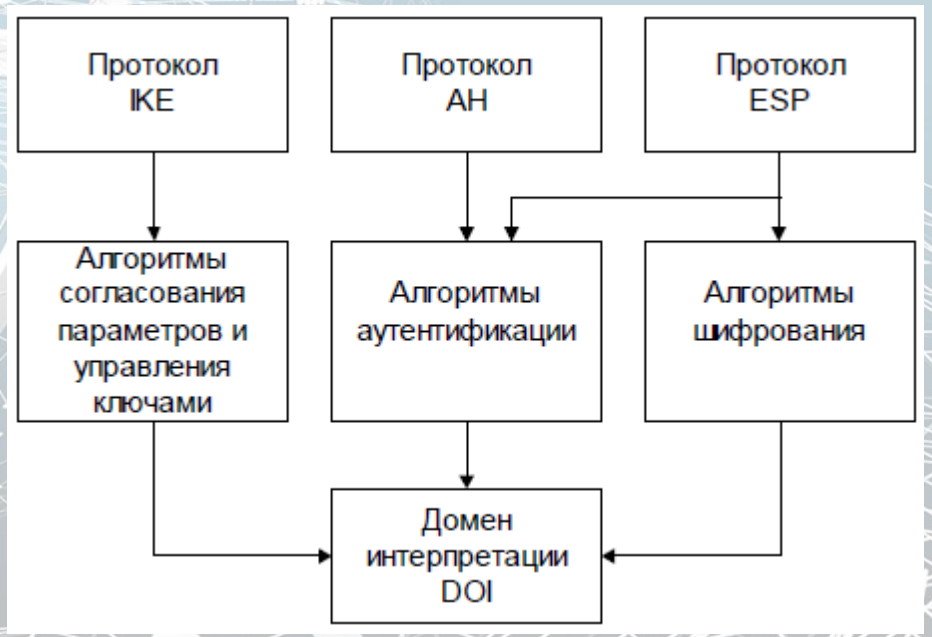
Всі протоколи, що входять в IPSec, можна розділити на дві групи:

- протоколи, які безпосередньо обробляють дані, що передаються (для забезпечення їх захисту);
- Протоколи, що дозволяють автоматично узгоджувати параметри безпечного з'єднання, необхідні для першої групи протоколів.

Ядро IPSec складається з трьох протоколів: протоколу Authentication Header (AH), протоколу Encapsulating Security Payload (ESP) і протоколу обміну ключами Інтернету (IKE) для узгодження параметрів віртуального каналу та керування ключами.

Архітектура засобів захисту IP представлена на рис.. На верхньому рівні розташовані такі протоколи:

- Протокол координації віртуальних каналів і керування ключами IKE, який визначає, як ініціалізується захищений канал, включаючи узгодження використовуваних алгоритмів шифрування, а також процедури обміну секретними ключами та керування ними в межах захищеного з'єднання.
- протокол аутентифікуючого заголовка AH, що забезпечує аутентифікацію джерела даних, перевірку їх цілісності та автентичності після прийому, а також захист від накладення повторних повідомлень;
- протокол інкапсуляційного захисту вмісту ESP, що забезпечує криптографічне закриття, аутентифікацію та цілісність даних, що передаються, а також захист від накладення повторних повідомлень.



Можливі способи реалізації IPSec

Існує кілька способів реалізації IPSec на хості або разом з маршрутизатором або міжмережним екраном (для створення шлюзу безпеки).

- Інтеграція IPSec у конкретну реалізацію протоколу IP. Це вимагає доступу до вихідного коду IP і робиться як на хостах, так і на шлюзах безпеки.
- "in-the-stack" (BITS) реалізації, коли IPSec реалізований "знизу" існуючої реалізації стека IP-протоколів, вбудовуючи свою реалізацію між стандартною реалізацією IP-протоколів і локальних мережних драйверів. Доступу до вихідного коду стека IP у цьому випадку не потрібно. Даний підхід звичайно реалізується на хостах, коли IPSec реалізований у вигляді бібліотеки, яка підключається.
- Використання зовнішнього криптопроцесору. Це називається "in- the-wire" (BITW) реалізацією. Такі реалізації можуть використовуватися як на хостах, так і на шлюзах. Звичайно BITW-пристрої є IP-адресуємими.

Протокол керування криптографічними ключами IKE

Для того, щоб протоколи AH і ESP могли виконувати свою роботу із захисту даних, що передаються, протокол IKE встановлює між двома кінцевими точками логічне з’єднання (рис.), яке в стандартах IPSec носить назву безпечної асоціації (Security Association, SA).

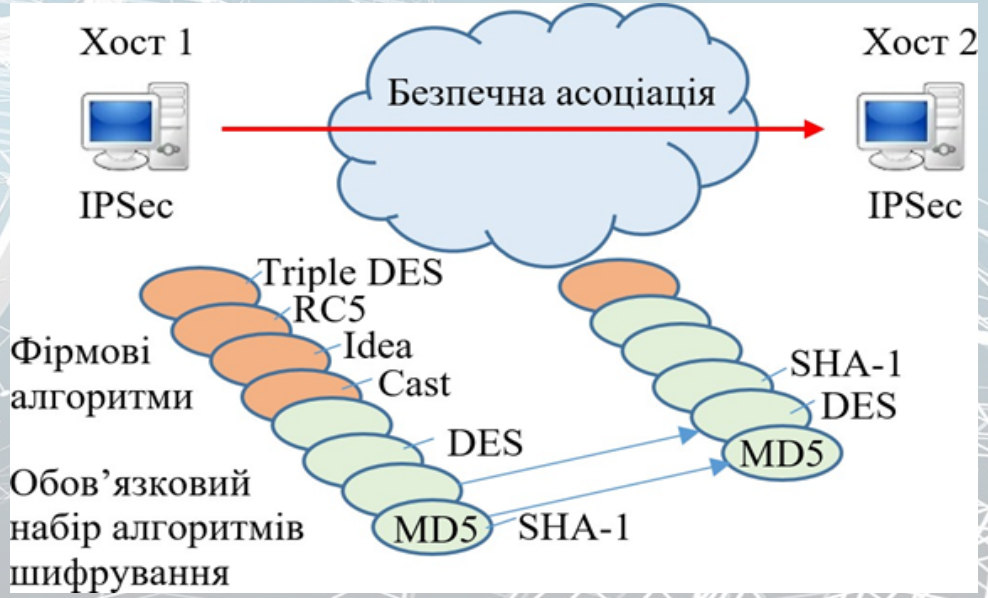
Протокол IPSec допускає як автоматичне, так і ручне встановлення безпечної асоціації. При ручному способі адміністратор конфігурує кінцеві вузли так, щоб вони підтримували узгоджені параметри асоціації, включаючи секретні ключі. При автоматичній процедурі встановлення SA протоколи IKE, що працюють по різні боки каналу, вибирають параметри в ході переговорного процесу. Для кожного завдання, що вирішуються протоколами AH і ESP, пропонується кілька схем автентифікації і шифрування (рис.)

Протоколи IKE виконують три функції:

- провести аутентифікацію взаємодіючих сторін, узгодити алгоритми шифрування та ключові характеристики для використання в захищеному сеансі обміну інформацією;
- забезпечувати створення та управління ключовою інформацією про з'єднання, безпосередній обмін ключами (включаючи можливість їх частої заміни);
- керувати параметрами з'єднання та захистом від певних типів атак, а також стежити за виконанням усіх досягнутих домовленостей.



. Безпечна асоціація



Узгодження параметрів в протоколі ESP

Протокол керування криптографічними ключами IKE

Політика безпеки передбачає три можливі варіанти обробки IP-пакета:

- Скидання пакетів
- Передача пакету без модифікації
- обробка за допомогою IPSec.

Криптографічні ключі, що використовуються в VPN, можна розділити на такі типи за тривалістю використання:

- базові ключі, які застосовуються протягом відносно тривалого періоду часу (від тижня до декількох місяців);
- тимчасові ключі, кожен з яких генерується для шифрування інформації в межах одного захищеного каналу.

Існує два основних способи побудови безпечного віртуального тунелю між двома вузлами в комп'ютерній мережі:

- Формування захищеного каналу для кожного з'єднання, встановленого програмним додатком;
- формування загального захищеного каналу між вузлами мережі і створення окремих захищених з'єднань в рамках цього каналу.

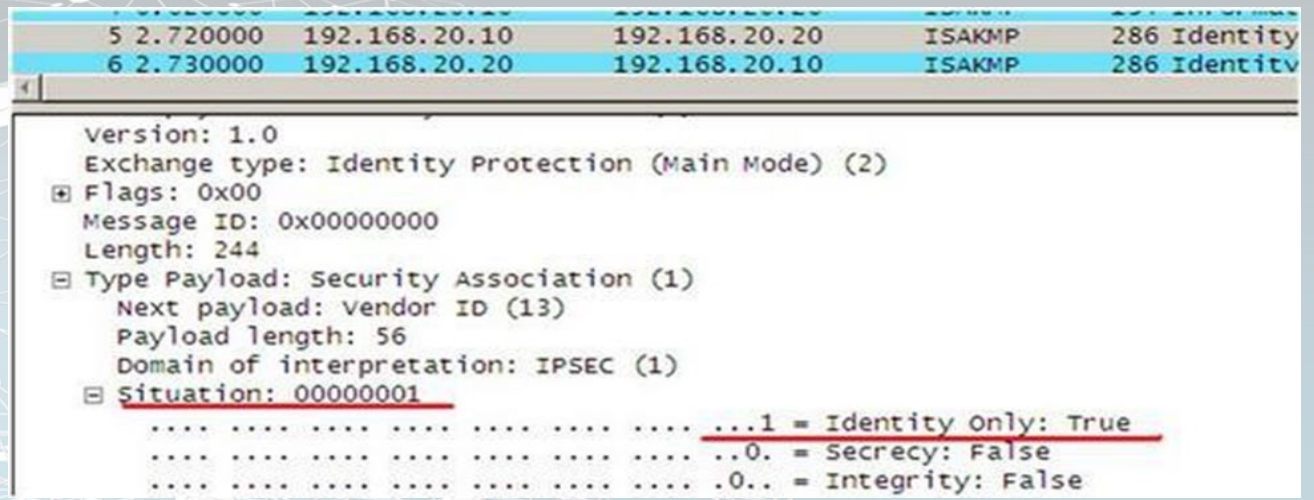
Формування захищеного віртуального каналу для кожного з'єднання включає в себе наступні етапи:

- видача запиту одній зі сторін і досягнення домовленості про створення захищеного віртуального каналу;
- Аутентифікація сторін за допомогою раніше розподілених майстер-ключів шифрування або призначених паролів.
- Розподіл тимчасових ключів і узгодження параметрів захищеного каналу.

Домен IPSec

При описі домену визначаються наступні поняття:

- Схема іменування ідентифікаторів протоколів.
- Можливість визначення умови виконання протоколів і загальні вимоги до політики безпеки на кінцевих точках.
- Синтаксис атрибутів SA.
- Синтаксис умісту повідомлень.
- Можливі типи обміну ключа.
- Можливі типи повідомлень (Notification).

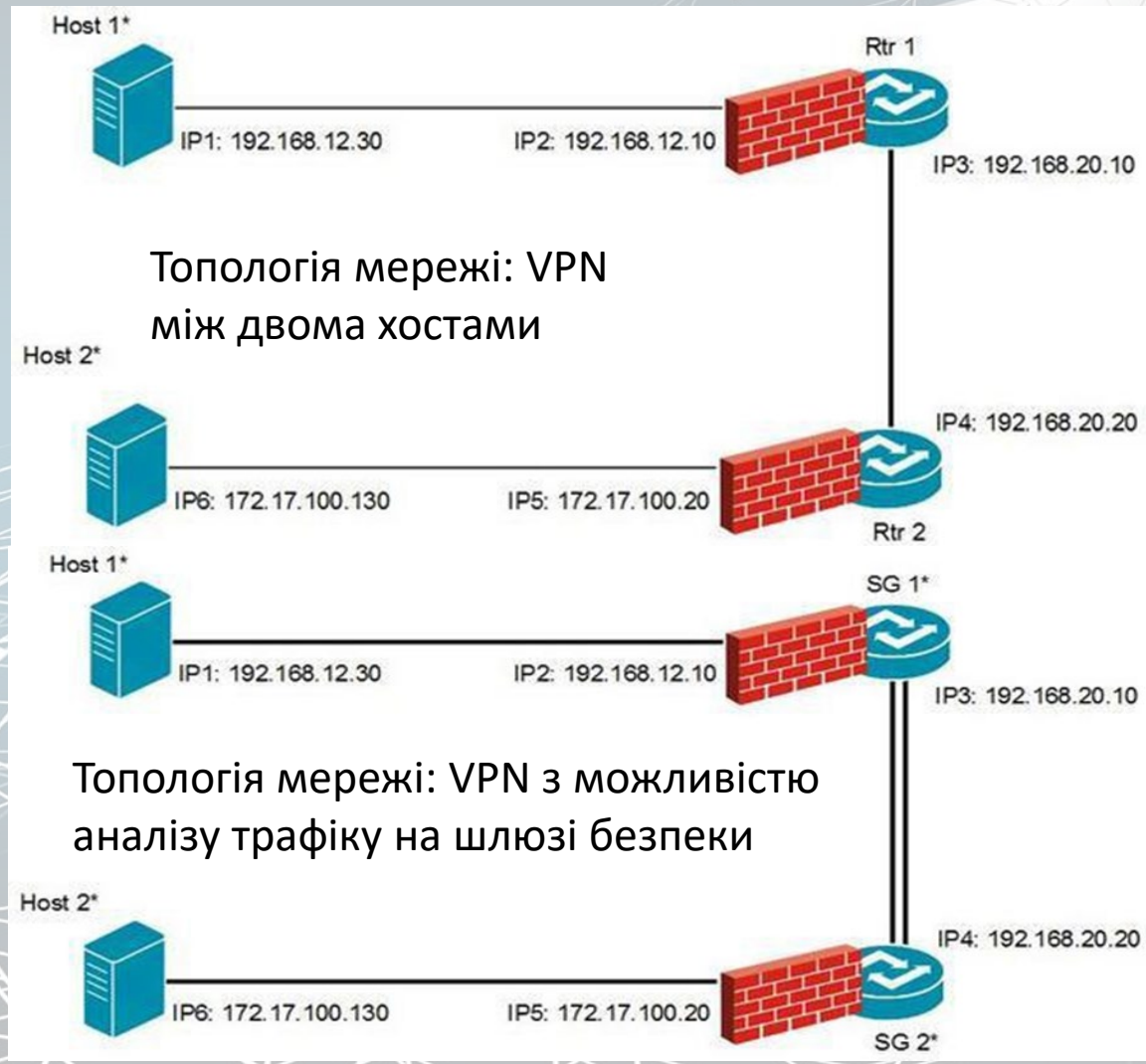


У заголовку повідомлень існує поле Situation, у якому втримується інформація, на основі якої Одержувач може зробити вивід про вимоги політики по обробки вхідного трафіку SA. Для IPSec-домену DOI визначені наступні значення:

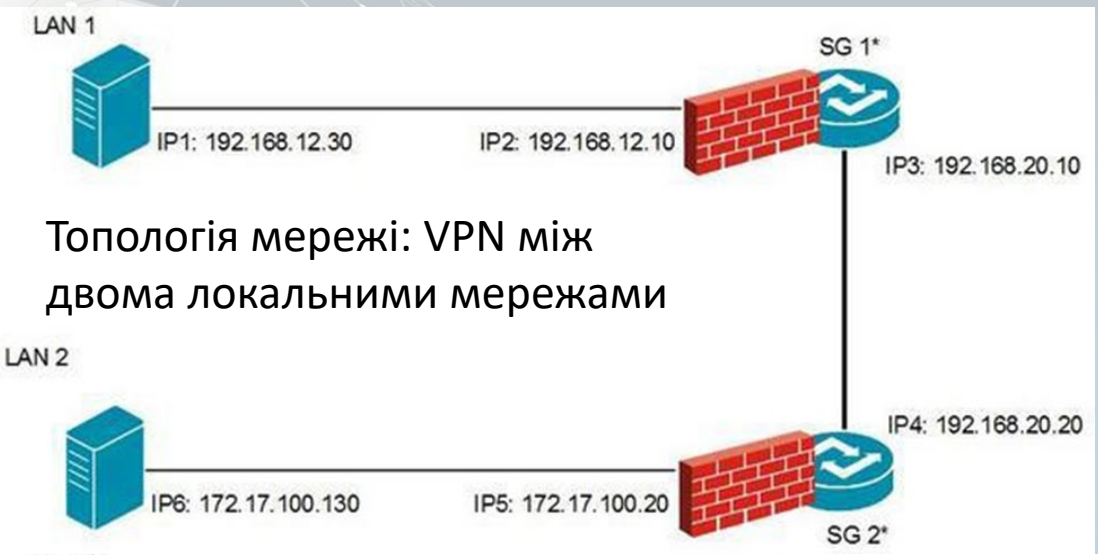
Умова	Значення
SIT_IDENTITY_ONLY	0x01
SIT_SECRECY	0x02
SIT_INTEGRETY	0x04

- Умова SIT_IDENTITY_ONLY вказує, що безпечна асоціація визначається ідентифікаційною інформацією джерела, що перебуває у вмісті SA.
- Умова SIT_SECRECY вказує, що SA встановлюється в оточенні, в якому потрібний захист.
- Умова SIT_INTEGRETY вказує, що SA встановлюється в оточенні, у якому потрібне забезпечення цілісності.

Можливі топології IPSec



Топологія мережі: VPN між двома хостами



Топологія мережі: VPN між двома локальними мережами

Топологія мережі: VPN з можливістю аналізу трафіку на шлюзі безпеки



Топологія мережі: захищений доступ користувача в локальну мережу

Специфіка впровадження інструментів IPSec

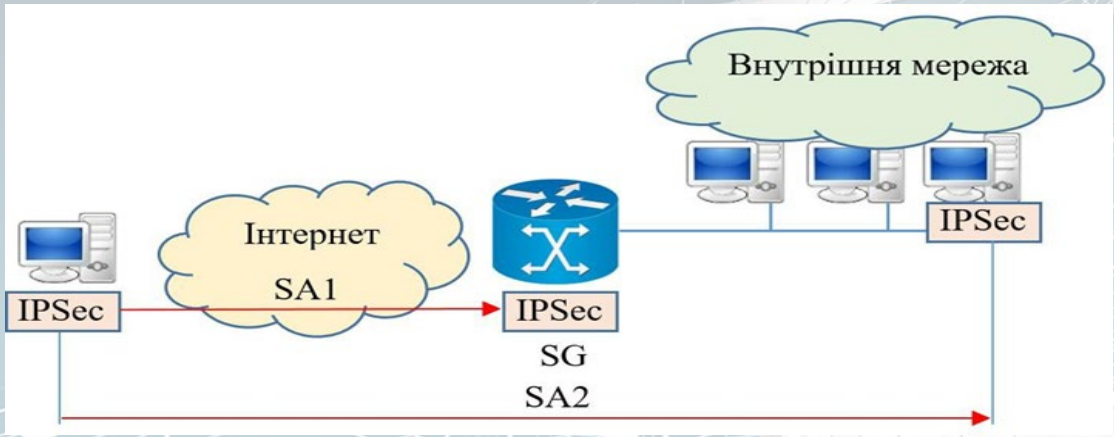
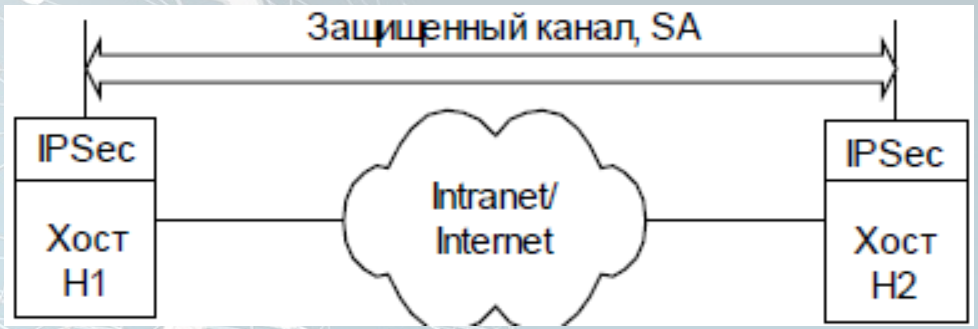


Схема захищеного каналу хост-шлюз



Діаграма хост-хост

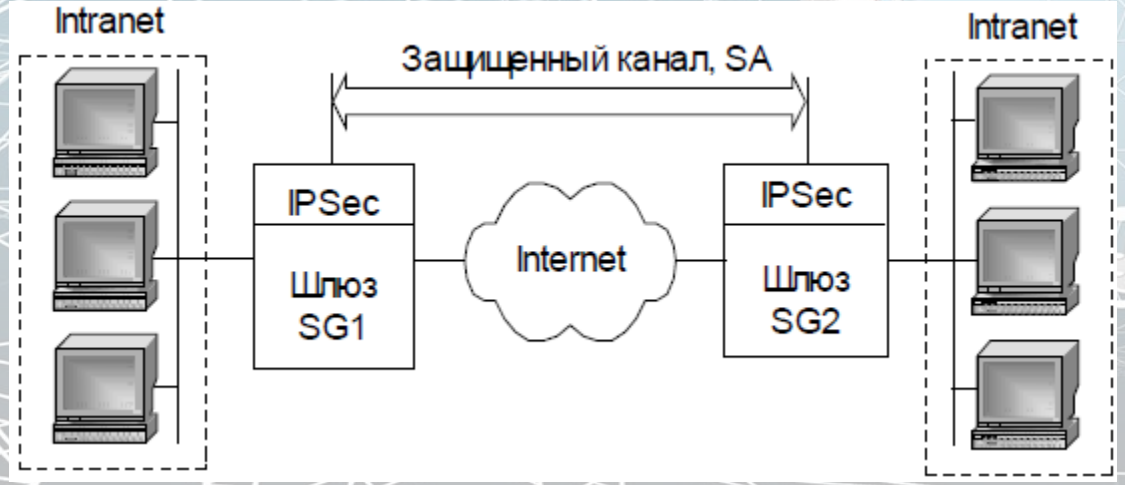
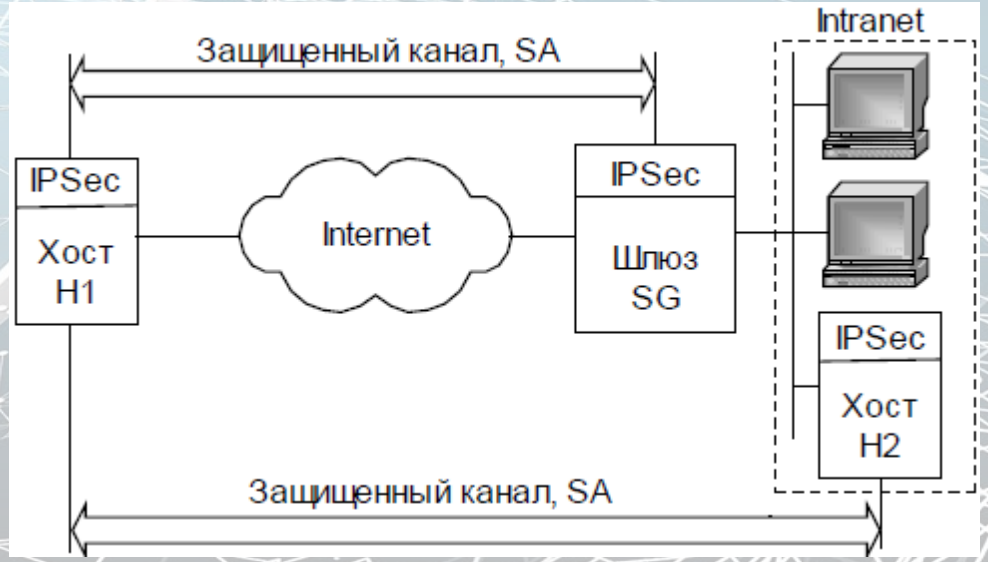


Схема шлюз-шлюз



Діаграма хост-шлюз, доповнена каналом хост-хост

Протокол заголовка аутентифікації AH

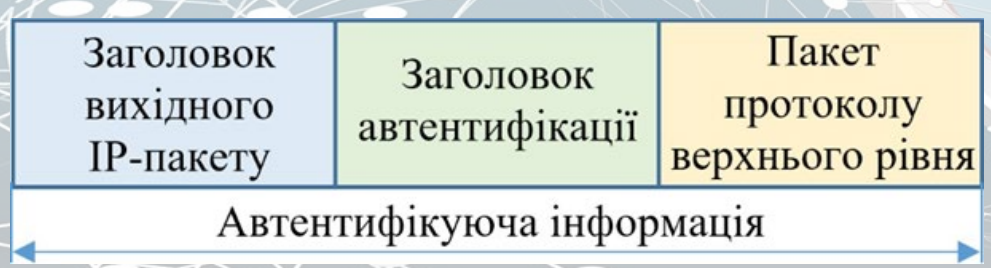
Протокол аутентифікуючого заголовка AH і протокол захисту інкапсуляційного контенту ESP можуть працювати в режимі тунелю або транспортування. Для виконання своїх завдань щодо забезпечення безпечної передачі даних протоколи AH і ESP включають в оброблювані ними пакети додаткову службову інформацію, форматуючи її у вигляді заголовків. Нижче ми детально розглянемо вміст заголовків AH та ESP та пов'язаний з ними функціонал.

Протокол AH дозволяє приймаючій стороні переконатися, що:

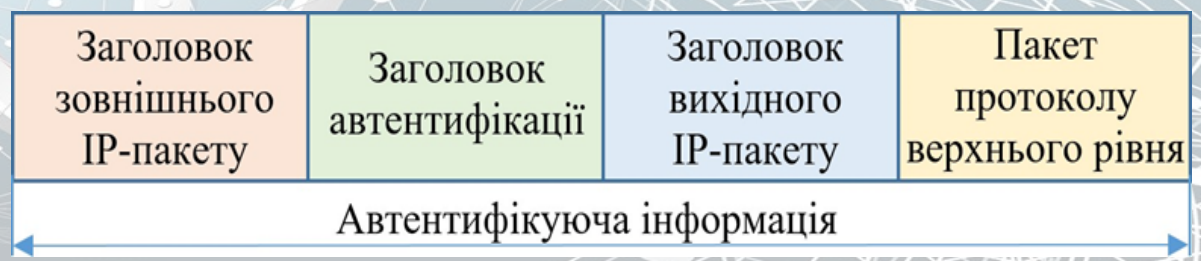
- пакет був відправлений стороною, з якою встановлена безпечна асоціація;
- вміст пакета не було спотворено в процесі його передачі по мережі;
- пакет не є дублікатом вже отриманого пакета.



Структура заголовку протоколу AH



Структура IP-пакету, обробленого протоколом AH в ранспортному режимі

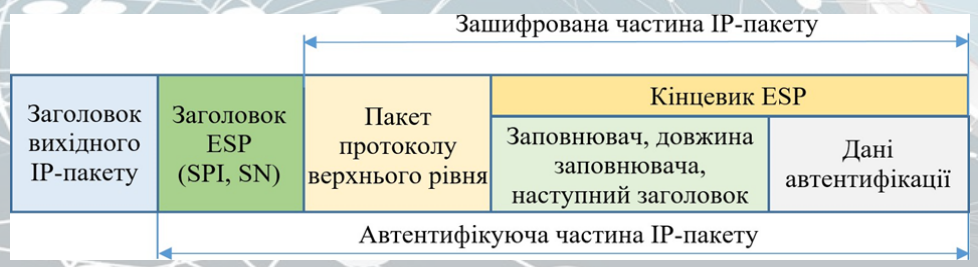


Структура IP-пакету, обробленого протоколом AH в тунельному режимі

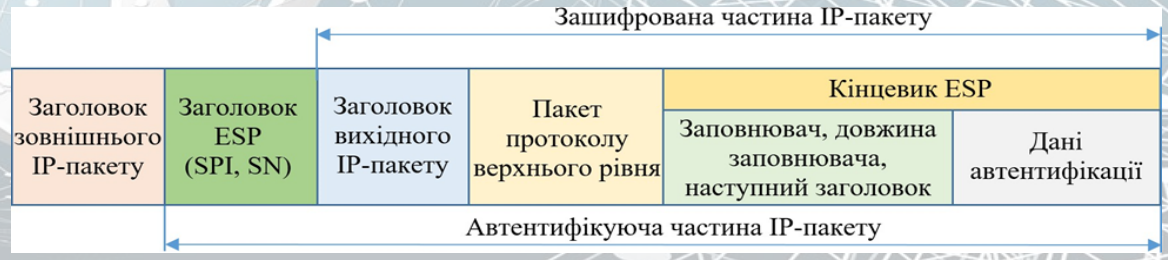
Протокол захисту від інкапсуляції ESP

Заголовок ESP містить наступні поля:

- Індекс параметрів безпеки (SPI) — використовується разом з адресою одержувача та протоколом безпеки (AH або ESP). Вказує відповідну CA. Одержувач використовує це значення для визначення угоди про захист, з якою ідентифікується посилка;
- Порядковий номер SN (порядковий номер) — забезпечує захист від повторення для SA. Це 32-розрядне число, спочатку рівне 1 і збільшується з кроком в 1. Він не повторюється циклічно і вказує номер пакета, що відправляється за цим договором. Одержувач перевіряє це поле, щоб переконатися, що пакет з цим номером ще не прийнятий. Якщо такий пакет вже існував, він не приймається;
- дані про корисне навантаження;
- Placeholder (Padding) – додається від 0 до 255 байт для 32-бітного вирівнювання з розміром блоку шифру;
- Довжина доповнення: визначає довжину поля заповнювача в байтах.
- Next Header – вказує на характер даних, що передаються (наприклад, TCP або UDP);
- Дані автентифікації – містять код цілісності ICV та код автентифікації повідомлення, які використовуються для перевірки автентичності відправника та цілісності повідомлення. Значення ICV обчислюється для заголовка ESP, даних, що передаються, і кінцевої мітки ESP. Поле Autthentication Data розміщується в заголовку ESP тільки при включеній аутентифікації.



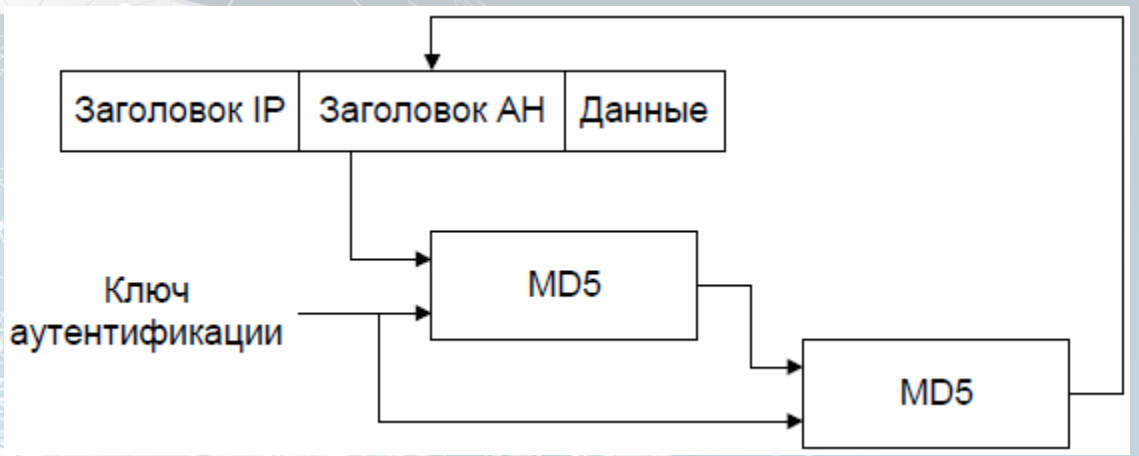
Структура IP-пакету, обробленого протоколом ESP в транспортному режимі



Структура IP-пакету, обробленого протоколом ESP в тунельному режимі

Алгоритми аутентифікації та шифрування в IPSec

Принцип роботи алгоритму HMAC полягає в подвійній обробці пакета хеш-функцією, керованою ключем аутентифікації (наприклад, хеш-функцією MD5).



Алгоритми шифрування визначаються при створенні SA і застосовуються для шифрування даних, переданих по SA. У протоколі ESP використовуються симетричні алгоритми шифрування.

Алгоритм автентифікації, використовуваний для обчислення Integrity Check Value (ICV), визначається при створенні SA. Для обчислень точка-точка відповідні алгоритми автентифікації використовують MAC із ключем, заснованим на симетричних алгоритмах шифрування (наприклад, DES) або на однобічних геш-функціях (наприклад, MD5 або SHA-1).

Обробка вихідного пакета IPSec

1. Пошук підходящої SA. ESP застосовується до вихідного пакета після того, як визначено, який SA належить пакет

2. Шифрування пакета. Відправник виконує наступні дії:
   - Інкапсуляція в поле ESP Payload:
   - Для транспортного режиму – тільки вихідна інформація протоколу верхнього рівня.
   - Для тунельного режиму – вся вихідна IP-дейтаграма.
   - Додавання необхідного доповнення (поле Padding).
   - Шифрування отриманих даних (Payload Data, Padding, Pad Length, Next Header), використовуючи ключ, алгоритм шифрування, режим алгоритму, зазначені в SA.

3. Обчислення Sequence Number. Перший пакет, що посилається по заново створеної SA, має Sequence Number, рівний 1.

4. Обчислення значення перевірки цілісності

- 5. Фрагментація. Після описаних вище ESP-перетворень при необхідності може виконуватися фрагментація пакета

Протокол SSL/TLS (1)

SSL (англ. Secure Sockets Layer – рівень захищених сокетів) – криптографічний протокол, що має на увазі більш безпечний зв'язок, який забезпечує встановлення безпечного з’єднання між клієнтом і сервером.

Протокол широко використовувався для обміну миттєвими повідомленнями й передачі голосу через IP (англ. Voice over IP – VoIP), у таких додатках, як електронна пошта, Інтернет-Факс та інше. У цей час відомо, що протокол не є безпечним. На підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що одержав ім'я TLS. SSL повинен бути виключений з роботи на користь TLS.

TLS (англ. Transport Layer Security) – безпека транспортного рівня, як і його попередник SSL (англ. Secure Sockets Layer – рівень захищених сокетів) – криптографічні протоколи, що забезпечують захищену передачу даних між вузлами в мережі Інтернет. TLS і SSL використовують:

- асиметричну криптографію для автентифікації;
- симетричне шифрування для конфіденційності;
- коди автентичності повідомлень для збереження цілісності повідомлень.

Протокол SSL/TLS (2)

SSL включає три основні фази:

1. Діалог між сторонами, метою якого є вибір алгоритму шифрування.

2. Обмін ключами на основі криптосистем з відкритим ключем або автентифікація на основі сертифікатів.

3. Передача даних, зашифрованих за допомогою симетричних алгоритмів шифрування.

Перелічимо завдання протоколу SSL/TLS у порядку їхнього пріоритету:

1. Криптографічна безпека: SSL/TLS повинен використовуватися для встановлення криптографічно безпечного з'єднання між двома учасниками.

2. Інтероперабельність: незалежні розроблювачі повинні мати можливість створювати додатки, які будуть взаємодіяти за протоколом SSL/TLS, що дозволить установлювати безпечні з'єднання.

3. Розширюваність: SSL/TLS визначає загальний каркас, у який можуть бути вбудовані нові алгоритми відкритого ключа й симетричного шифрування.

4. Відносна ефективність: криптографічні операції інтенсивно використовують ЦП, особливо операції з відкритим ключем.

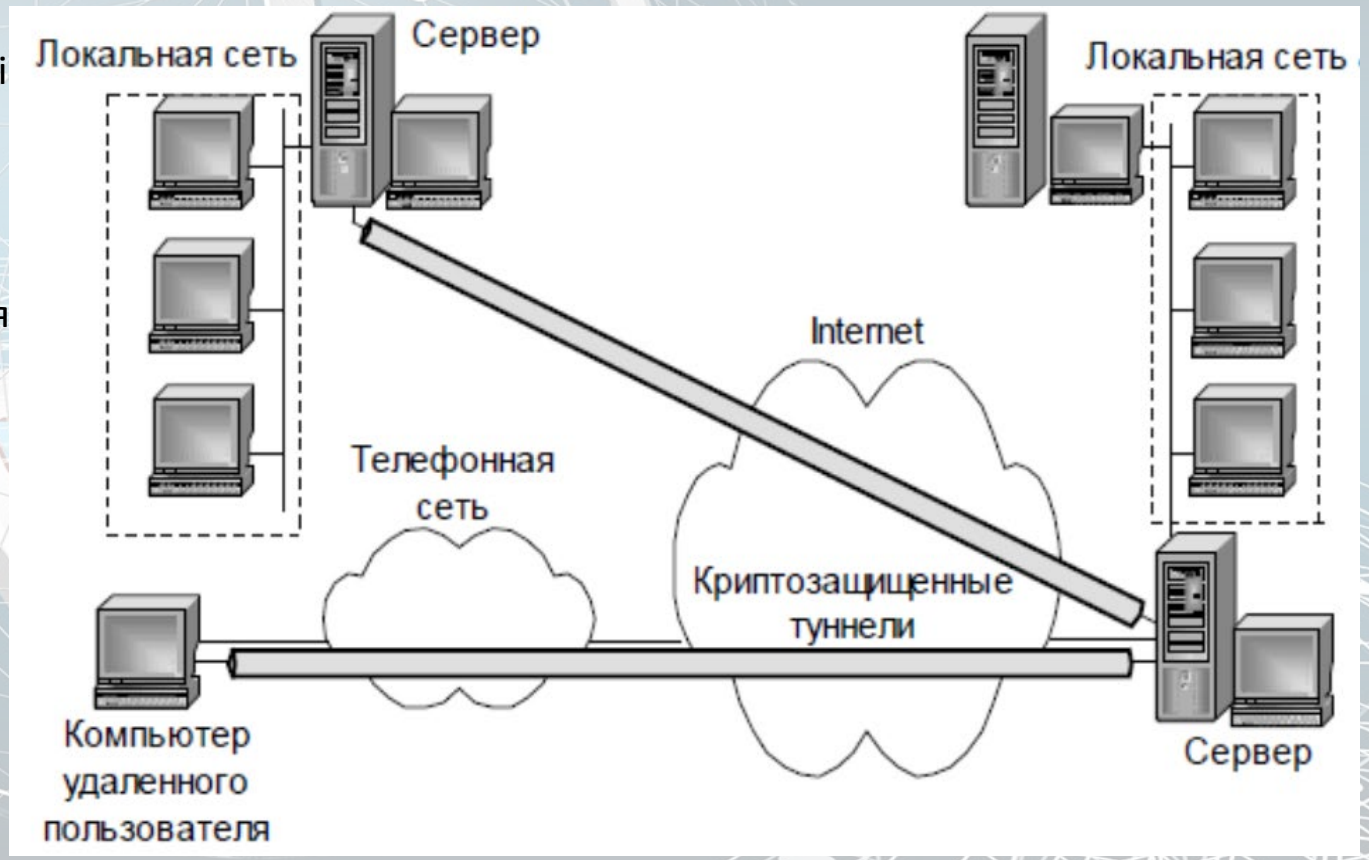
- Конфіденційність з'єднання.
- Цілісність з'єднання.

Протокол SSL/TLS (3)

- Протокол SSL передбачає наступні етапи взаємодії клієнта і сервера при формуванні і підтримці захищеного з'єднання:
- встановлення SSL-сесії;
- Безпечний зв'язок.

У процесі налагодження SSL-сесії вирішуються такі задачі:

- автентичність сторін;
- узгодження криптографічних алгоритмів та алгоритмів стиснення, які будуть використовуватися у захищеному обміні інформацією;
- формування загальної секретної відмички;
- генерація загальних секретних сеансових ключів на основі згенерованого майстер-ключа для шифрування обміну інформацією.



Криптографічно захищені тунелі, сформовані на основі протоколу SSL

Автентифікація сторін

Цифрові сертифікати в основному служать двом цілям:

- встановити особу власника;
- зробити доступним первинний ключ власника.

Є три способи отримати SSL-сертифікат:

1. Використовувати сертифікат від Центру сертифікації;
2. Використовувати самопідписаний сертифікат;
3. Використовувати «порожній» сертифікат

Центри сертифікації (CA) – це організації, яким довіряє уся галузь і які займаються видачою Інтернет-сертифікатів.

Самопідписаний сертифікат – це сертифікат, створений самим користувачем.

В загальному, «порожні» сертифікати містять фіктивну інформацію, яку використовують як тимчасове рішення для налаштування SSL і перевірки його функціонування в конкретному середовищі.

Процедура рукостискання

Під час рукостискання клієнт і сервер домовляються про різні параметри, які будуть використані, щоб забезпечити безпеку з’єднання.

- 1. Рукостискання починається тоді, коли клієнт підключається до SSL сервера. Клієнт надсилає серверу номер версії SSL клієнта, підтримувані ним алгоритми шифрування і хеш-функції, специфічні дані для сеансу і іншу інформацію, яка потрібна серверу, щоб спілкуватися з клієнтом, використовуючи SSL.
- 2. Сервер надсилає клієнту номер версії SSL сервера, алгоритми стиснення і шифрування, хеш-функцію (вибрані з надісланих раніше клієнтом), специфічні дані для сеансу і іншу інформацію, яка потрібна серверу, щоб спілкуватися з клієнтом по протоколу SSL. Сервер також надсилає свій сертифікат, який вимагає перевірки автентичності клієнта. Після ідентифікації сервер запитує сертифікат клієнта.
- 3. Клієнт використовує інформацію, передану сервером для перевірки автентичності. Якщо сервер не може бути перевірений, користувач отримує попередження про проблему і про те, що шифрування і автентифікація з’єднання не може бути встановлена. Якщо сервер успішно пройшов перевірку, то клієнт переходить до наступного кроку.
- 4. Використовуючи всі дані, отримані до сих пір від процедури рукостискання, клієнт (у співпраці з сервером) створює попередній секрет сесії, в залежності від використовуваного шифру від сервера, шифрує його з допомогою відкритого ключа сервера (отриманого з сертифіката сервера, відправленого на 2-му кроці), а потім відправляє його на сервер.
- 5. Якщо сервер запросив автентифікацію клієнта (необов’язковий крок рукостискання), клієнт також підписує ще один фрагмент даних, який є унікальним для цього рукостискання і відомий як для клієнта, так і сервера. У цьому випадку, клієнт відправляє всі підписані дані і власний сертифікат клієнта на сервер разом з попередньо зашифрованих секретом.
- 6. Сервер намагається автентифікувати клієнта. Якщо клієнт не може пройти перевірку автентичності, сеанс закінчується. Якщо клієнт може бути успішно автентифікований, сервер використовує свій закритий ключ для розшифровки попереднього секрету, а потім виконує ряд кроків (які клієнт також виконує), щоб створити головний секрет.
- 7. І клієнт, і сервер використовують секрет для генерації ключів сеансів, які є симетричними ключами, що використовуються для шифрування і розшифрування інформації, якою обмінюються під час SSL сесії. Відбувається перевірка цілісності (тобто, для виявлення будь-яких змін в даних між часом коли він був надісланий, і часом його отримання на SSL-з’єднанні).
- 8. Клієнт надсилає повідомлення серверу, інформуючи його, що майбутні повідомлення від клієнта будуть зашифровані за допомогою ключа сеансу. Потім він відправляє окреме, зашифроване повідомлення про те, що частина рукостискання закінчена.
- 9. І на закінчення, сервер надсилає повідомлення клієнту, інформуючи його, що майбутні повідомлення від сервера будуть зашифровані за допомогою ключа сеансу. Потім він відправляє окреме, зашифроване повідомлення про те, що частина рукостискання закінчена.

Встановлення SSL-сесії

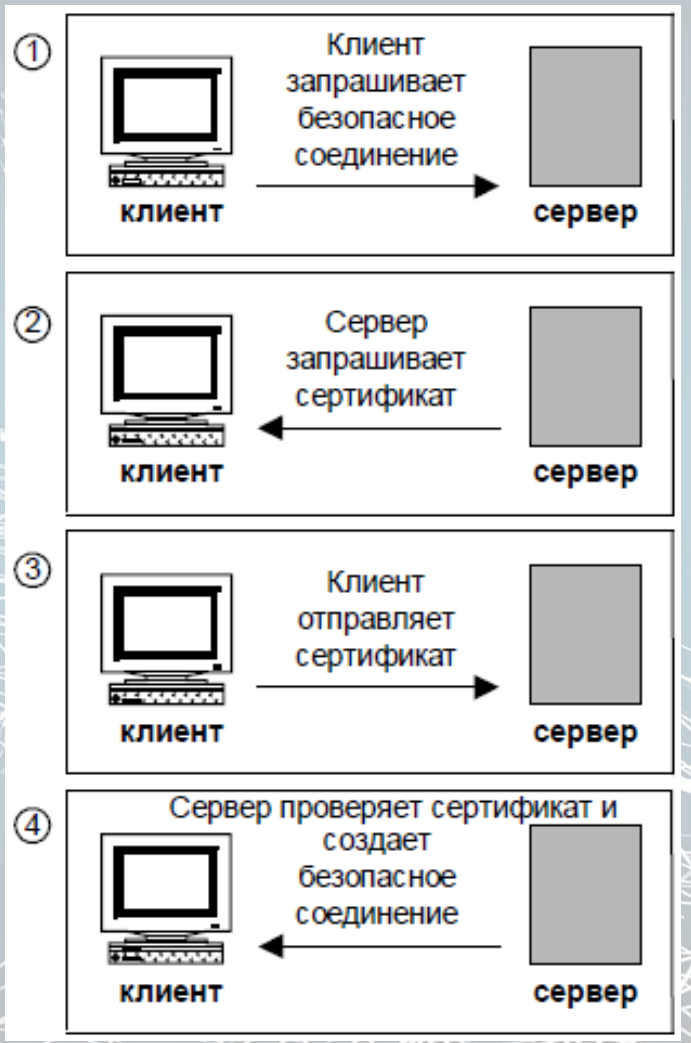
В процесі встановлення SSL-сесії вирішуються наступні завдання:

- автентифікація сторін;
- формування загального секретного майстер-ключа;
- генерація на основі сформованого майстер-ключа загальних секретних сеансових ключів для криптозахисту інформаційного обміну.

SSL забезпечує два типи аутентифікації:

- аутентифікація сервера клієнтом;
- Аутентифікація клієнта сервером.

Аутентифікація клієнта SSL дозволяє серверу підтвердити особистість користувача. Використовуючи ті самі методи, що й автентифікація сервера, програмне забезпечення сервера з підтримкою SSL може перевіряти, що сертифікат клієнта та відкритий ключ дійсні та видані джерелом сертифіката, який входить до списку надійних джерел сервера. Це підтвердження може бути важливим, якщо, наприклад, сервером є банк, який надсилає клієнту конфіденційну фінансову інформацію, і він хоче перевірити особу одержувача. Процес аутентифікації клієнта сервером ілюструється на рис.



Алгоритм процедури встановлення з’єднання по протоколу рукостискання

Послідовність дій при встановленні TLS –з’єднання:

1. Клієнт підключається до сервера, що підтримує TLS і запрошує захищене з’єднання.

2. Клієнт надає список підтримуваних алгоритмів шифрування і хеш- функцій.

3. Сервер вибирає із списку, наданого клієнтом, найбільш стійкі алгоритми, які також підтримуються сервером, і повідомляє про свій вибір клієнтові.

4. Сервер відправляє клієнтові цифровий сертифікат для власної автентифікації. Зазвичай, цифровий сертифікат містить ім’я сервера, ім’я довіреного Центру Сертифікації і відкритий ключ сервера.

5. Клієнт може зв’язатися з сервером довіреного Центру Сертифікації і підтвердити автентичність переданого сертифікату до початку передачі даних.

6. Для того, щоб згенерувати сеансовий ключ для захищеного з’єднання, клієнт шифрує випадково згенеровану цифрову послідовність відкритим ключем сервера і надсилає результат на сервер. Зважаючи на специфіку алгоритму асиметричного шифрування, що використовується для встановлення з’єднання, тільки сервер може розшифрувати отриману послідовність, використовуючи свій закритий ключ.

Протокол Запису

Вище протоколу Запису можуть розташовуватися наступні протоколи:

- протокол Рукостискання;
- Alert-протокол;
- протокол зміни шифрування;
- прикладний протокол, безпека якого забезпечується.

У протоколі вводиться поняття стану з'єднання, що визначає параметри виконання протоколу Запису. Такими параметрами є:

- алгоритм стиску;
- алгоритм шифрування;
- MAC-алгоритм;
- параметри цих алгоритмів, тобто секрети MAC, ключі алгоритму шифрування й ініціалізаційні вектора.

Для кожного напрямку (відповідно читання або запис) параметри з'єднання можуть розрізнятися.

Існує чотири стани з'єднання:

- поточні стани читання й запису;
- очікувані стани читання й запису.

Стан з'єднання

Параметри безпеки для очікуваних станів встановлюються протоколом Рукостискання, а протокол зміни шифрування робить очікуваний стан поточним, у результаті чого відповідні параметри поточного стану скидаються й заміняються параметрами очікуваного стану. Параметри очікуваного стану ініціалізуються порожніми значеннями. Початковий поточний стан завжди визначається без використання шифрування, стиску й MAC.

Кінець з'єднання	Кожний учасник є або "клієнтом", або "сервером"
Алгоритм симетричного шифрування	Алгоритм, що використовується для симетричного шифрування, і його параметри – довжина ключа алгоритму, довжина блоку алгоритму, ключ шифрування, ініціалізаційний вектор (IV) і ін.
MAC алгоритм	Алгоритм, що використовується для перевірки цілісності повідомлення, секрет MAC.
Алгоритм стискування	Алгоритм, що використовується для стискання даних.
Майстер-Секрет	48-байтний секрет, поділюваний обома учасниками з'єднання.
Випадкове число клієнта SecurityParameters.client_random	32-байтне значення, створюване клієнтом у протоколі Рукостискання.
Випадкове число сервера SecurityParameters.server_random	32-байтне значення, створюване сервером у протоколі Рукостискання.
Послідовний номер	Кожний стан з'єднання містить послідовний номер, що обчислюється незалежно для станів читання й запису. Послідовний номер повинен установлюватися в нуль при ініціалізації стану. Послідовні номери не можуть бути більше $2^{64} – 1$. Послідовний номер зростає після створення чергового запису.

Методи обміну ключами

- Анонімний обмін ключами
  Повністю анонімна сесія може бути встановлена при використанні алгоритму RSA або Діффі-Хеллмана для створення ключів обміну. У разі використання RSA клієнт шифрує секрет (pre-master secret) за допомогою відкритого ключа несертифікованого сервера.
- Обмін ключами при використанні RSA
  У цьому випадку обмін ключами та автентифікація сервера може бути комбінована. Відкритий ключ також може міститися в сертифікаті сервера або може бути використаний тимчасовий ключ RSA, який надсилається в повідомленні обміну ключами від сервера.
- Обмін ключами при використанні алгоритму Діффі-Хеллмана
  У цьому випадку сервер може також підтримувати алгоритм Діффі-Хеллмана або може використовувати повідомлення обміну ключами від сервера для посилки набору часових параметрів підписаних сертифікатами DSS або RSA.

Протокол Рукостискання (1)

- Протокол Рукостискання складається із трьох підпротоколів, використання яких дозволяє учасникам погодити криптографічні алгоритми, автентифікувати один одного, і повідомити один одному про виникнення тих або інших помилок.
- У результаті виконання протоколу Рукостискання будуть створені наступні елементи сесії:

Ідентифікатор сесії	Довільна послідовність байтів, обирана сервером для ідентифікації активного або поновлюваного стану сесії.
Сертифікат учасника	X.509 v3 сертифікат учасника. Цей елемент може бути нульовим.
Метод стиску	Алгоритм, використовуваний для стиску даних перед шифруванням.
Набір алгоритмів	Алгоритм симетричного шифрування даних (наприклад, NULL, DES, AES і т.д.), MAC-алгоритм (такий як MD5 або SHA-1) і параметри цих алгоритмів.
Майстер-Секрет	48-байтний секрет, поділюваний клієнтом і сервером.
Поновлювано	Прапор, що визначає, чи може дана сесія використовуватися для створення нового TCP-з'єднання.

Протокол Рукостискання (2)

- Протокол зміни шифрування
  Протокол складається з єдиного повідомлення, що зашифроване й стисле, як визначено в поточному стані з'єднання.
- Alert-протокол
  Одним із протоколів, що виконуються вище протоколу Запису, є протокол Alert.
- Протокол Рукостискання
  Криптографічні параметри сесії створюються протоколом Рукостискання, що виконується вище протоколу Запису.

Протокол Рукостискання складається з наступних кроків:

1. Обмін повідомленнями Hello для узгодження алгоритмів, обміну випадковими значеннями й перевірки поновлюємості сесії.

2. Обмін необхідними криптографічними параметрами, які дозволяють клієнтові й серверу погодити премайстер-секрет.

3. Обмін сертифікатами й криптографічною інформацією, що дозволяє клієнтові й серверу автентифікувати один одного.

4. Надання параметрів безпеки на рівень Запису.

5. Можливість клієнтові й серверу перевірити, що вони обчислили ті самі параметри безпеки й що Рукостискання відбулося без втручання зловмисника.

Протокол Рукостискання (3)

Послідовність повідомлень при повному Рукостисканні



Послідовність повідомлень при скороченому Рукостисканні



- Повідомлення Certificate (сервера). Сервер повинен посилати сертифікат, якщо метод обміну ключів не є анонімним. Дане повідомлення завжди іде відразу за повідомленням Server Hello.
- Повідомлення Certificate Request. Неанонімний сервер може додатково запросити сертифікат клієнта, якщо це потрібно для політики безпеки сервера.
- Повідомлення Server Hello Done. Повідомлення Server Hello Done посилається сервером як ознака закінчення фази Server Hello.
- Повідомлення Certificate (клієнта). Це перше повідомлення, що клієнт посилає після одержання повідомлення Server Hello Done. Воно посилається тільки в тому випадку, якщо сервер запросив автентифікацію клієнта.
- Повідомлення Client Key Exchange. Дане повідомлення посилається клієнтом завжди. Воно іде відразу за повідомленням Client Certificate, якщо воно посилалося.
- Перевірка цілісності за допомогою сертифіката клієнта. Дане повідомлення використовується для виконання перевірки цілісності переданих і отриманих повідомлень Рукостискання й автентифікації клієнта.
- Повідомлення Finished завжди посилається безпосередньо після повідомлення Change Cipher Spec для перевірки успішного виконання обміну ключа й процесів автентифікації.
- Обчислення майстер-секрету. Незалежно від методів обміну ключа використовується наступний алгоритм для перетворення премайстер-секрету в майстра-секрет

Додавання додаткових можливостей до протоколу

- Дозволити клієнтам надавати серверу ім'я сервера, з яким вони встановлюють з'єднання. Дана функціональність забезпечує можливість встановлення безпечних з'єднань із хостами, що мають кілька віртуальних серверів на одній мережевій адресі.
- Вести перемовини про максимальну довжину переданих фрагментів. Дана функціональність необхідна через обмеження пам'яті в деяких клієнтів і обмеження смуги пропущення в деяких типах мереж.
- Вести перемовини про використання URL для вказівки сертифікатів клієнта. Дана функціональність потрібна для економії пам'яті клієнта.
- Дозволити клієнтам вказати серверам сертифікати які вони мають в кореневих CA. Дана функціональність необхідна, щоб клієнти з обмеженою пам'яттю могли зберігати тільки невелике число сертифікатів кореневих CA.
- Дозволити клієнтам і серверам вести перемовини про використання урізаних MAC. Дана функціональність дає можливість зменшити трафік, що може бути необхідним в певних типах мереж.
- Дозволити клієнтам і серверам вести перемовини про те, щоб сервер при Рукостисканні посилав клієнтові інформацію про статус сертифіката (наприклад, відповідь OCSP). Дана функціональність дозволяє уникнути посилки CRL і тим самим скоротити трафік і обчислювальне навантаження на клієнта.

URL сертифікат клієнта

- SSL/TLS вимагає, щоб при виконанні автентифікації клієнта сертифікати клієнта посилали серверу в протоколі Рукостискання. Для клієнтів, що мають обмеження пам'яті, існує можливість посилати URL сертифікат замість самих сертифікатів, щоб вони могли не зберігати свої сертифікати й тим самим не займати пам'ять.
- Вказівка довіреного CA. Клієнти, які мають обмежену пам'ять, можуть зберігати тільки невелику кількість сертифікатів кореневих CA. У цьому випадку вони можуть вказати серверу, якими кореневими сертифікатами вони володіють.
- Урізаний HMAC. У даний момент набір шифрування використовує в якості MAC HMAC або з MD5, або з SHA-1 для автентифікації з'єднань рівня запису. Результат обчислення геш-функції використовується як значення MAC.

Атаки проти протоколу SSL

Основні види атак, які можуть бути здійснені проти протоколу SSL наступні:

- розкриття шифрів; , якщо здійснити успішну атаку на асиметричні криптоалгоритми, то SSL не може вже вважатися безпечним.
- атака «зловмисник посередині»; зловмисник може перехоплювати всі повідомлення, які йдуть в обох напрямках, і підміняти їх. Зловмисник представляється сервером для клієнта і клієнтом для сервера. У разі обміну ключами по алгоритму Діффі-Хеллмана дана атака є ефективною, оскільки цілісність прийнятої інформації і її джерело перевірити неможливо.
- атака відбиттям; Зловмисник записує комунікаційну сесію між сервером і клієнтом. Пізніше, він намагається встановити з'єднання з сервером, відтворюючи записані повідомлення клієнта.
- атака проти протоколу рукостискання. Зловмисник може спробувати вплинути на обмін рукостисканнями для того, щоб сторони обрали різні алгоритми шифрування, а не ті, що вони обирають зазвичай.

Протокол SOCKS (1)

Протокол SOCKS організовує процедуру обміну даними між клієнтом і сервером додатків на рівні сеансу моделі OSI через сервер посередництва, або проксі-сервер.

В цілому програми посередництва, які традиційно використовуються в брандмауерах, можуть виконувати такі функції:

- ідентифікація та аутентифікація користувачів;
- шифрування даних, що передаються;
- розмежування доступу до внутрішніх мережевих ресурсів;
- розмежування доступу до зовнішніх мережевих ресурсів;
- фільтрація та перетворення потоку повідомлень, наприклад, сканування на віруси та прозоре шифрування інформації;
- переклад внутрішніх мережевих адрес для вихідних потоків повідомлень.

Протокол SOCKS (2)

Загальну схему встановлення з'єднання за допомогою протоколу SOCKS версії 5 можна описати так:

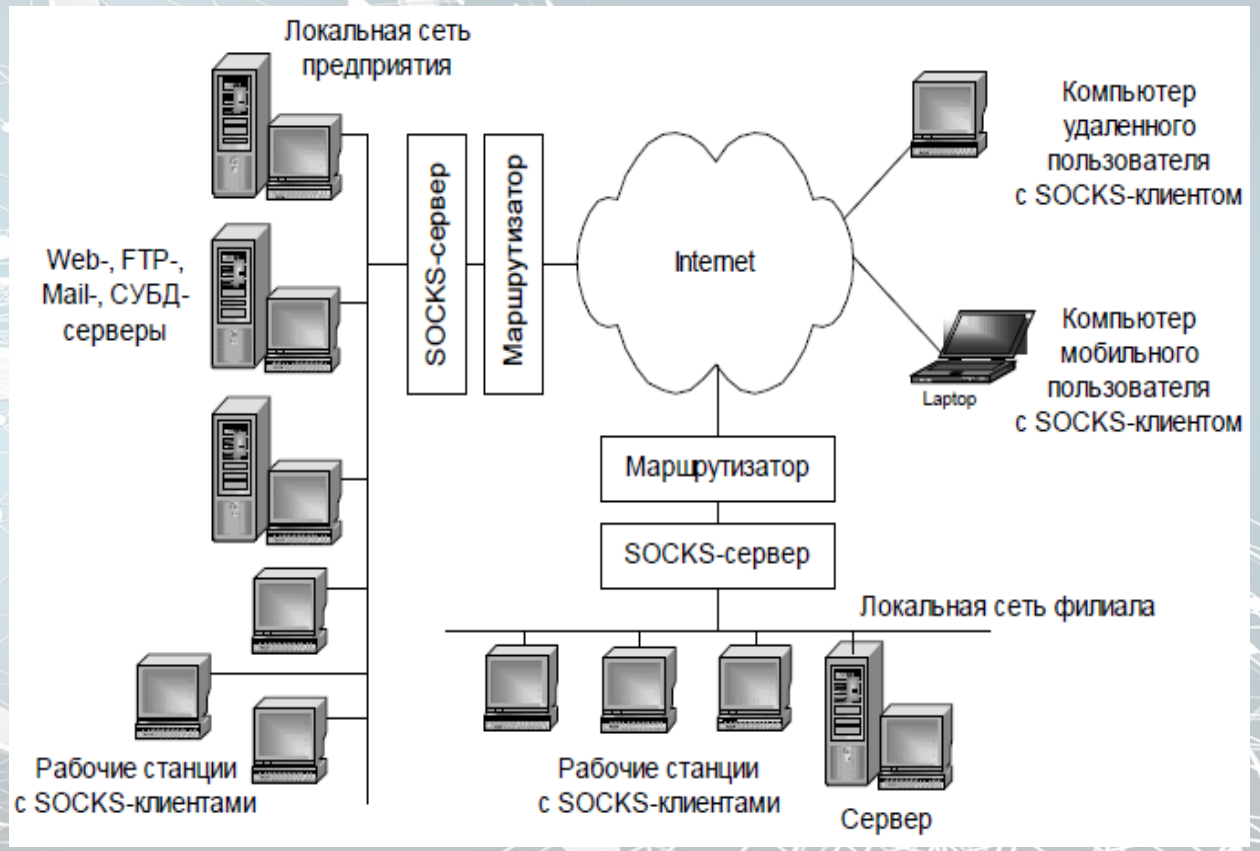
- Запит від клієнта програми, який бажає встановити з'єднання з сервером додатків в мережі, перехоплює клієнт SOCKS, встановлений на тому ж комп'ютері.
- при підключенні до сервера SOCKS клієнт SOCKS надає йому ідентифікатори всіх методів аутентифікації, які він підтримує;
- сервер SOCKS вирішує, який метод автентифікації використовувати (якщо сервер SOCKS не підтримує жоден із методів автентифікації, запропонованих клієнтом SOCKS, з'єднання розривається).
- якщо підтримується будь-який із запропонованих методів аутентифікації, сервер SOCKS проводить аутентифікацію користувача, від імені якого клієнт SOCKS діє відповідно до обраного методу; у разі невдалої аутентифікації сервер SOCKS розриває з'єднання;
- після успішної аутентифікації клієнт SOCKS передає на сервер SOCKS DNS-ім'я або IP-адресу запитуваного сервера додатків в мережі, після чого сервер SOCKS приймає рішення про встановлення з'єднання з цим сервером додатків на основі існуючих правил контролю доступу;

Протокол SOCKS (3)

Крім аутентифікації користувача, трансляції IP-адрес і шифрування трафіку, сервер SOCKS може виконувати такі функції, як:

- розмежування доступу до внутрішніх мережевих ресурсів;
- розмежування доступу до зовнішніх мережевих ресурсів;
- Фільтрація потоку повідомлень, наприклад, динамічне сканування на віруси.
- Реєстрація на захід та реагування на зазначені події
- кешування даних, що запитуються із зовнішньої мережі.

Схема взаємодії SOCKS



Питання для самоконтролю

1. Для чого потрібен і особливості протоколу PPTD?
2. Опишіть архітектуру протоколу L2TP.
3. У чому полягають особливості та особливості протоколу L2TP?
4. Як формується захищений віртуальний канал за допомогою протоколу L2TP?
5. Яке призначення та основні компоненти стека протоколів IPSec?
6. Опишіть архітектуру безпеки IP.
7. Як забезпечується захист переданих даних за допомогою протоколів AN і ESP в IPSec?
8. Опишіть алгоритми автентифікації та шифрування, які використовуються в IPSec.
9. Вкажіть призначення та функціональні можливості протоколу IKE в IPSec.
10. Які функції безпеки надає SSL? Які переваги та недоліки протоколу SSL?
11. Для чого потрібен і особливості протоколу SOCKS?

МІЖМЕРЕЖЕВІ ЕКРАНИ (ФАЄРВОЛИ, БРАНДМАУЕРИ)

Основні положення (1)

В основу забезпечення безпеки локальних мереж і розміщених у них інформаційних систем повинні бути покладені наступні основні принципи:

- Забезпечення інформаційної безпеки вимагає комплексного й цілісного підходу. Інформаційна безпека повинна бути невід'ємною частиною систем керування в організації. Велике значення для забезпечення безпеки інформаційної системи мають соціальні фактори, а також міри адміністративної, організаційної й фізичної безпеки.
- Інформаційна безпека повинна бути економічно виправданою.
- Відповідальність за забезпечення безпеки повинна бути чітко визначена.
- Безпека інформаційної системи повинна періодично аналізуватися й переоцінюватися.

Фаєрвол (міжмережевий екран, або брандмауер) – це комплекс програмно-апаратних засобів, що здійснює інформаційний захист однієї частини комп’ютерної мережі від іншої шляхом аналізу і фільтрації трафіку, що проходить між ними.

Основні положення (2)

Атакуючий, бажаючий одержати доступ у локальну мережу або до інформаційних систем, може переслідувати наступні цілі:

- одержати доступ до інформації з метою читання або модифікації даних, що зберігаються в системі;
- здійснити атаки на сервіси, щоб перешкодити використовувати їх або змінити їхнє функціонування.

Розглянемо технології запобігання небажаного доступу в локальну мережу й до інформаційних систем.

Сервіси безпеки, які запобігають небажаний доступ, можна розбити на дві категорії:

- Перша категорія складається із процедур входу, заснованих на використанні різного роду автентифікаторів (паролів, апаратних ключів, сертифікатів і т.п.). Це дозволяє здійснити доступ тільки законним користувачам. До цієї категорії відносяться також різні міжмережеві екрани (firewall), які запобігають атакам, що засновані на використанні уразливостей на різних рівнях стека протоколів TCP/IP.
- Друга категорія складається з різних моніторів, що аналізують доступ і діяльність користувачів.

Основні положення (3)

Для забезпечення максимально ефективної роботи міжмережевих екранів варто дотримуватися наступних принципів:

- Визначити всі вимоги, які накладає зовнішнє оточення на функціонування міжмережевого екрана. Необхідно визначити топологію мережі, яка захищається, використовувані транспортні протоколи (IPv4 або IPv6) і специфіку сервісів, що захищаються, й типи технологій міжмережевих екранів, які найбільш ефективні в цьому випадку. Також варто пам'ятати про продуктивність і про інтеграцію міжмережевого екрана в існуючу мережеву інфраструктуру й інфраструктуру безпеки. Необхідно враховувати вимоги до фізичного оточення й до кваліфікації персоналу, а також вимоги, які можуть виникнути надалі, такі як перехід на технології IPv6 або впровадження VPN.
- Створити політику міжмережевого екрана, у якій визначено, як варто обробляти вхідний і вихідний трафік. Необхідно виконати аналіз ризиків і визначити при яких умовах якому типу трафіку дозволено проходити через міжмережевий екран. Звичайно весь вхідний і вихідний трафік, що явно не дозволений політикою міжмережевого екрана, повинен бути заборонений. Це знижує ризик атак і може зменшити обсяг трафіку в мережі. У політиці повинно бути визначено, як міжмережевий екран обробляє вхідний і вихідний трафік для конкретних IP-адрес, діапазонів адрес, протоколів, застосунків і типів умісту.
- Розробити набір правил міжмережевого екрана, які реалізують політику безпеки в організації й забезпечують максимальну продуктивність міжмережевого екрана. Проаналізувати продуктивність міжмережевого екрана. Набір політик безпек повинен максимально ефективно обробляти трафік. При створенні набору правил варто визначити типи дозволеного трафіку, включаючи протоколи, які необхідні для керування самим міжмережевим екраном. Деталі створення набору правил залежать від типу міжмережевого екрана й конкретного виробника, але часто продуктивність міжмережевого екрана залежить від оптимізації набору правил. Наприклад, більшість міжмережевих екранів послідовно порівнюють трафік із правилами доти, поки не буде знайдена відповідність. Для таких міжмережевих екранів правила, які найчастіше будуть відповідати шаблонам трафіку, повинні бути розміщені вгорі списку.
- Управляти архітектурою, політиками, ПЗ й іншими компонентами міжмережевого екрана треба протягом усього часу його функціонування. Існує багато аспектів, що стосується керування міжмережевим екраном. Наприклад, вибір одного або декількох типів міжмережевих екранів і їхнє розташування в мережі може істотно впливати на політику безпеки, що зможуть реалізовувати ці міжмережеві екрани. При зміні вимог в організації може знадобитися змінити набір правил, щоб у мережі могли функціонувати нові додатки або хости. Необхідно також стежити за продуктивністю компонентів міжмережевого екрана, щоб потенційні проблеми з ресурсами були вчасно визначені. Також повинні постійно проглядатися логи й оповіщення для визначення загроз, як здійснених, так і не здійснених.

Параметри брандмауера

Існує дві основні версії брандмауерів – програмна та апаратна. У свою чергу, програмно-апаратна версія брандмауерів має два різновиди - у вигляді спеціалізованого пристрою і у вигляді модуля в роутері або комутаторі.

- У програмно-апаратних комплексах використовуються спеціалізовані або звичайні операційні системи (як правило, на базі FgeeBSD, Linux або Microsoft Windows NT/2000), зведені до виконання заданих функцій і відповідають ряду вимог:
- володіти засобами розмежування доступу до ресурсів системи;
- заблокувати доступ до ресурсів комп'ютера в обхід наданого інтерфейсу програми;
- Заборонити привілейований доступ до ваших ресурсів з локальної мережі.
- містять інструменти для моніторингу/аудиту будь-яких адміністративних дій.

Спеціалізовані програмно-апаратні рішення мають такі переваги:

- простота впровадження в технологію обробки інформації. Такі інструменти поставляються з попередньо встановленою та налаштованою операційною системою та механізмами безпеки, тому вам потрібно лише підключити їх до мережі, що робиться протягом кількох хвилин;
- простота в експлуатації. Цими інструментами можна керувати з будь-якої робочої станції Windows або UNIX. Взаємодія консолі управління з пристроєм здійснюється або за допомогою стандартних протоколів, наприклад, Telnet або SNMP, або за допомогою спеціалізованих або захищених протоколів, наприклад, SSH або SSL;
- відмовостійкість і висока доступність. Конструкція брандмауера у вигляді спеціалізованого програмно-апаратного комплексу дозволяє реалізувати механізми забезпечення не тільки програмної, але і апаратної відмовостійкості і високої доступності;
- висока продуктивність і надійність. За рахунок виключення з операційної системи всіх зайвих служб і підсистем, програмно-апаратний комплекс працює більш ефективно з точки зору продуктивності і надійності;
- спеціалізація з оборони. Вирішення тільки завдань мережевої безпеки не призводить до витрат ресурсів на виконання інших функцій, таких як маршрутизація і т.д.

Загрози та політики безпеки

Уніфіковане управління загрозами

- Міжмережеві екрани для веб-додатків
- Міжмережеві екрани для віртуальних інфраструктур
- Міжмережеві екрани для окремих хостів і домашніх мереж

Політика міжмережевого екрану

- політики, засновані на IP-адресації і протоколах (IP-адреси та інші характеристики IP, IPv6, протоколи TCP і UDP, протокол ICMP);
- політики, засновані на додатках;
- політики, засновані на ідентифікації користувача;
- політики, засновані на мережевій активності.

Функції брандмауера

Брандмауер, що захищає відразу багато вузлів внутрішньої мережі, покликаний вирішити дві основні проблеми:

- обмеження доступу зовнішніх користувачів до внутрішніх ресурсів корпоративної мережі.
- розмежування доступу користувачів захищеної мережі до зовнішніх ресурсів.

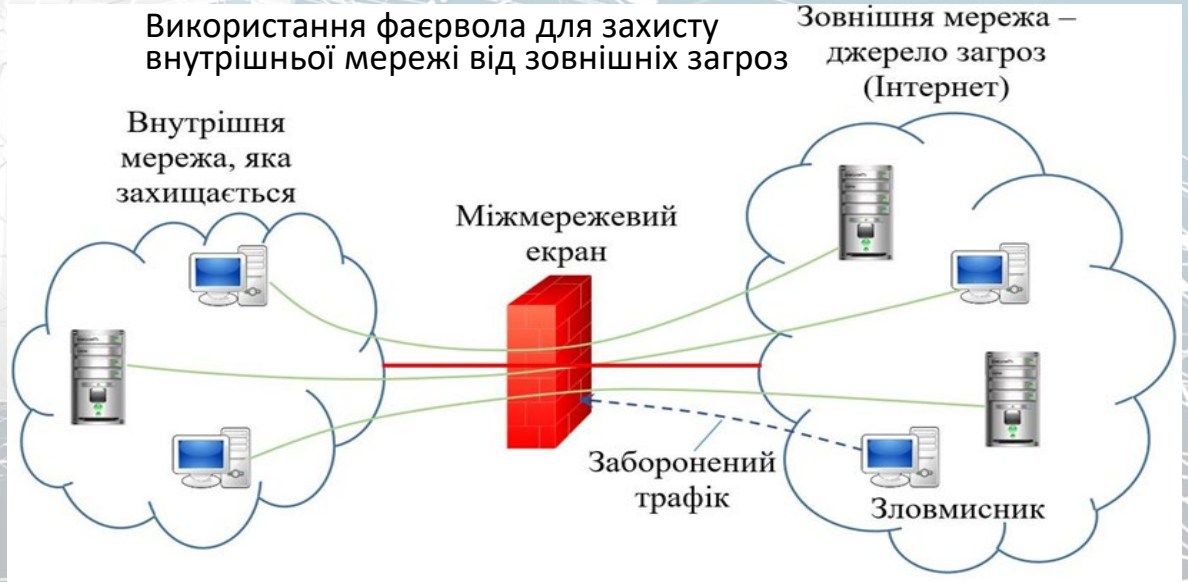
Основними функціями фаєрвола є:

- фільтрація трафіку з метою захисту внутрішніх ресурсів мережі;
- аудит – фаєрвол повинен фіксувати всі події, пов’язані з виявленням і блокуванням підозрілих пакетів.

Поряд з цими двома базовими функціями на фаєрвол можуть бути покладені і інші допоміжні функції захисту, зокрема:

- антивірусний захист;
- шифрування трафіку;
- логічне посередництво між внутрішніми клієнтами та зовнішніми серверами (функція проксі-сервера);
- фільтрація повідомлень по вмісту, включаючи типи файлів, що передаються, імена DNS і ключові слова;
- попередження і виявлення вторгнень і мережевих атак;
- функції VPN;
- трансляція мережевих адрес (NAT).

Використання фаєрвола для захисту внутрішньої мережі від зовнішніх загроз



Посередництво (1)

Брандмауер виконує посередницькі функції за допомогою спеціальних програм, які називаються посередницькими програмами або екрануючими агентами. Ці програми є резидентними і забороняють пряму передачу пакетів повідомлень між зовнішньою і внутрішньою мережею.

В цілому посередницькі програми, блокуючи прозору передачу потоку повідомлень, можуть виконувати такі функції:

- перевірка достовірності переданих даних;
- фільтрація та перетворення потоку повідомлень, таке як динамічне сканування на віруси та прозоре шифрування інформації;
- розмежування доступу до внутрішніх мережевих ресурсів;
- розмежування доступу до зовнішніх мережевих ресурсів;
- кешування даних, що запитуються із зовнішньої мережі.
- ідентифікація та аутентифікація користувачів;
- переклад внутрішніх мережевих адрес для пакетів вихідних повідомлень;
- реєстрація заходу, реагування на зазначені події, а також аналіз зареєстрованої інформації та формування звітів.

Посередництво (2)

Методи розмежування доступу до ресурсів внутрішньої мережі практично не відрізняються від методів диференціації, що підтримуються на рівні операційної системи.

При розмежуванні доступу до зовнішніх мережевих ресурсів найчастіше використовується один з наступних підходів:

- дозвіл доступу тільки до вказаних адрес у зовнішній мережі;
- фільтрація запитів на основі оновлених списків невірних адрес та блокування пошуку інформаційних ресурсів за небажаними ключовими словами;
- накопичення та оновлення адміністратором авторизованих інформаційних ресурсів зовнішньої мережі в дисковій пам'яті брандмауера та повна заборона доступу до зовнішньої мережі.

Фільтрація та перетворення потоку повідомлень виконується брокером на основі заданого зводу правил. Тут слід розрізняти два типи програм медіації:

- агенти екранування, орієнтовані на аналіз потоку повідомлень для певних видів послуг, наприклад, FTP, NTTR, Telnet;
- Універсальні захисні агенти, які обробляють весь потік повідомлень, такі як агенти, орієнтовані на виявлення та нейтралізацію комп'ютерних вірусів або прозоре шифрування даних.

Технології міжмережевих екранів

- Канальний рівень (також називаний Data Link рівень) забезпечує взаємодію компонентів фізичної мережі. Міжмережеві екрани рідко мають справу з даними на цьому рівні. Блок даних, переданий на канальному рівні, називають кадром.
- Мережний рівень (також називаний IP-рівнем) маршрутизує пакети між локальними мережами. Блок даних, переданих по мережному рівню, називають дейтаграмою.
- Транспортний рівень надає сервіси, орієнтовані на з'єднання, які використовуються для передачі даних між мережами. На транспортному рівні виникає поняття сесії як потоку даних між двома додатками.
- Прикладний рівень посилає й одержує дані конкретних застосунків, таких як DNS, HTTP, SMTP. Прикладний рівень сам може складатися з декількох підрівнів. Наприклад, SMTP або HTTP можуть інкапсулювати інші формати, такі як HTML.
- Міжмережеві екрани аналізують дані одного або декількох рівнів. Вважається, що чим більше рівнів аналізує міжмережевий екран, тим більше розвиненим і ефективним він є.
- Незалежно від архітектури, міжмережевий екран може надавати додаткові сервіси. Ці сервіси включають трансляцію мережних адрес (NAT), підтримку протоколу динамічної конфігурації хосту (DHCP), функції шифрування, тим самим будучи кінцевою точкою VPN-шлюзу.

Стани TCP-з'єднання

Установлення TCP-з'єднання відбувається з використанням так званого "потрійного рукостискання". З'єднання ініціює клієнт, посилаючи пакет із установленим бітом SYN. Сервер відповідає клієнтові пакетом із установленими бітами SYN і ACK. Сервер також передає початковий порядковий номер у поле Sequence Number. Нарешті, клієнт посилає серверу повідомлення із установленим бітом ACK, у поле Sequence Number вказує свій початковий номер, у поле Acknowledgement Number вказує отриманий від сервера початковий порядковий номер, збільшений на одиницю.
Протягом свого життєвого циклу з'єднання проходить через кілька станів.

Стани на стороні клієнта:

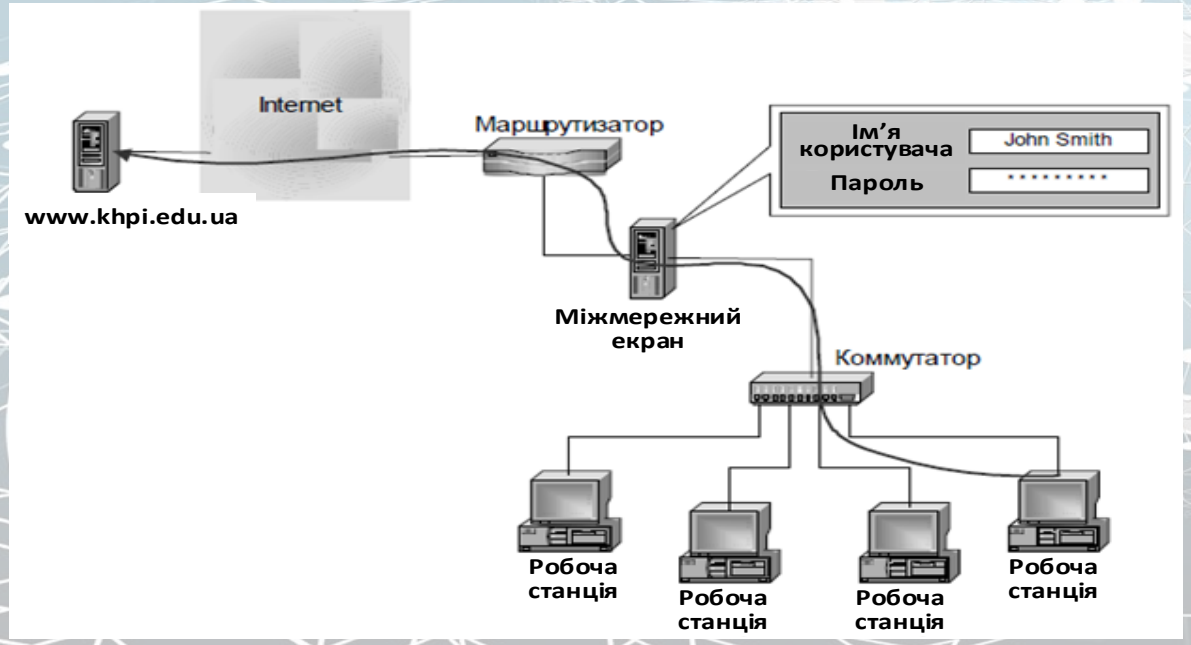
- CLOSED;
- SYN-SENT;
- ESTABLISHED;
- FIN-WAIT-1;
- CLOSE-WAIT;
- FIN-WAIT-2;
- CLOSING;
- LAST-ACK;
- CLOSED;

Стани на стороні сервера:

- CLOSED;
- LISTEN;
- SYN-RESEIVED;
- ESTABLISHED;
- FIN-WAIT-1;
- CLOSE-WAIT;
- FIN-WAIT-2;
- CLOSING;
- TIME-WAIT;
- CLOSED.

Додаткові можливості брандмауера

Ідентифікація та аутентифікація користувача іноді проводяться при пред'явленні звичайного ідентифікатора (імені) і пароля. Однак ця схема вразлива з точки зору безпеки – пароль може бути перехоплений і використаний іншою людиною. Багато інцидентів в Інтернеті сталися частково через вразливість традиційних паролів для повторного використання. Зловмисники можуть стежити за каналами в інтернеті і перехоплювати паролі, передані у відкритому тексті, тому така схема аутентифікації вважається неефективною. Пароль повинен передаватися по публічних комунікаціях в зашифрованому вигляді (рис.ліворуч). Трансляція мережевих адрес. Для здійснення безлічі атак зловмиснику необхідно знати адресу своєї жертви. Щоб приховати ці адреси, а також топологію всієї мережі, брандмауери виконують дуже важливу функцію – Network Address Translation. (рис.праворуч).





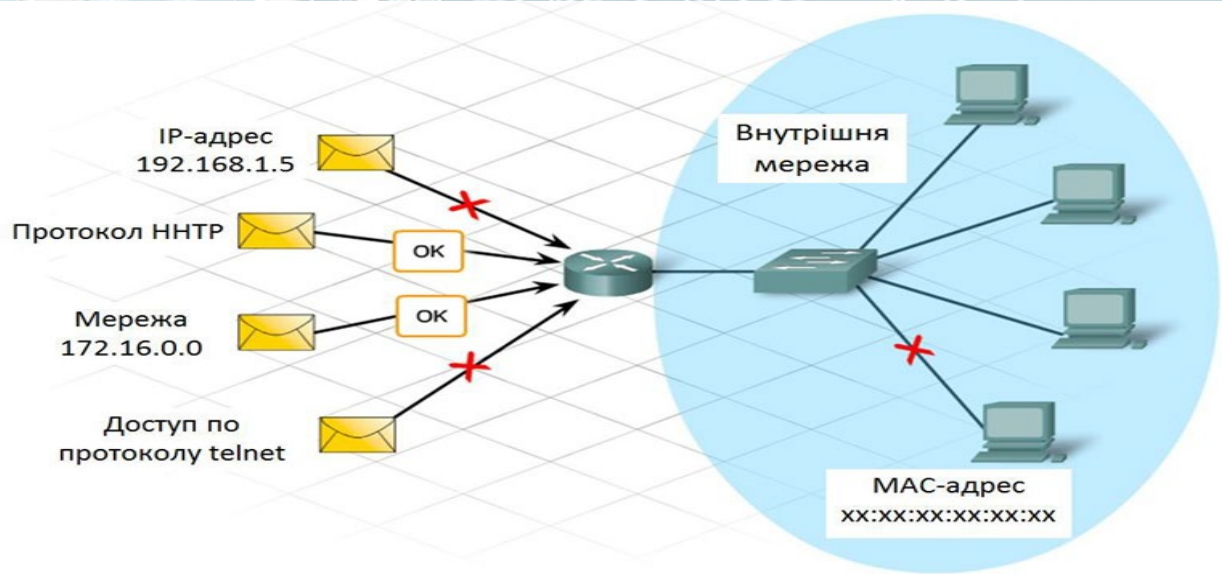
Технології безпеки на основі фільтрування і моніторингу трафіка (1)

Фільтрація інформаційних потоків полягає в їх вибірковому проходженні через екран, можливо, з виконанням деяких перетворень (рис.зверху)

Фільтрація пакетів може бути простою і складною і може забороняти або дозволяти трафік за наступними критеріями (рис. знизу):

- вихідна IP-адреса;
- кінцева IP-адреса;
- MAC-адреси;
- протоколи;
- тип програми.





Технології безпеки на основі фільтрування і моніторингу трафіка (2)

Кожен фільтр призначений для інтерпретації окремих правил фільтрації шляхом виконання наступних дій:

- Аналіз інформації за критеріями, зазначеними в інтерпретованих правилах, наприклад, за адресами одержувача і відправника або за типом заявки, для якої ця інформація призначена.
- Прийняття одного з наступних рішень на основі тлумачених правил:
  - не пропустити дані;
  - обробити дані від імені одержувача та повернути результат відправнику;
  - Передайте дані в наступний фільтр, щоб продовжити аналіз.
  - Пропустіть дані, ігноруючи наступні фільтри.

У число пристроїв, що найчастіше використовуються для фільтрації трафіку, входять наступні:

- міжмережеві екрани, вбудовані в інтегровані маршрутизатори;
- виділені пристрої забезпечення безпеки;
- сервери.

У правилах фільтрації також можуть бути вказані додаткові дії, які пов'язані з функціями посередництва, наприклад, трансформація даних, реєстрація подій тощо.

- дозвіл або заборона подальшої передачі даних;
- виконання додаткових захисних функцій.
- В якості критеріїв аналізу інформаційного потоку можуть бути використані такі параметри:
- службові поля пакетів повідомлень, що містять мережеві адреси, ідентифікатори, адреси інтерфейсів, номери портів та інші значущі дані;
- Безпосередній вміст пакетів повідомлень, просканований, наприклад, на наявність комп'ютерних вірусів.
- Зовнішні характеристики інформаційного потоку, такі як час, частотні характеристики, обсяг даних і т.д.

Класифікація брандмауерів (1)

За функціонуванням на рівнях моделі OSI:
- пакетний фільтр (екрануючий маршрутизатор);
- Шлюз на рівні сеансу (екрануючий транспорт)
- Шлюз додатків;
- Шлюз експертного рівня (брандмауер Stateful Inspection).

За технологією використовують:
- Державна інспекція;
- на основі проксі-модулів.

За виконанням:
- апаратні та програмні засоби;
- програма.

За схемою підключення:
- єдина схема захисту мережі;
- Схема із захищеними закритими та незахищеними відкритими сегментами мережі.
- схема з роздільним захистом замкнутих і відкритих сегментів мережі.

Класифікація брандмауерів (2)

У найзагальнішому вигляді за способом реалізації розрізняють програмний, апаратний і програмно-апаратний фаєрволи:

- програмний фаєрвол реалізований як програмна система, що працює під управлінням універсальної ОС, такої як Microsoft Windows, Linux або Mac OS;
- апаратний фаєрвол реалізований як набір додаткових функцій маршрутизатора, що стосуються фільтрації (рідше - Ethernet-комутатора);
- програмно-апаратний фаєрвол включає як програмну систему, так і спеціалізований сервер, операційна система якого і апаратура мають конфігурацію і налаштування, оптимізовані для роботи фаєрвола

Залежно від способу фільтрації розрізняються фаєрволи без запам'ятовування стану і фаєрволи із запам'ятовуванням стану:

- фаєрволи без запам'ятовування стану (stateless) виконують фільтрацію на основі статичних правил, при цьому не відслідковуються стани з'єднань (сеансів);
- фаєрволи з запам'ятовуванням стану (stateful) приймають рішення динамічно з врахуванням поточного стану сеансу і його передісторії.

Класифікація брандмауерів (3)

За рахунок додаткових модулів фаєрволи прикладного рівня можуть підтримувати різні функції захисту програмного забезпечення, наприклад:

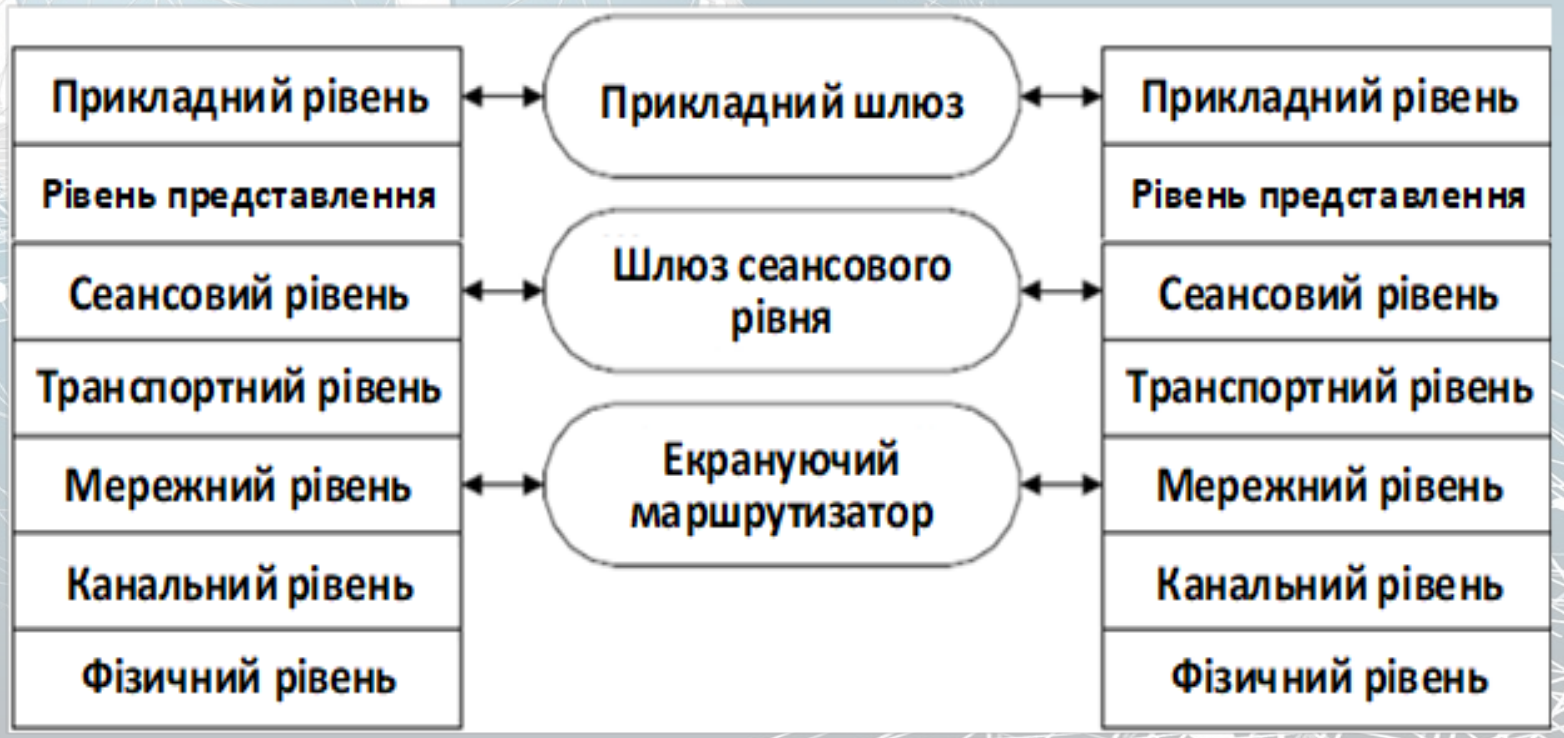
- антивірусний контроль в реальному часі завантажуваних користувачем файлів і одержуваних листів;
- контроль контенту, що полягає, наприклад, в обмеженні доступу користувачів до зовнішніх веб-сайтів, сторінки яких містять задані ключові слова; такий же контроль може застосовуватися до електронних листів, що відправляються зовні;
- транзитна автентифікація користувачів, що звертаються до деякого додатку на внутрішньому сервері, – ця функція корисна для тих додатків, які або не виконують автентифікацію користувачів зовсім, або роблять це незахищеним способом, як, наприклад, FTP-сервер, який приймає паролі користувачів в відкритому вигляді: фаєрвол перехоплює звернення користувача до FTP-сервера і організовує сеанс логічного входу користувача, наприклад, з сервером автентифікації Kerberos, якщо саме такий спосіб автентифікації застосовується в корпоративної мережі;
- централізоване шифрування електронних листів користувачів, що позбавляє користувачів від необхідності конфігурувати таку функцію на своїх клієнтських комп’ютерах (для цього фаєрвол повинен зберігати цифрові сертифікати користувачів);
- функції шлюзу VPN з віддаленими підрозділами підприємства і віддаленими користувачами;
- трансляція внутрішніх IP-адрес користувачів на основі стандарту NAT.

Особливості функціонування брандмауерів на різних рівнях моделі OSI

Найчастіше інтегрований екран функціонує на мережевому, сеансовому та прикладному рівнях еталонної моделі. Відповідно розрізняють такі неподільні ME (рис.), як:

- екрануючий фрезер;
- шлюз на рівні сеансу
- шлюз прикладного рівня (shielding gateway)

Шлюз сеансового рівня охоплює транспортний і мережевий рівні моделі OSI. При аналізі пакетів повідомлень екрануючий роутер перевіряє їх заголовки не тільки на мережевому рівні, але і на транспортному рівні.



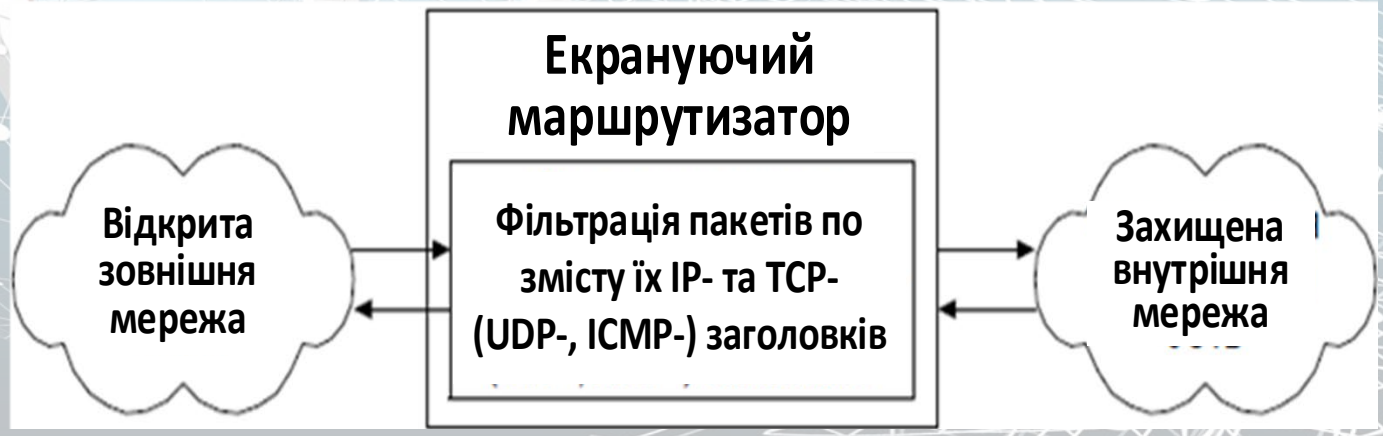
Екрануючий фільтр

Маршрутизатор екранування, також відомий як фільтр фільтра, призначений для фільтрації пакетів повідомлень і забезпечення прозорого зв'язку між внутрішніми та зовнішніми мережами. Він функціонує на мережевому рівні еталонної моделі OSI, але також може охоплювати транспортний рівень еталонної моделі для виконання її окремих функцій.

Рішення про пропуск або відхилення даних приймається на основі кожного пакета на основі вказаних вами правил фільтрації. Для прийняття рішення аналізують заголовки пакетів мережевого і транспортного рівнів (рис. 9.6).

Для аналізу полів заголовків IP і TCP (UDP) кожного пакета можна використовувати наступне:

- Адреса відправника
- адреса отримувача;
- Тип упаковки
- Прапорець фрагментації пакетів
- Номер порту джерела
- Номер порту одержувача.



Шлюз на рівні сеансу

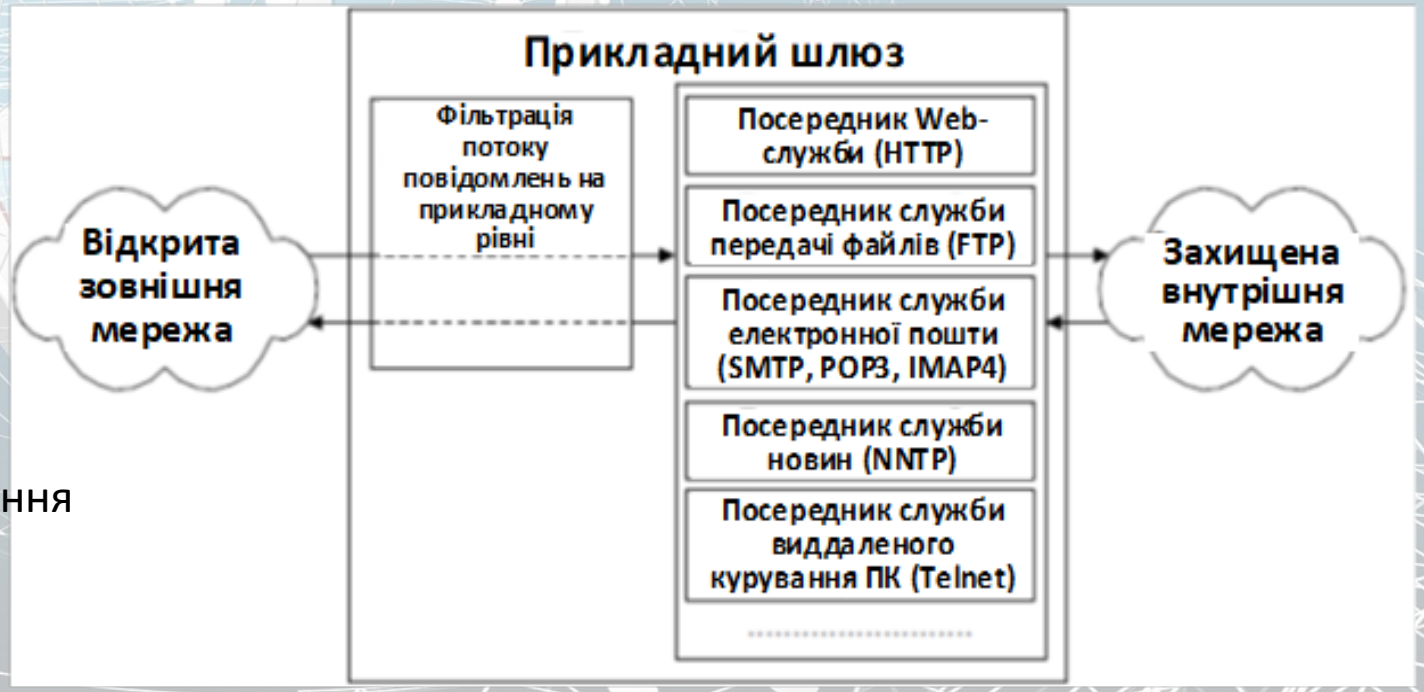
- Шлюз на рівні сеансу, який також називають екрануючим транспортом, призначений для керування віртуальними з'єднаннями та трансляцією IP-адрес під час зв'язку із зовнішньою мережею. Вона функціонує на рівні сеансу моделі CI, охоплюючи також транспортний і мережевий рівні еталонної моделі. Функції безпеки шлюзу на рівні сеансу називаються функціями посередництва.
- Для управління віртуальними з'єднаннями в шлюзах на рівні сеансів використовуються спеціальні програми, які називаються посередниками каналів (Peer Proxies).
  Ці посередники встановлюють віртуальні канали між внутрішньою і зовнішньою мережами, а потім контролюють передачу по цих каналах пакетів, що генеруються TCP/IP додатками (рис.)



Шлюз додатків

Шлюз додатків, званий також екрануючим шлюзом, функціонує на прикладному рівні моделі OSI, також охоплюючи презентаційний рівень, і забезпечує надійний захист міжмережевих взаємодій. Функції безпеки шлюзу додатків, як і шлюз на рівні сеансу, називаються функціями посередництва. Однак шлюз додатків, на відміну від шлюзу на рівні сеансу, може виконувати значно більшу кількість функцій безпеки, до яких можна віднести наступне:

- ідентифікація та аутентифікація користувачів при спробі встановлення з'єднань через брандмауери;
- перевірка достовірності інформації, що передається через шлюз;
- розмежування доступу до внутрішніх і зовнішніх мережевих ресурсів;
- Фільтрація та перетворення потоку повідомлень, наприклад, динамічне сканування на віруси та прозоре шифрування інформації.
- реєстрація заходу, реагування на зазначені події, а також аналіз зареєстрованої інформації та формування звітів;
- кешування даних, що запитуються із зовнішньої мережі.



Шлюз експертного рівня

Для усунення такого істотного недоліку шлюзів додатків, як відсутність прозорості для користувачів і зниження пропускної здатності при реалізації взаємоз'єднань, компанії Checkpoint Point і ON Technology розробили технологію пакетної фільтрації, яку іноді називають фільтрацією Stateful Inspection або фільтрацією на рівні експерта. Така фільтрація проводиться на основі спеціальних методів багаторівневого аналізу стану SMLT (Stateful Multi-Lauer Teshnique).

Ця гібридна технологія дозволяє контролювати стан мережевого з'єднання шляхом перехоплення пакетів на мережевому рівні і вилучення з них інформації прикладного рівня, яка використовується для контролю з'єднання. Швидке порівняння переданих пакетів з відомим станом (State) «дружніх» пакетів може значно скоротити час обробки в порівнянні з брандмауерами прикладного рівня.

Брандмауери на основі описаної технології фільтрації називаються брандмауерами експертного рівня.

Таким чином, брандмауери експертного рівня дають можливість контролювати:

- кожен переданий пакет базується на існуючій таблиці правил;
- кожна сесія – на основі таблиці станів;
- кожен додаток базується на розроблених посередниках.

Схеми захисту мережі на основі брандмауера

При підключенні корпоративної або локальної мережі до глобальних мереж потрібно вирішити такі завдання:

- захист корпоративної або локальної мережі від несанкціонованого віддаленого доступу з глобальної мережі;
- приховування інформації про структуру мережі та її компоненти від користувачів глобальної мережі;
- Розмежування доступу до захищеної мережі з глобальної мережі і з захищеної мережі до мережі WAN.

Для ефективного захисту взаємоз'єднання система брандмауера повинна бути правильно встановлена та налаштована. Цей процес складається з наступних етапів:

- формування політики міжмережевої взаємодії;
- Підбір схеми підключення та налаштування параметрів брандмауера.

Формування політики взаємоз'єднання

Крос-мережева політика є невід'ємною частиною загальної політики безпеки в організації. Політика взаємозв'язку визначає вимоги до безпеки обміну інформацією організації з навколишнім світом. Ця політика повинна відображати два аспекти:

- політика доступу до мережевих сервісів;
- політика роботи брандмауера.
- Політика роботи брандмауера задає основний принцип управління взаємоз'єднаннями, який є основою для функціонування брандмауерів. Можна вибрати один з двох таких принципів:
- все, що явно не дозволено, заборонено;
- дозволено все, що прямо не заборонено.

Брандмауер не симетричний. У ньому є окремі правила, які обмежують доступ з внутрішньої мережі до зовнішньої мережі і навпаки. У загальному випадку робота брандмауера заснована на динамічному виконанні двох груп функцій:

- фільтрація інформаційних потоків, що проходять через нього;
- посередництво при здійсненні міжмережевих взаємодій.

Основні схеми підключення брандмауера

Організації часто необхідно мати в корпоративній мережі кілька сегментів з різним рівнем безпеки:

- сегменти у вільному доступі (наприклад, рекламний WWW-сервер);
- Сегмент з обмеженим доступом (наприклад, для доступу до співробітників в організації з віддалених сайтів).
- Приватні сегменти (наприклад, фінансова локальна підмережа організації).

Для підключення брандмауерів можуть використовуватися різні схеми, які залежать від умов експлуатації захищеної мережі, а також від кількості мережевих інтерфейсів та інших характеристик використовуваних брандмауерів. Широко використовуються такі схеми підключення брандмауера:

- схеми захисту мережі з використанням екрануючого маршрутизатора;
- схеми єдиного захисту локальної мережі;
- схеми з захищеними закритими і незахищеними відкритими підмережами;
- схеми з роздільним захистом замкнутої і відкритої підмереж.

Схема захисту за допомогою екрануючого екрану

Пакетний брандмауер є найбільш поширеним і простим у реалізації. Він складається з екрануючого маршрутизатора, розташованого між захищеною мережею і потенційно ворожою відкритою зовнішньою мережею (рис.). Екрануючий маршрутизатор (пакетний фільтр) налаштований на блокування або фільтрацію вхідних і вихідних пакетів на основі аналізу їх адрес і портів.

Брандмауери на основі фільтрації пакетів мають ті ж недоліки, що і екрануючі маршрутизатори, і ці недоліки стають більш вираженими в міру того, як вимоги до безпеки захищеної мережі стають більш жорсткими. Відзначимо деякі з них:

- складність правил фільтрації, в деяких випадках комбінація цих правил може стати некерованою;
- неможливість повноцінно протестувати правила фільтрації, що призводить до того, що мережа стає вразливою до неперевірених атак.
- практично немає можливості реєстрації подій, що ускладнює для адміністратора визначення того, чи був маршрутизатор атакований і скомпрометований.

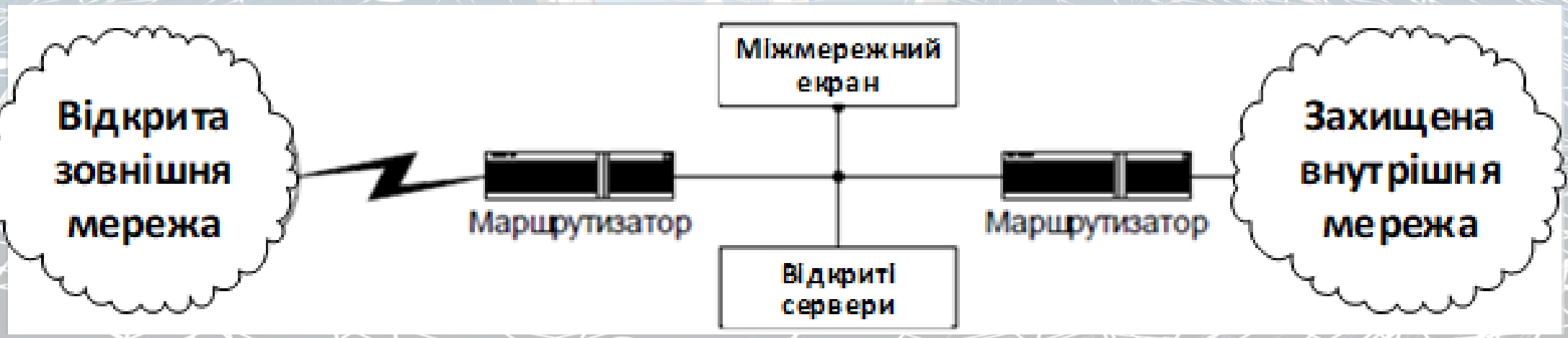


Схеми підключення брандмауерів з безліччю мережевих інтерфейсів

Схеми захисту з брандмауерами з єдиним мережевим інтерфейсом (рис.) недостатньо ефективні як з точки зору безпеки, так і з точки зору зручності налаштування. Вони фізично не розрізняють внутрішні та зовнішні мережі, і, відповідно, не можуть забезпечити надійний захист міжмережевих взаємодій.

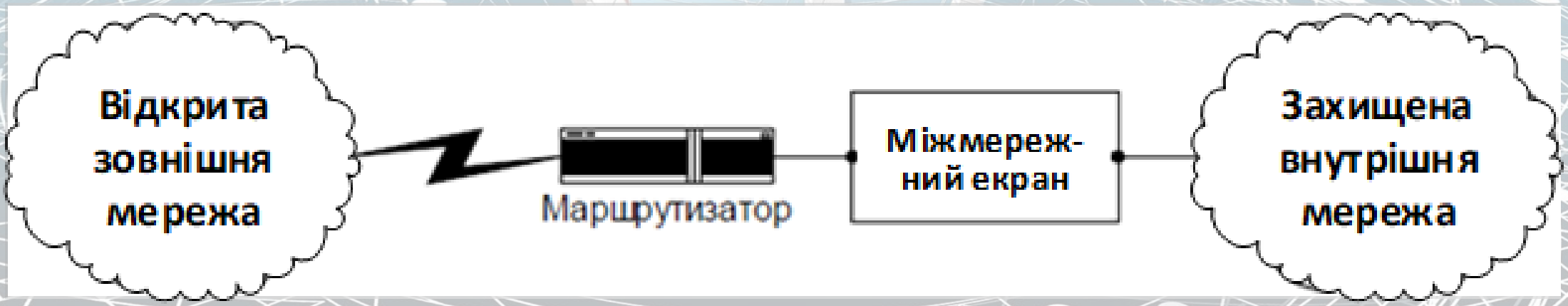
Серед безлічі можливих схем підключення КП можна виділити наступні:

- схема єдиного захисту локальної мережі;
- діаграма з захищеними закритими і незахищеними відкритими підмережами;
- схема з роздільним захистом закритої і відкритої підмереж.



Єдина схема захисту локальної мережі.

- Дана схема є найпростішим рішенням (рис.), при якому брандмауер повністю екранує локальну мережу від потенційно ворожої зовнішньої мережі. Між роутером і брандмауером є тільки один шлях, по якому йде весь трафік. У цій редакції Мінекономіки реалізує політику безпеки, засновану на принципі «все, що явно не дозволено, заборонено»; При цьому користувач має доступ не до всіх сервісів, крім тих, для яких визначені відповідні дозволи.
- Відкриті сервери, що входять до складу локальної мережі, також будуть захищені брандмауером. Однак об'єднання серверів, доступних із зовнішньої мережі, разом з іншими ресурсами захищеної локальної мережі значно знижує безпеку міжмережевих взаємодій.



Діаграма із захищеними закритими та незахищеними відкритими підмережами

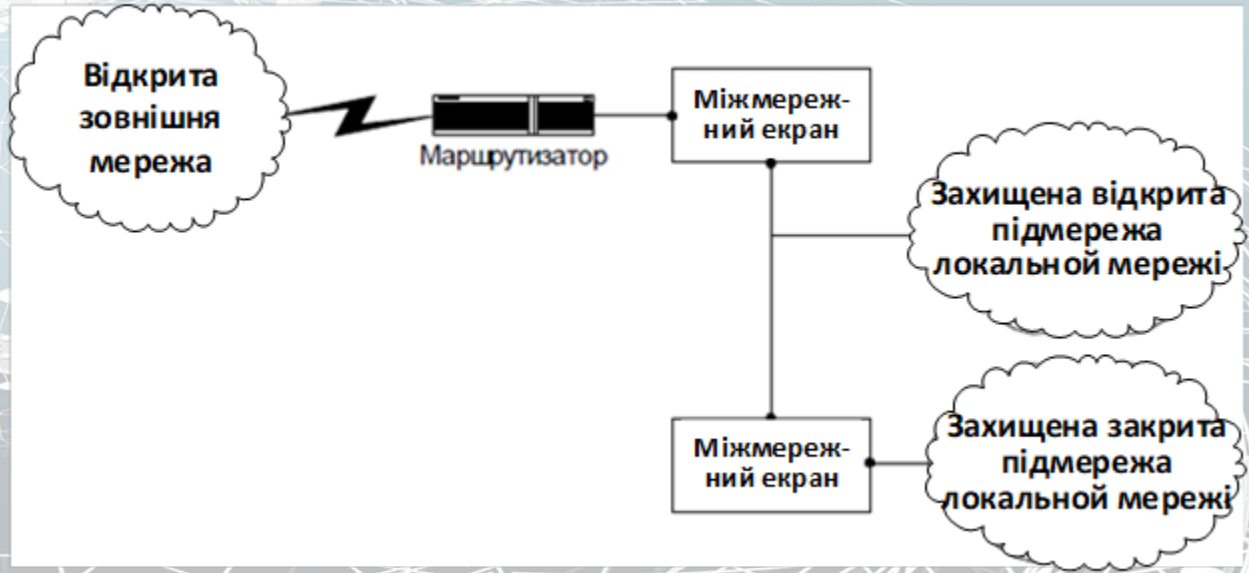
- Якщо в локальній мережі є відкриті сервери загального користування, то їх доцільно перенести як відкриту підмережу перед брандмауером (рис.). Цей метод має більш високу безпеку закритої частини локальної мережі, але забезпечує знижену безпеку для відкритих серверів, розташованих перед брандмауером.
- Схему підключення брандмауера з захищеними закритими і незахищеними відкритими підмережами доцільно використовувати тільки в тому випадку, якщо вимоги до безпеки відкритої підмережі не високі.



Схеми з роздільним захистом закритої і відкритої підмереж

- Така схема може бути побудована на базі одного брандмауера з трьома мережевими інтерфейсами (рис. лівопуч) або на базі двох міжмережевих екранів з двома мережевими інтерфейсами (рис. праворуч). В обох випадках доступ до відкритої і закритої підмереж локальної мережі можливий тільки через брандмауер. Однак доступ до загальнодоступної підмережі не дозволяє отримати доступ до приватної підмережі.
- З цих двох схем більший ступінь безпеки міжмережевих взаємодій забезпечує схема з двома брандмауерами, кожен з яких утворює окремий ешелон захисту для закритої підмережі. Захищена загальнодоступна підмережа тут виступає в ролі екрануючої підмережі.





Персональні та розподілені брандмауери

- Для індивідуальних користувачів представляє інтерес технологія персонального брандмауера. В цьому випадку брандмауер встановлюється на захищений персональний комп'ютер. Такий брандмауер, званий персональним брандмауером або системою брандмауерів, відстежує весь вхідний і вихідний трафік незалежно від усіх інших систем захисту. За рахунок екранування окремо взятого комп'ютера забезпечується доступність мережевих служб, але при цьому знижується навантаження, викликане зовнішньою активністю. В результаті знижується вразливість внутрішніх служб захищеного таким чином комп'ютера, так як сторонній зловмисник повинен спочатку проникнути на екран, де особливо ретельно і жорстко налаштовані засоби захисту. Для захисту робочого місця користувача необхідно мати, крім персонального брандмауера, антивірусне програмне забезпечення з актуальними сигнатурами, захист доступу до корпоративної мережі через VPN.
- Розподілений брандмауер – це централізовано керований набір міні-брандмауерів, які захищають окремі комп'ютери в мережі. При побудові розподілених брандмауерів системи їх функціональні компоненти розподіляються між вузлами мережі і можуть мати різне призначення. При виявленні підозрілих ознак, схожих на атаку, керуючі модулі розподіленого брандмауера можуть адаптивно змінювати конфігурацію, склад і розташування компонентів.

Архітектура міжмережевих екранів

Особливості міжмережевих екранів:

- Трафік ззовні всередину і навпаки повинен проходити через брандмауер.
- Трафік дозволений (або ні) на основі політики, що застосовується на брандмауері.
- Очікується, що МЕ не застрахований від проникнення. Брандмауери повинні бути висококваліфікованими пристроями із захищеними операційними системами.

Політики МЕ щодо трафіку визначається на основі:

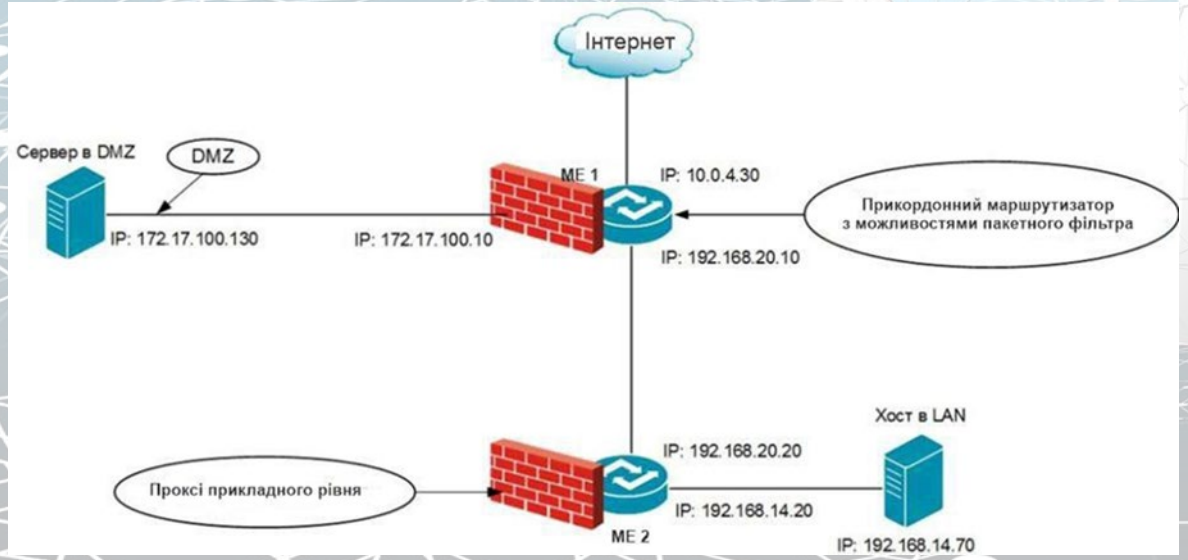
- Діапазону IP-адрес (явно дозволяти або забороняти);
- Мережевих протоколів;
- Програм що діють в мережі;
- Типу вмісту трафіку;
- Спрямованості трафіку (вхідний чи вихідний)

Особливості, які використовують МЕ для фільтрації трафіку:

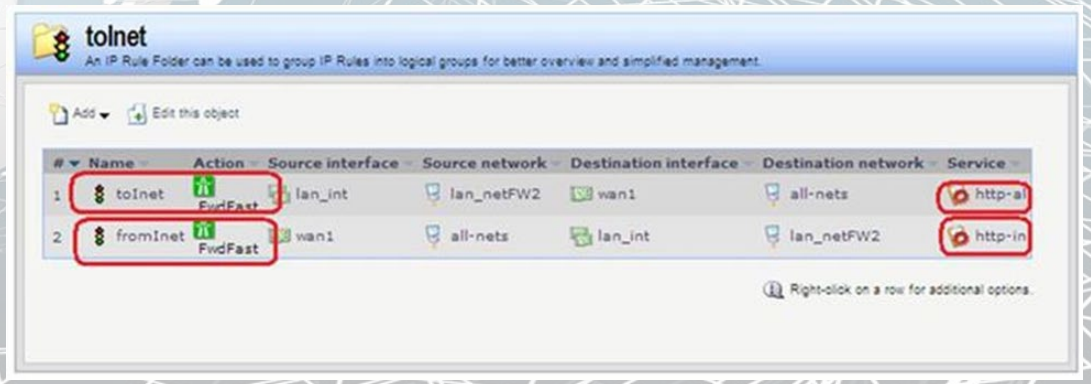
- IP адреса й значення полів протоколів - цей тип фільтрації використовується пакетним фільтром та брандмауерами, що перевіряють стан. Зазвичай використовується для обмеження доступу до певних послуг.
- Прикладний протокол - цей тип фільтрації використовується шлюзом на рівні додатків, який ретранслює та контролює обмін інформацією для конкретних прикладних протоколів.
- Ідентифікатор користувача - зазвичай для внутрішніх користувачів, які ідентифікують себе за допомогою певної форми технології безпечної автентифікації.
- Мережева активність - керує доступом на основі таких міркувань, як час або запит, швидкість запитів або інші схеми діяльності.

Схема розташування пакетного фільтру в комп'ютерній мережі

На рисунку показана топологія мережі, в якій прикордонний маршрутизатор з можливостями пакетного фільтра використовується як перша лінія оборони. Маршрутизатор приймає пакети від сумнівної мережі, наприклад, Інтернет, виконує контроль доступу у відповідності зі своєю політикою, наприклад, блокує SNMP, дозволяє HTTP і т.п. Потім він передає пакети могутнішому міжмережевому екрану для подальшого керування доступом і фільтрування даних на більш високих рівнях стека протоколів. На рисунку також показана проміжна мережа між прикордонним маршрутизатором і внутрішнім міжмережевим екраном, що називається DMZ-мережею







Пакетні фільтри з аналізом стану

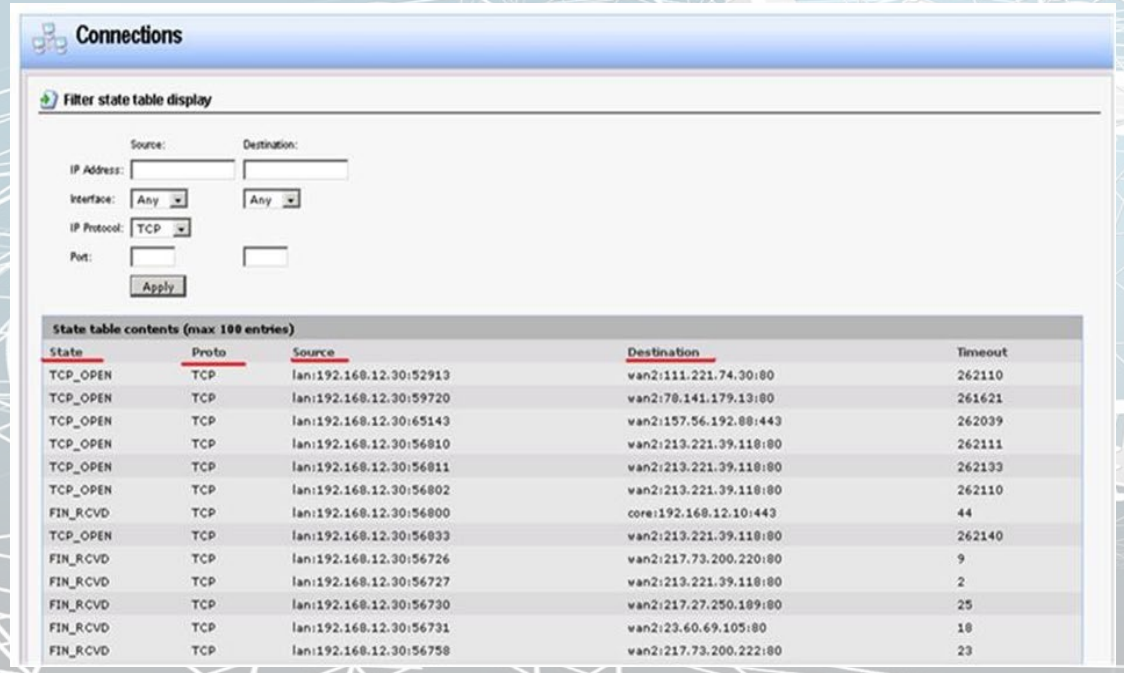
Аналіз стану додає можливість відстеження стану з'єднання й блокування пакетів, які не відповідають очікуваному стану. Для цього виконується аналіз даних транспортного рівня. У TCP-протоколі існують три основні стани – з'єднання: встановлюється, використовується й завершується.

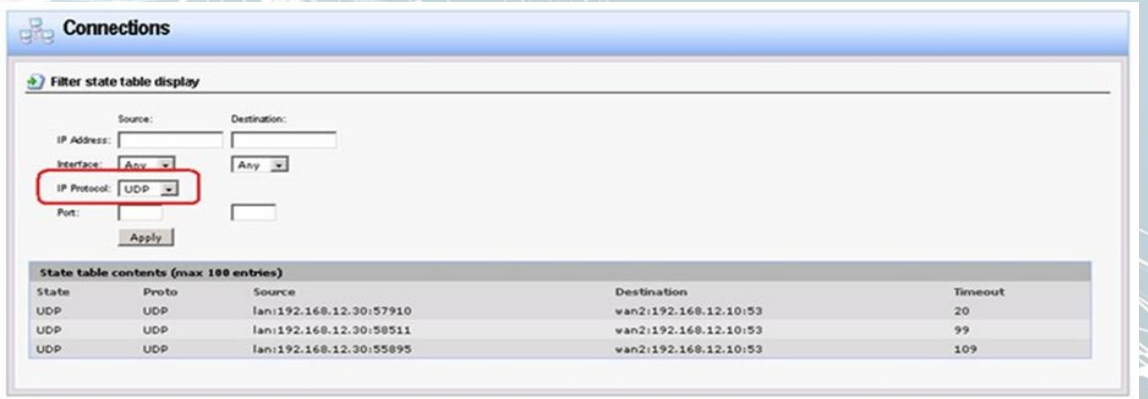
Переваги міжмережевих екранів з аналізом стану:

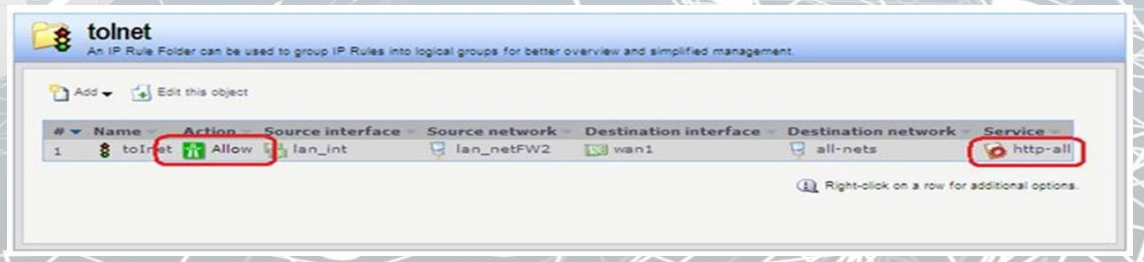
- дозволяють проходження пакетів тільки для встановлених з'єднань;
- прозорі для клієнтів і серверів, так як не розривають TCP- з'єднання.

Недоліки міжмережевих екранів з аналізом стану:

- Реально використовуються тільки в мережевій інфраструктурі TCP/IP. Хоча треба відзначити, що міжмережеві екрани з аналізом стану можна реалізувати в інших мережевих протоколах так як й пакетні фільтри.







Міжмережеві екрани та Проксі-шлюзи прикладного рівня

Міжмережеві екрани прикладного рівня доступні для багатьох протоколів, включаючи HTTP, БД (SQL), поштові (SMTP, POP, IMAP), VoIP і XML.

Переваги:

- має можливість виконувати аутентифікацію користувача;
- менш уразливий для атак підробки адреси;
- мають більше можливостей аналізувати весь мережевий пакет, а не тільки мережеві адреси і номери портів;
- створюють більш докладні логи;

Недоліки:

- витрачається багато часу на аналіз кожного пакета;
- обробляють обмежену кількість мережевих додатків і протоколів і не можуть автоматично підтримувати нові мережеві додатки та протоколи.

Комбінують управління доступом на нижньому рівні з функціональністю верхнього рівня. Вони мають проксі-агента, що діє як посередник між двома хостами, які хочуть взаємодіяти один з одним, і ніколи не допускає прямої взаємодії між ними. Результатом успішної спроби встановлення з'єднання є створення двох окремих з'єднань - одне між клієнтом і проксі-агентом, інше - між проксі-агентом і реальним сервером.

Переваги:

- проксі має можливість запросити аутентифікацію користувача;
- є менш уразливими для атак підробки адреси;
- більше можливостей аналізувати весь мережевий пакет, а не тільки мережеві адреси і номери портів;
- створюють більш докладні логи;

Недоліки:

- витрачає багато часу на аналіз кожного пакета;
- обробляють обмежену кількість мережевих додатків і протоколів і не можуть автоматично підтримувати нові мережеві додатки та протоколи.

Виділені проксі-сервера

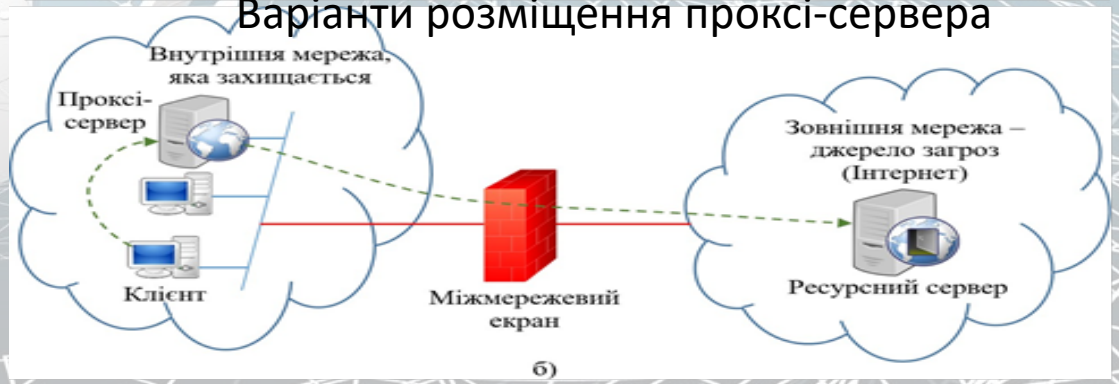
Проксі-сервер (Proxy Server) – це особливий тип додатку, який виконує функції посередника між клієнтськими і серверними частинами розподілених мережевих додатків, причому передбачається, що клієнти належать до внутрішньої (що захищається) мережі, а сервери – до зовнішньої (потенційно небезпечної) мережі.

Схема розташування виділеного проксі серверу в комп'ютерній мережі





Варіанти розміщення проксі-сервера



Функції проксі-серверів

Найчастіше проксі-сервери застосовуються для наступних цілей:

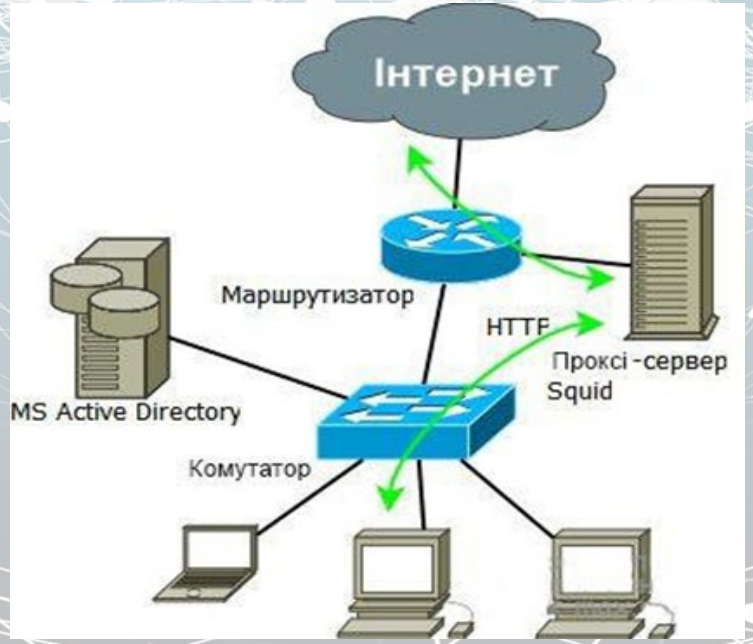
- Забезпечення доступу з комп'ютерів локальної мережі в Інтернет.
- Кешування даних: якщо часто відбуваються звернення до одних і тих ж зовнішніх ресурсів, то можна тримати їх копію на проксі-сервері і видавати по запиту, знижуючи тим самим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом запитаної інформації.
- Стиснення даних: проксі-сервер завантажує інформацію з Інтернету і передає інформацію кінцевому користувачеві в стислому вигляді. Такі проксі- сервери використовуються в основному з метою економії зовнішнього трафіку.
- Захист локальної мережі від зовнішнього доступу: наприклад, можна налаштувати проксі-сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі (вони побачать тільки проксі-сервер).
- Обмеження доступу з локальної мережі до зовнішньої: наприклад, можна заборонити доступ до певних веб-сайтів, обмежити використання Інтернету якимось локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу і віруси.
- Анонімізація доступу до різних ресурсів. Проксі-сервер може приховувати відомості про джерело запиту або користувача. У такому випадку цільовий сервер бачить лише інформацію про проксі-сервер, наприклад, IP- адресу, але не має можливості визначити дійсне джерело запиту. Існують також проксі-сервери, які передають цільовому серверу помилкову інформацію про справжнього користувача.
- Багато проксі-серверів використовуються для кількох цілей одночасно. Деякі проксі-сервери обмежують роботу декількома портами: 80 (HTTP), 443 (шифровані з'єднання HTTPS), 20,21 (FTP).

Типи проксі-серверів (1)

Проксі-сервер може працювати в наступних трьох основних режимах:

- Прозорий режим
- Аутентифікуючий режим
- Зворотній проксі-сервер







Типи проксі-серверів (2)

Крім зазначених типів міжмережевих екранів також виділяють наступні:

- Кінцеві точки VPN. Для шифрування певного трафіку між захищеними мережами. Двома найбільш часто використовуваними архітектурами VPN є шлюз-шлюз і хост-шлюз.
- Гібридні технології міжмережевих екранів. Багато міжмережевих екранів поєднують функціональності кількох різних типів міжмережевих екранів. Наприклад, багато виробників прикладних проксі реалізують базову функціональність пакетних фільтрів.
- Додаткові можливості керування доступом в мережу. Необхідність вирішення вхідних з'єднань не тільки після виконання аутентифікації віддаленого користувача, але і перевірки параметрів безпеки для користувача комп'ютера.

Фаєрволи з функцією NAT

NAT (Network Address Translation – перетворення мережевих адрес) є методом, за допомогою якого виконується перетворення IP-адрес при пересиланні пакета з однієї області адрес в іншу, забезпечуючи прозору маршрутизацію між кінцевими хостами.

Існує 3 базових концепції трансляції адрес: статична (Static Network Address Translation), динамічна (Dynamic Network Address Translation), маскарад (NAPT, NAT Overload, PAT).

- Статичний NAT - Відображає незареєстровану IP-адресу на зареєстровану IP-адресу на підставі один до одного. Особливо корисно, коли пристрій повинен бути доступним ззовні мережі.
- Динамічний NAT - Відображає незареєстровану IP-адресу на зареєстровану адресу з групи зареєстрованих IP-адрес. Динамічний NAT також встановлює безпосереднє відображення між незареєстрованою та зареєстрованою адресами, але відображення може змінюватися в залежності від зареєстрованої адреси, доступної в пулі адрес, під час комунікації.
- Перевантажений NAT (NAPT, NAT Overload, PAT, маскарадінг) - форма динамічного NAT, який відображає кілька незареєстрованих адрес в єдиний зареєстрований IP-адреса, скориставшись різними портами. Відомий також як PAT (Port Address Translation). При перевантаженні кожен комп'ютер в приватній мережі транслюється в ту же саму адресу, але з різним номером порту.

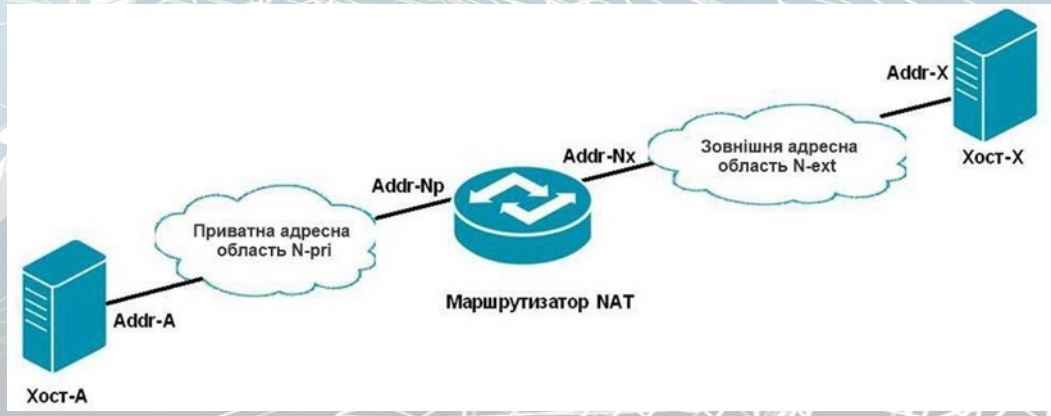


Схема розташування міжмережевого екрану з можливостями NAT

Традиційна технологія NAT

Технологія трансляції мережевих адрес має кілька різновидів, найбільш популярна з яких – традиційна технологія трансляції мережевих адрес – дозволяє вузлам з приватної мережі, прозорим для користувачів чином, отримувати доступ до вузлів зовнішніх мереж. В даному варіанті NAT вирішується проблема організації тільки тих сеансів зв’язку, які виходять з приватної мережі. Напрямок сеансу в даному випадку визначається положенням ініціатора: якщо обмін даними ініціюється додатком, що працює на вузлі внутрішньої мережі, то сеанс називається вихідним, незважаючи на те що в його рамках в мережу можуть надходити дані ззовні.

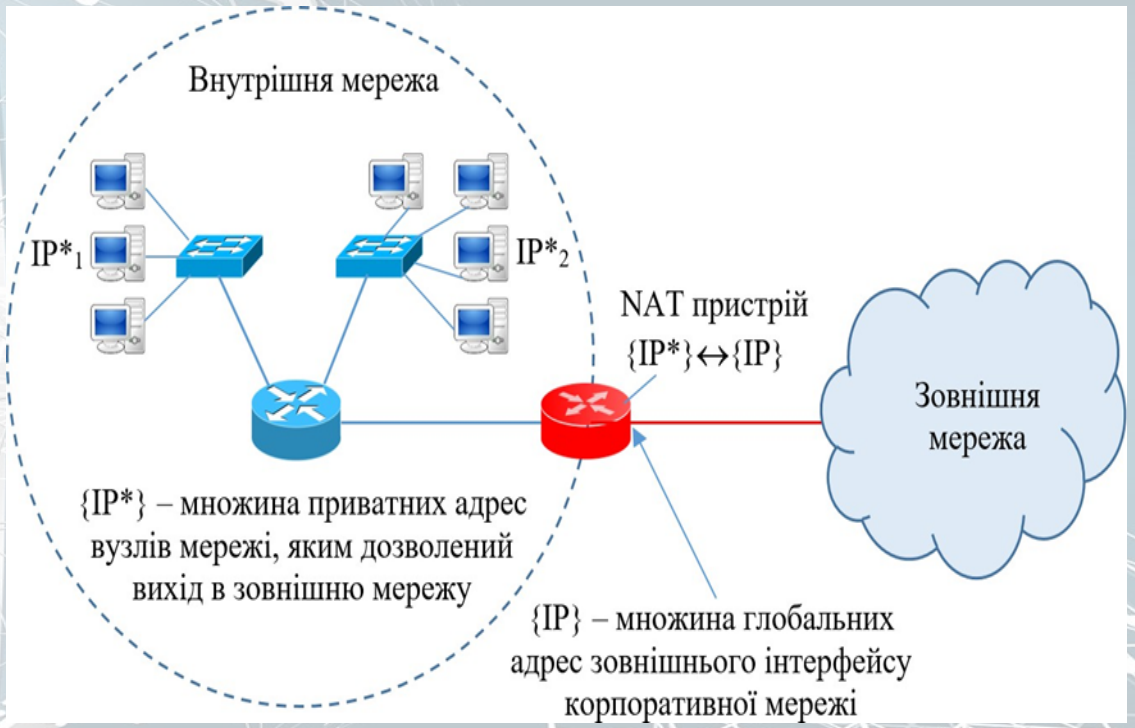
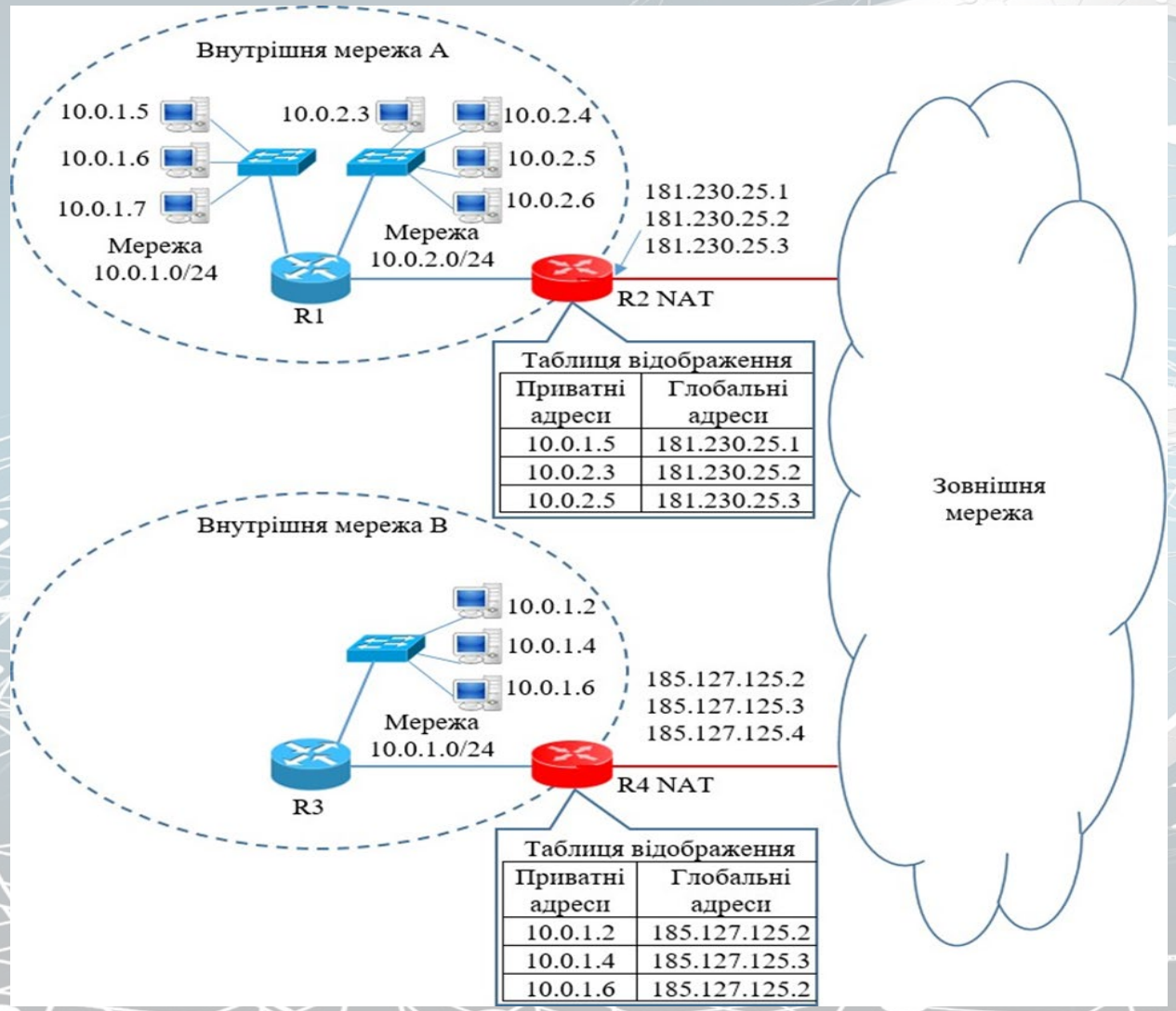


Схема дії традиційної технології NAT

Трансляція мережевих адрес і портів

Базова трансляція мережевих адрес



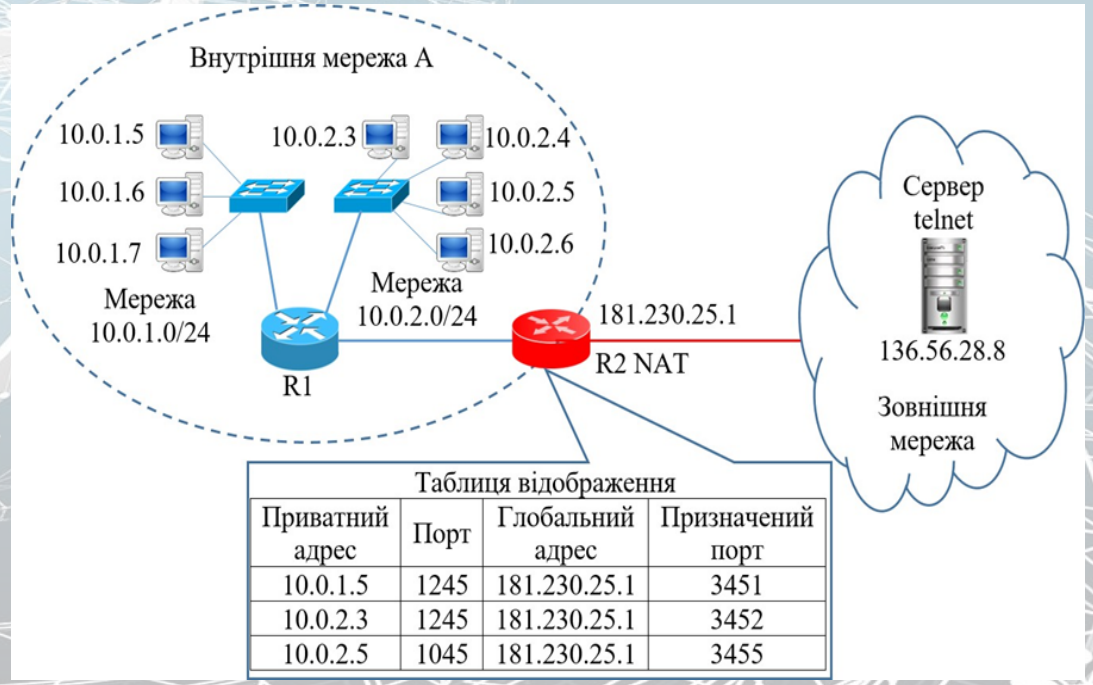
Таблиця відображення

Приватні адреси	Глобальні адреси
10.0.1.5	181.230.25.1
10.0.2.3	181.230.25.2
10.0.2.5	181.230.25.3

Таблиця відображення

Приватні адреси	Глобальні адреси
10.0.1.2	185.127.125.2
10.0.1.4	185.127.125.3
10.0.1.6	185.127.125.2

Трансляція мережевих адрес і портів



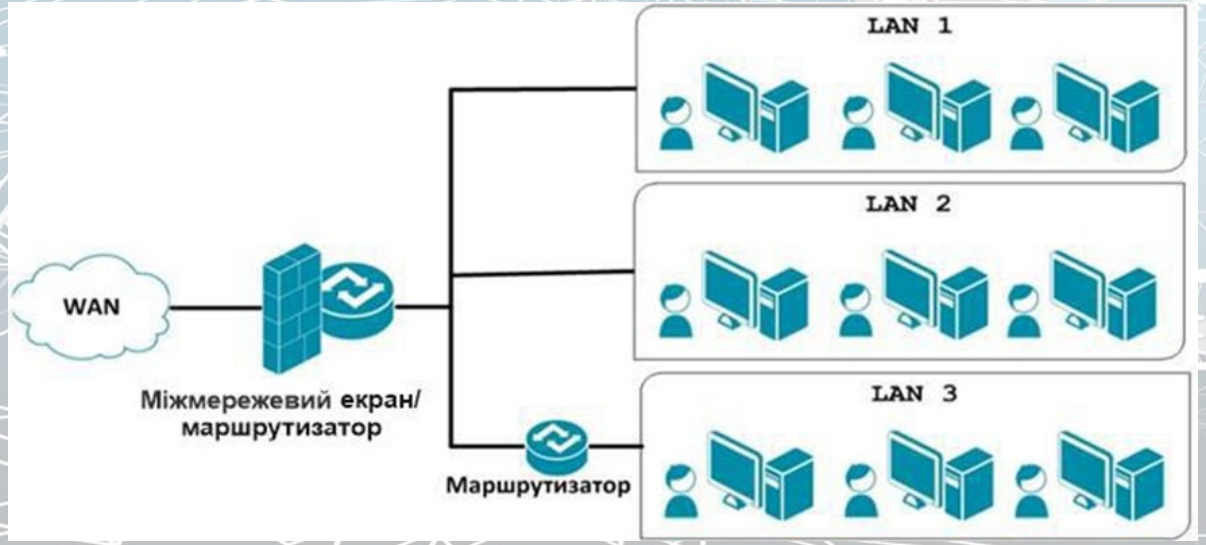
Таблиця відображення

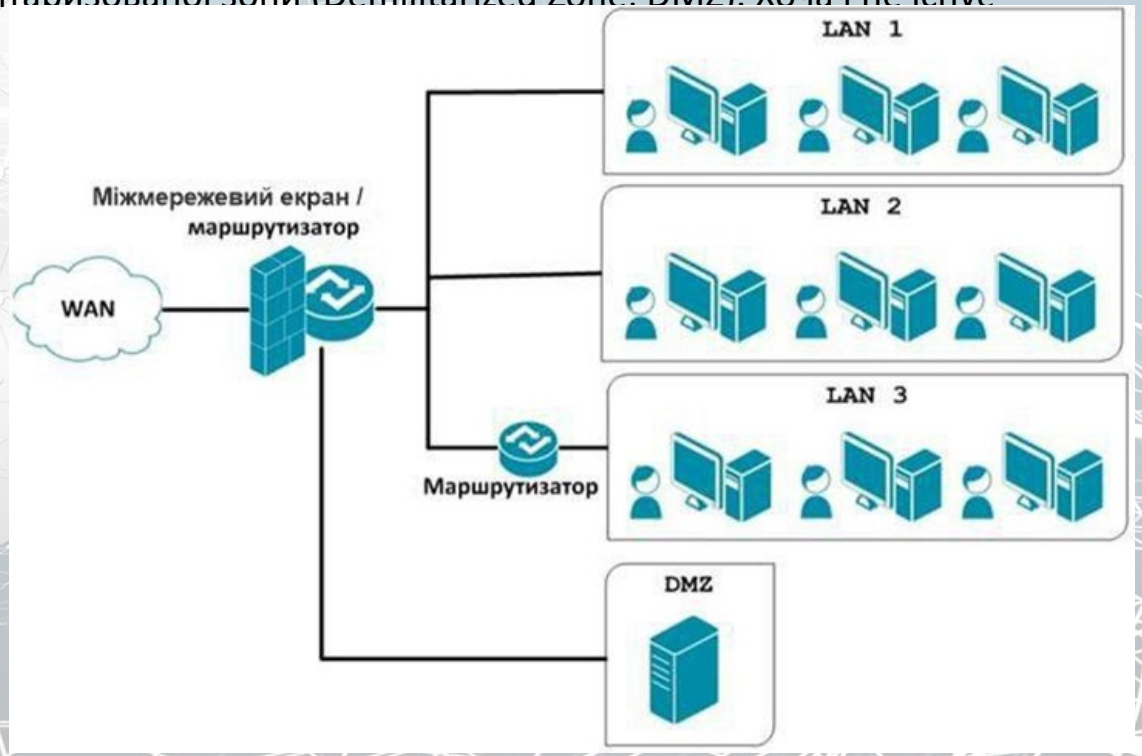
Приватний адрес	Порт	Глобальний адрес	Призначений порт
10.0.1.5	1245	181.230.25.1	3451
10.0.2.3	1245	181.230.25.1	3452
10.0.2.5	1045	181.230.25.1	3455

Топологія мережі при використанні міжмережевих екранів

Так як початкової функцією брандмауера є запобігання небажаного вхідного трафіку в мережу (і в деяких випадках вихідного), міжмережеві екрани повинні бути розташовані в точках входу на логічних межах мережі. Зазвичай це означає, що міжмережевий екран є вузлом, в якому мережевий трафік розділяється на кілька потоків, або збирається разом в єдиний потік (рис.ліворуч).

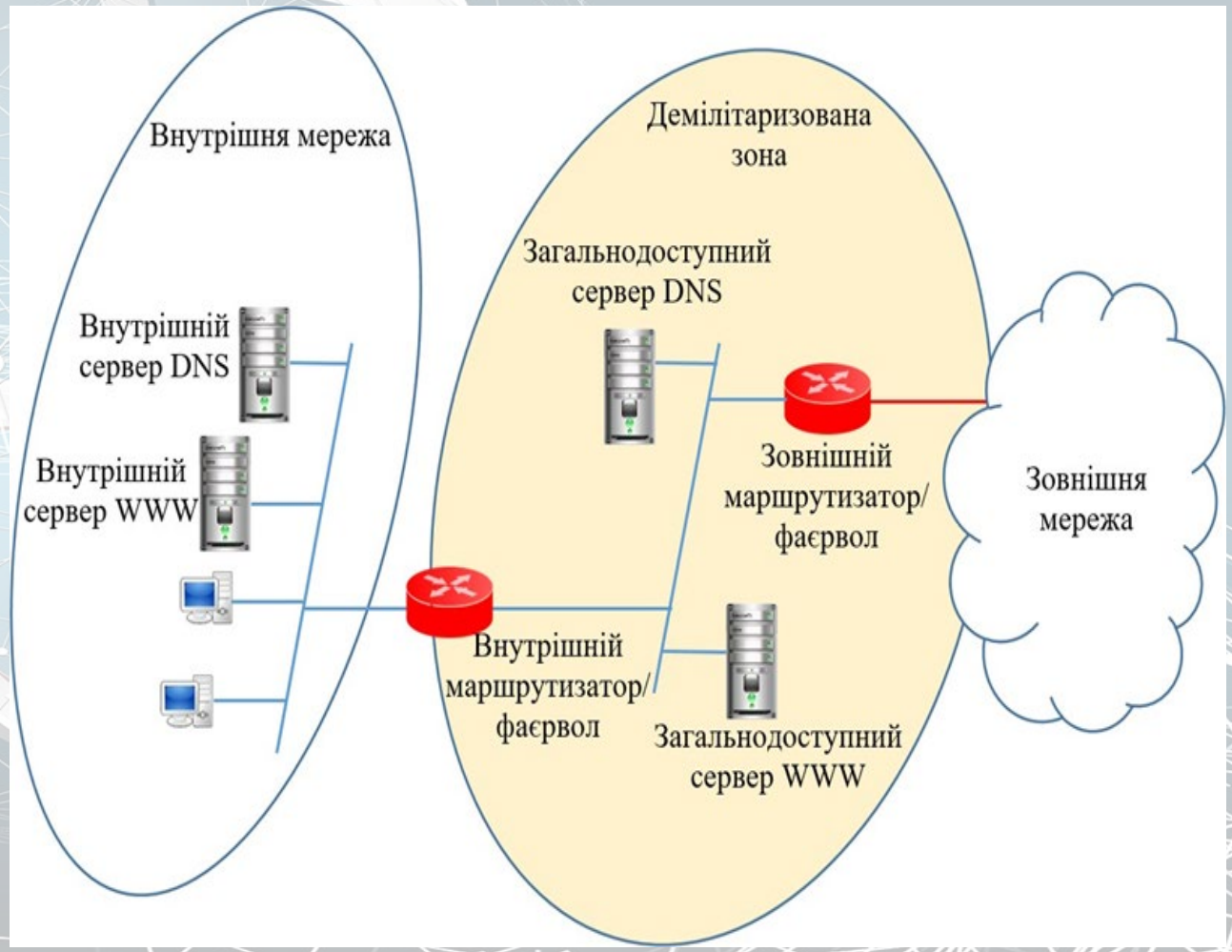
Ресурси корпоративної мережі, до яких звертаються зовнішні користувачі, безумовно, становлять відносно заходів безпеки окрему групу. Це такі ресурси, як поштовий сервер, веб-сервер, DNS- сервер. Звичною практикою є виділення таких ресурсів в окрему групу і розміщення їх в підмережі, яка отримала назву демілітаризованої зони (Demilitarized Zone, DMZ). Хоча і не існує єдиного визначення для DMZ, зазвичай вони є інтерфейсами в міжмережевому екрані, для яких можливо задавати правила маршрутизації, і аналогічні інтерфейсам, що розташовані на захищеній стороні брандмауера (рис.праворуч)





Використання демілітаризованої зони

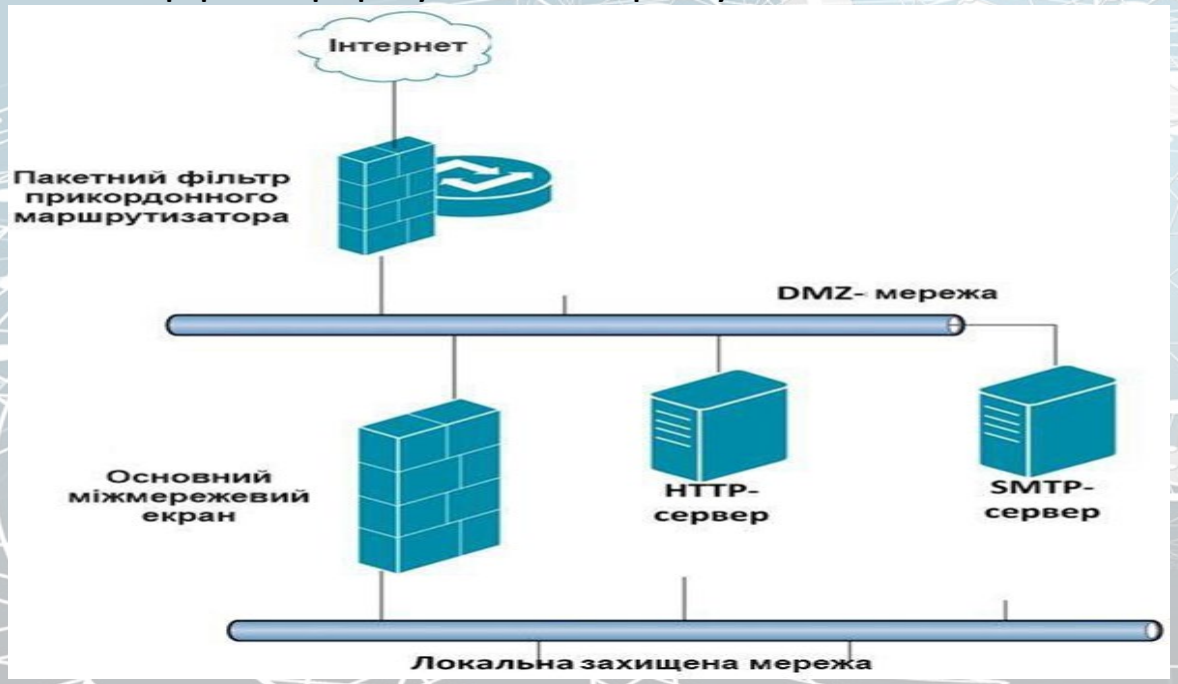
- У цій мережі на межі захисту встановлено два маршрутизатора, між якими розташовується демілітаризована зона. Маршрутизатор тут відіграють роль фаєрволів мережевого рівня. В даному випадку мережа DMZ є також мережею периметра, так як тільки вона з’єднує внутрішню мережу підприємства з зовнішніми мережами.
- В мережі DMZ розташовані два загальнодоступних сервера – зовнішній DNS-сервер і зовнішній веб-сервер підприємства. У цій зоні можуть бути розміщені також проксі-сервери.



DMZ-мережі (1)

DMZ-мережі призначені для розташування систем і ресурсів, які не повинні бути розміщені у внутрішніх захищених мережах, але до яких необхідно отримати доступ або тільки ззовні, або тільки зсередини, або і ззовні, і зсередини (рис. ліворуч). Причина в тому, що ніколи не можна гарантувати, що ці системи і ресурси не можуть бути зламані.

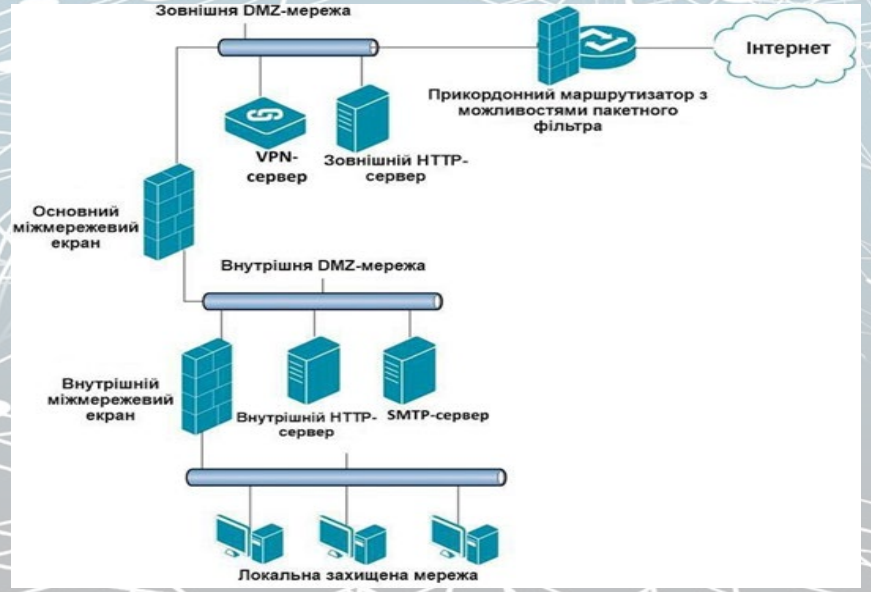
Однією з конфігурацій DMZ-мережі є так звана «service leg» конфігурація брандмауера (рис.праворуч). У цій конфігурації міжмережевий екран має як мінімум три мережевих інтерфейсу. Один мережевий інтерфейс з'єднується з інтернетом, інший з'єднується з внутрішньою мережею, третій мережевий інтерфейс формує DMZ-мережу.

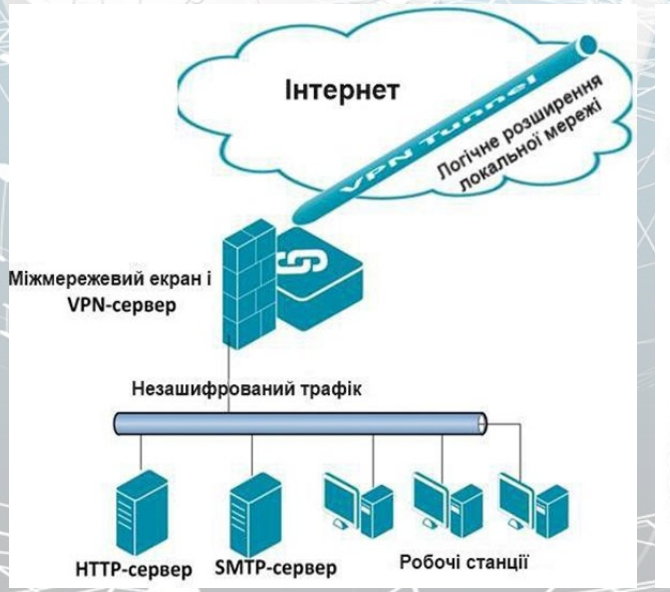


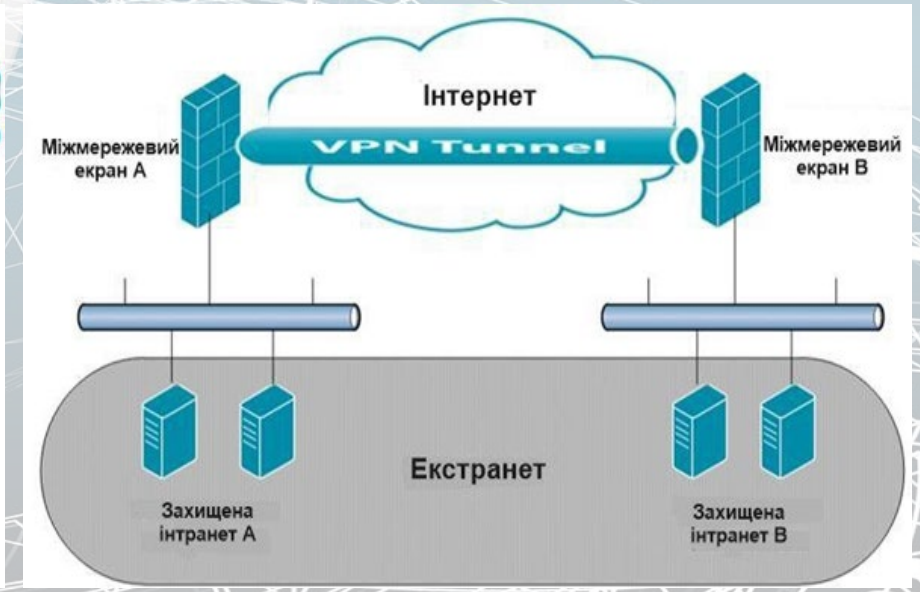


DMZ-мережі (2)

- У випадку оточення міжмережевого екрану двома DMZ-мережами (рис. ліворуч), прикордонний маршрутизатор буде фільтрувати пакети і забезпечувати захист серверів, перший міжмережевий екран буде забезпечувати управління доступом і захист серверів внутрішньої DMZ в разі, якщо зовнішні сервера атаковані.
- VPN застосовується для забезпечення безпечних мережевих з'єднань з використанням мереж, які не є довіреними системами. Наприклад, технологія VPN все частіше створюється для надання віддаленого доступу користувача до мереж організації через Інтернет (рис. посередині).
- Метою інтранет є представлення доступу до потенційно чутливої інформації віддаленим користувачам або організаціям, але при цьому забороняючи доступ всім іншим зовнішнім користувачам і системам (рис.праворуч).







Типи і використання списків контролю доступу (1)

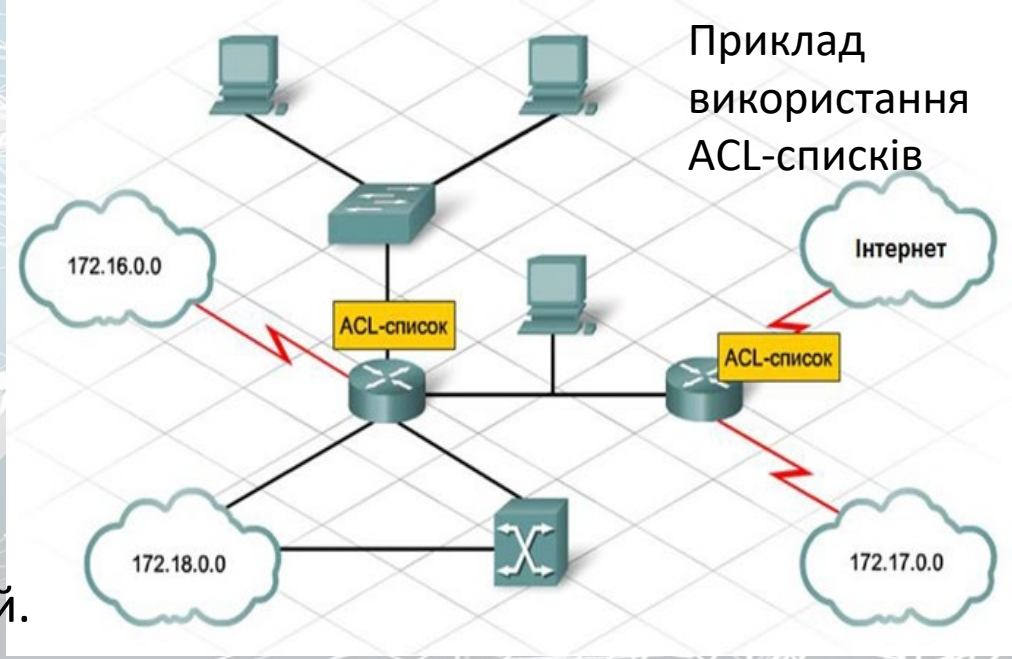
Одним з найбільш поширених способів фільтрації трафіку є використання списків контролю доступу (Access Control List, ACL). ACL-списки являють собою потужній інструмент для керування доступом як до сегмента мережі так і до зовнішніх стосовно сегмента ресурсів, з середини цього сегмента.

Основні функції ACL-списків включають в себе:

- фільтрування внутрішніх пакетів;
- захист внутрішньої мережі від несанкціонованого доступу;
- контроль доступу до портів віртуальних терміналів.

Використання ACL-списків може бути пов’язане з наступними потенційними проблемами:

- додаткове навантаження на маршрутизатор для перевірки всіх пакетів означає менший час на фактичну пересилку пакетів;
- погано організовані ACL-списки створюють більше навантаження на маршрутизатор і можуть порушити працездатність мережі;
- неправильно розміщені ACL-списки можуть блокувати допустимий трафік і дозволяти заборонений.



Приклад використання ACL-списків

Типи і використання списків контролю доступу (2)

Правила порівняння пакета зі списком доступу:

- Пакет завжди порівнюється з кожним рядком списку контролю доступу в порядку проходження рядків – спочатку виконується порівняння з рядком 1, потім з рядком 2 і т. д.
- Порівняння виконується доти, поки не буде виявлена відповідність пакета шаблону, що міститься в певному рядку. Після цього порівняння закінчується і пакет обробляється.
- Наприкінці кожного списку контролю доступу міститься неявна інструкція заборони всього трафіку – це означає, що, якщо пакет не задовольняє жодному із шаблонів ACL-списку, він відхиляється. Ця інструкція автоматично вставляється в кінець кожного ACL-списку, хоча і не присутня в ньому фізично.

При отриманні пакету на інтерфейс маршрутизатор перевіряє наступні параметри:

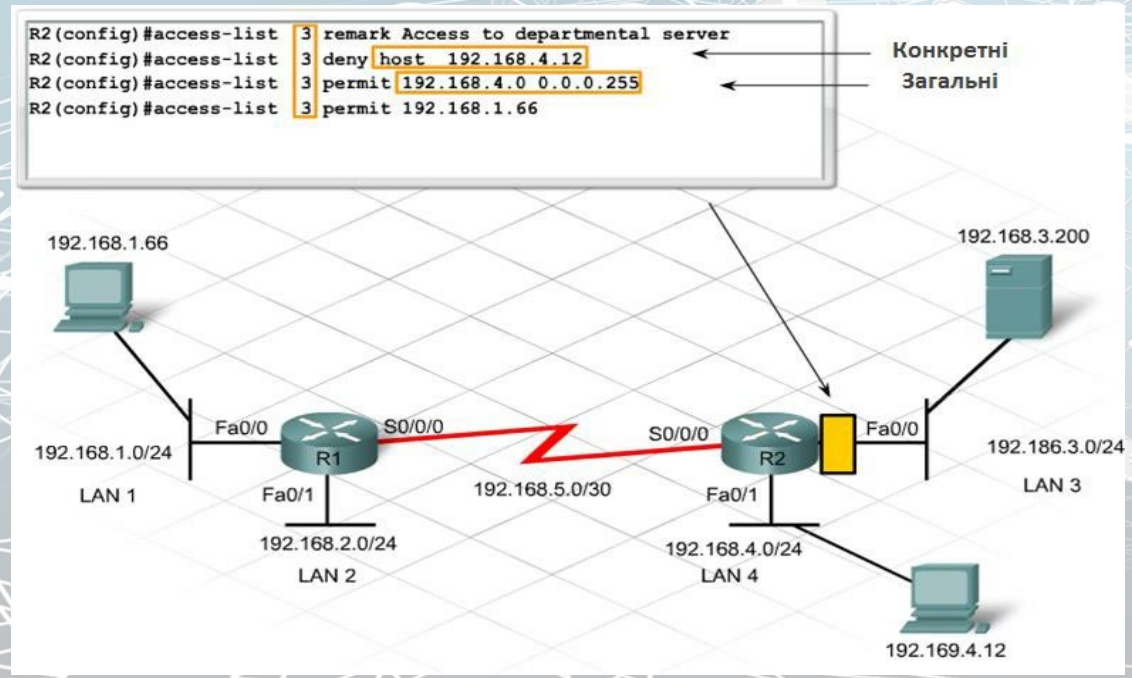
- наявність ACL-списку, пов’язаного з інтерфейсом;
- визначення типу ACL-списку (вхідний/вихідний);
- визначення відповідності трафіку дозволяючим або забороняючим умовам.

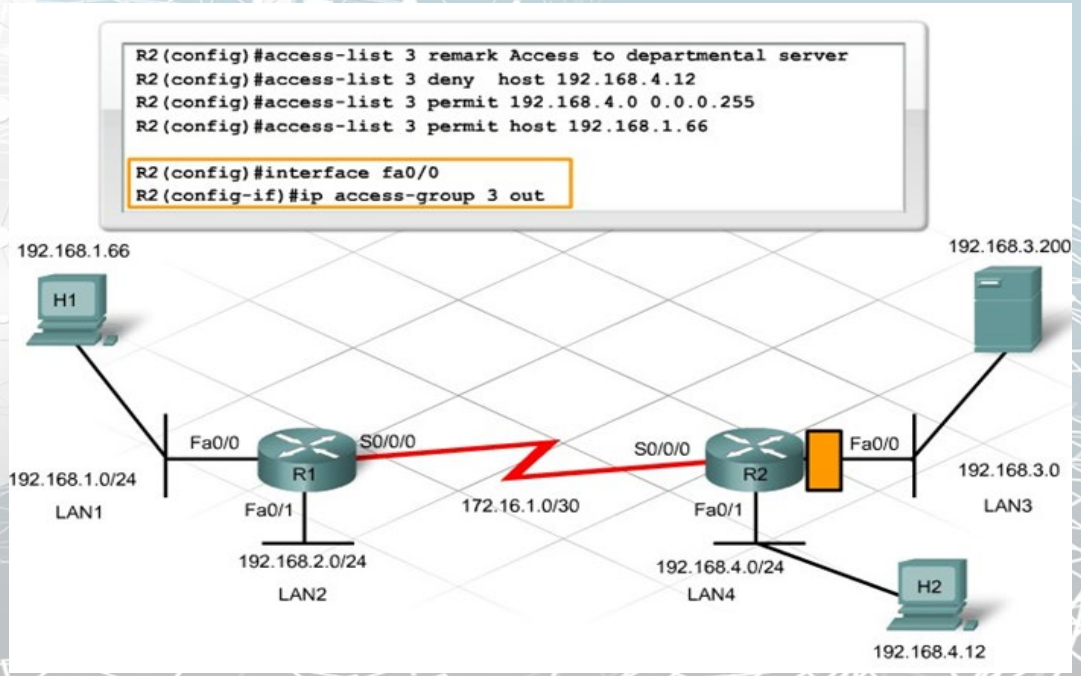
Існує три типи ACL-списків.

- Стандартні ACL-списки
- Розширені ACL-списки
- Іменовані ACL-списки

Стандартні списки контролю доступу

- На рис. ліворуч показано приклад використання стандартного ACL-списку. В даному прикладі дозволено доступ в мережу LAN 3 всім хостам з мережі LAN 4, окрім хоста 192.168.4.12, а також дозволено доступ хоста 192.168.1.66 з мережі LAN 1.
- Наступні команди дозволяють помістити список контролю доступу access- list 3 для інтерфейсу FastEthernet0/0 маршрутизатора R2 з фільтрацією вхідного трафіку (рис. праворуч)

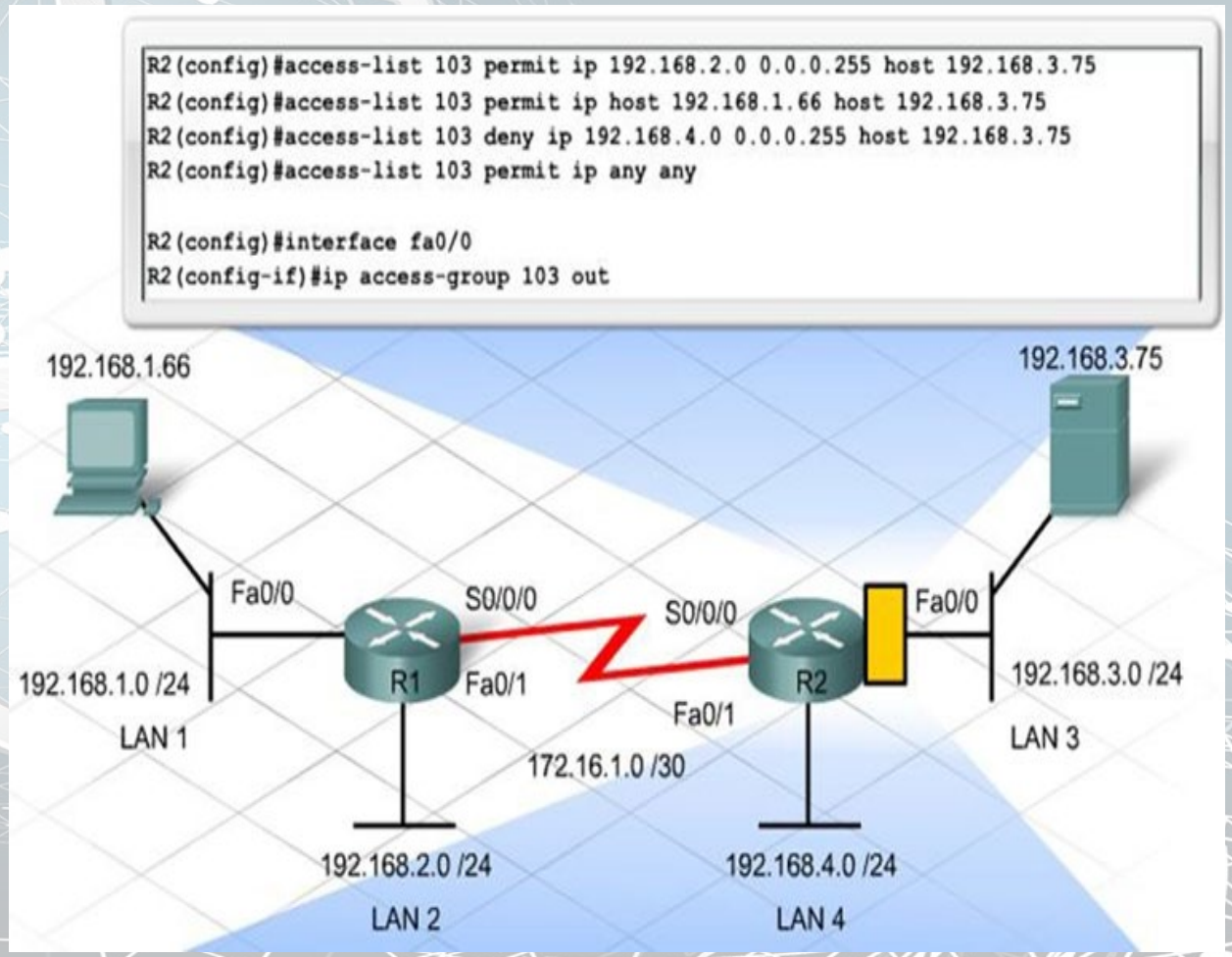




Розширені списки контролю доступу

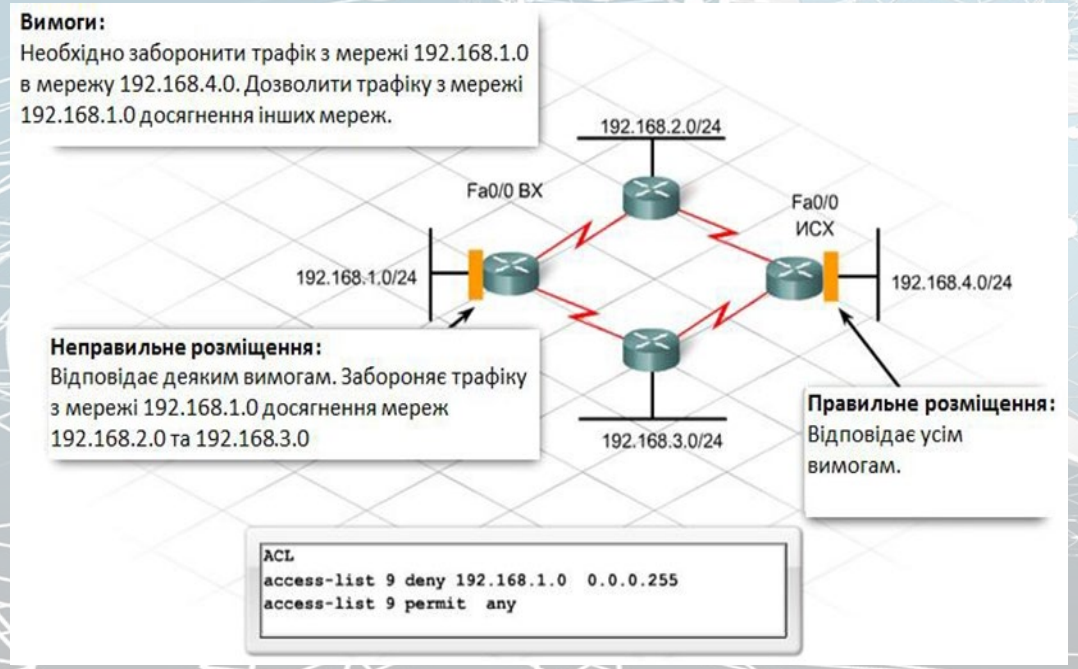
Функція розширених списків контролю доступу та ж, що й у стандартних списків, розходження полягає лише в критеріях фільтрації. Стандартні списки доступу дозволяють фільтрувати пакети тільки на основі їх вихідної адреси, у той час як розширені ACL-списки дозволяють застосовувати наступні критерії фільтрації:

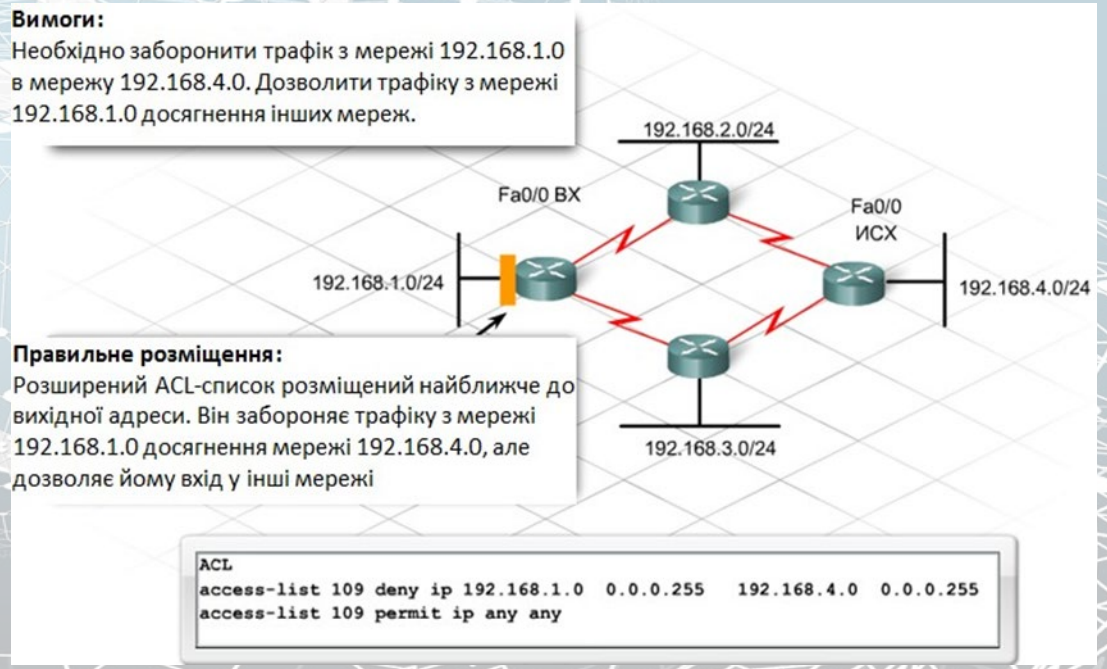
- вихідна адреса;
- адреса призначення;
- протокол (tcp, udp, icmp і т.д.)
- порт (www, dns, ftp і т.д.)



Розміщення стандартних і розширених списків контролю доступу

Вибір стандартного ACL-списку чи розширеного ACL-списку обумовлений поточними вимогами до фільтрації. Вибір типу ACL-списку може вплинути на гнучкість фільтрації, а також на продуктивність маршрутизатора і пропускну здатність мережі.





Моніторинг трафіку. Аналізатори протоколів

Моніторинг мережевого трафіку – це безперервний процес інструментального автоматизованого спостереження за окремими параметрами трафіку з метою перевірки дотримання SLA, планування мережі, а також запобігання негативних подій, таких як технічні аварії, загрози і атаки зловмисників.

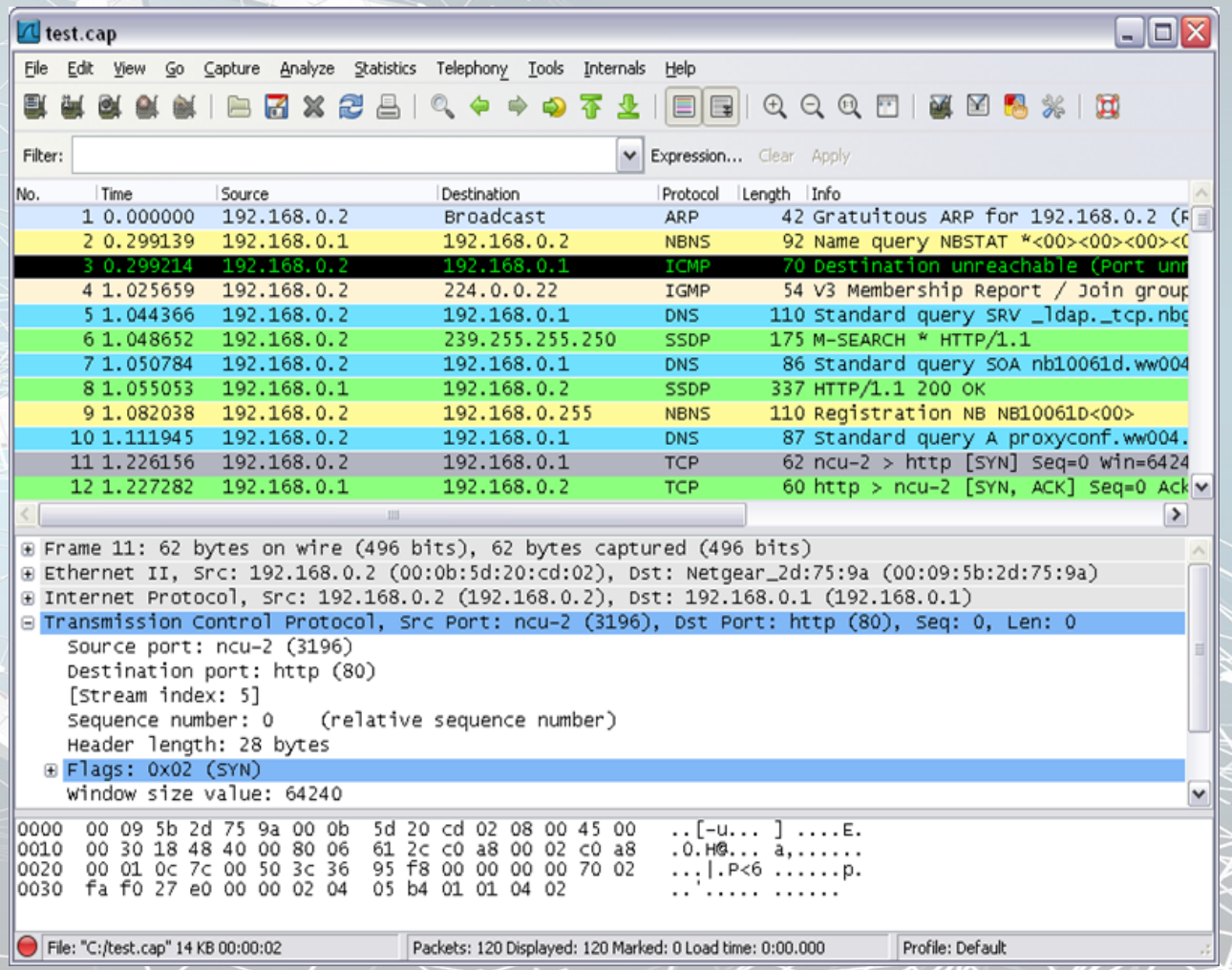
Основні засоби моніторингу мережевого трафіку наступні:

- аналізатори протоколів, або мережеві сніфери, дозволяють захоплювати трафік локальних мереж, представляти його в зручному для аналізу вигляді, але власне аналіз даних залишають адміністратору;
- маршрутизатори, що підтримують протокол NetFlow, збирають узагальнені дані про трафік глобальних мереж, передаючи його для аналізу програмним системам NetFlow, які автоматизують пошук атак і загроз;
- системи виявлення вторгнень (Intrusion Detection Systems, IDS) спеціалізуються на автоматичному розпізнаванні вторгнень і загроз в прослуховуючому трафіку локальних мереж.

Аналізатори протоколів

Аналізатори протоколів здатні на основі деяких заданих оператором логічних умов захоплювати окремі пакети і декодувати їх, тобто показувати в зручній для фахівця формі вкладеність пакетів протоколів різних рівнів один в одного з розшифровкою змісту полів кожного пакета. Аналізатори протоколів дозволяють користувачу виводити результати аналізу інтенсивності трафіку; отримувати миттєву і усереднену статистичну оцінку продуктивності мережі; задавати певні події і критичні ситуації для відстеження їх виникнення.

Аналізатор протоколів являє собою або самостійний спеціалізований пристрій, або персональний комп'ютер, зазвичай ноутбук, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням.

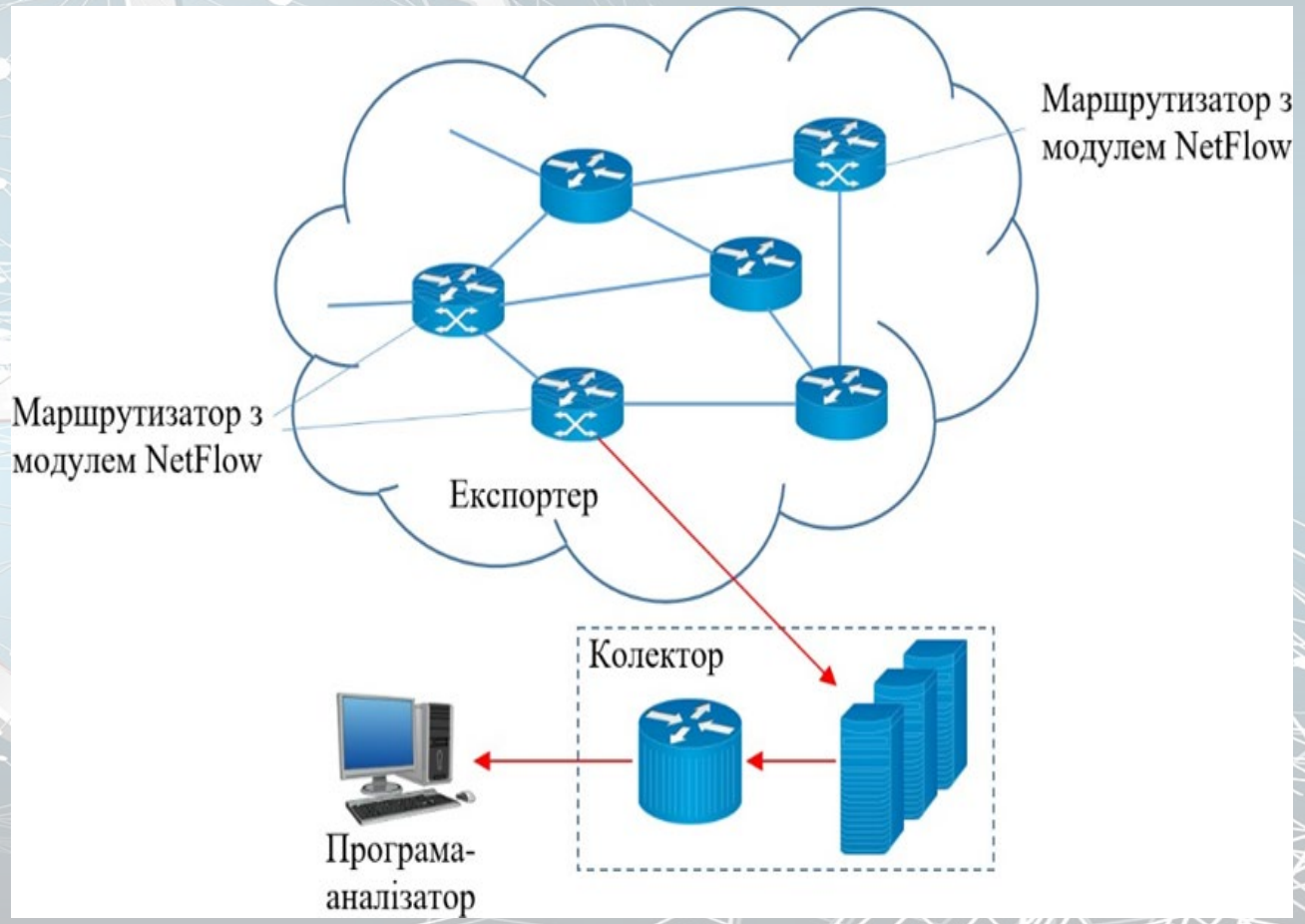


Система моніторингу NetFlow

Система моніторингу NetFlow сьогодні є основним засобом обліку та аналізу трафіку, який проходить через маршрутизатори та комутатори мережі. Мережеві вузли, які підтримують протокол NetFlow, не тільки виконують свою основну роботу – передачу пакетів відповідно до адреси призначення, а й збирають статистику про потоки даних, що проходять через них і періодично відправляють їх в колектори для зберігання і обробки такої інформації.

Типова система моніторингу на базі NetFlow включає наступні функціональні компоненти (рис.):

- Експортер потоку або сенсор
- Колектор
- Програма-аналізатор



Системи виявлення вторгнень

Система виявлення вторгнень (Intrusion Detection System, IDS) – це програмний або апаратний засіб, який виконує безперервне спостереження за мережевим трафіком і діяльністю суб'єктів системи з метою попередження, виявлення та протоколювання атак. На відміну від фаєрволів і проксі-серверів, які будують захист мережі виключно на основі аналізу мережевого трафіку, системи виявлення вторгнень враховують у своїй роботі різні підозрілі події, що відбуваються в системі.

Типова система IDS включає наступні функціональні елементи:

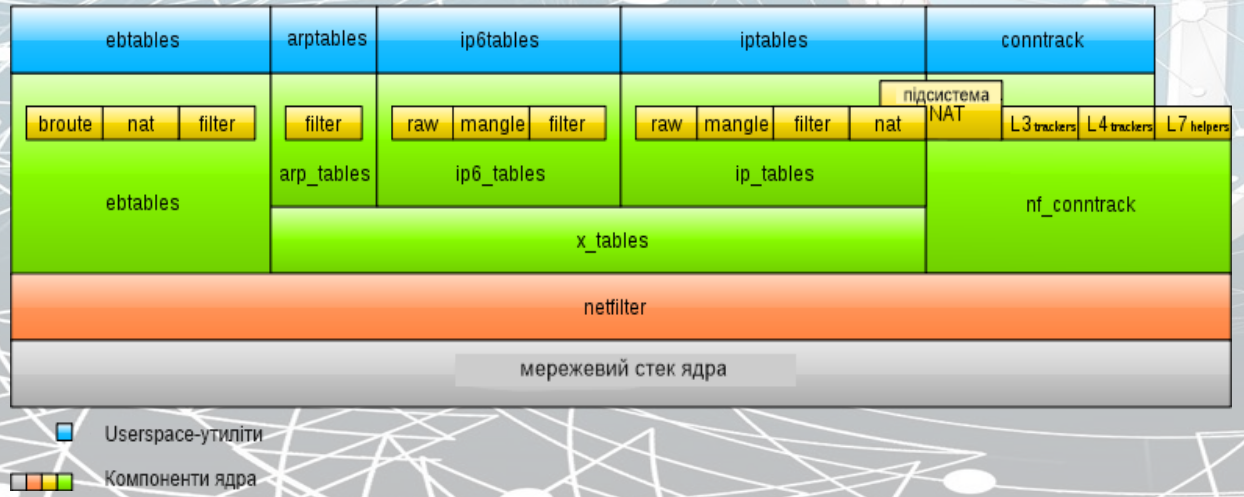
- джерела даних;
- давачі;
- аналізатор;
- адміністратор;
- оператор;
- менеджер.

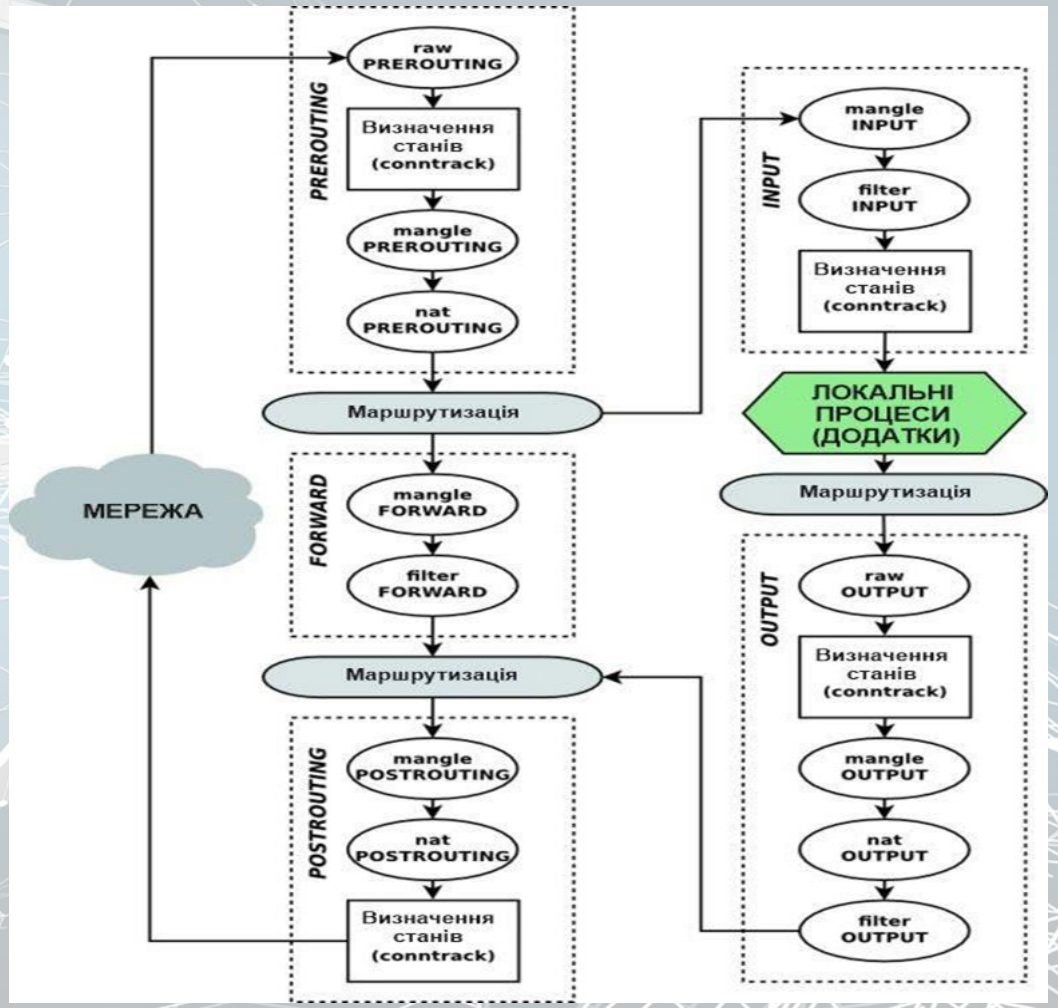
Міжмережевий екран ОС Linux iptables

Фреймворк netfilter, до складу якої входять iptables, дозволяє системному адміністратору визначити правила роботи з мережевими пакетами. Правила згруповані у ланцюги, кожен ланцюг - це упорядкований список правил. Ланцюги згруповані в таблиці - кожна таблиця пов'язана з різним видом обробки пакетів.

Взагалі netfilter – це компонент ядра Linux, що забезпечує фільтрацію і модифікацію трафіку. Власне, саме він і є фаєрволом (рис.)

На рис.праворуч представлено схему проходження пакетів в ланцюжках iptables.



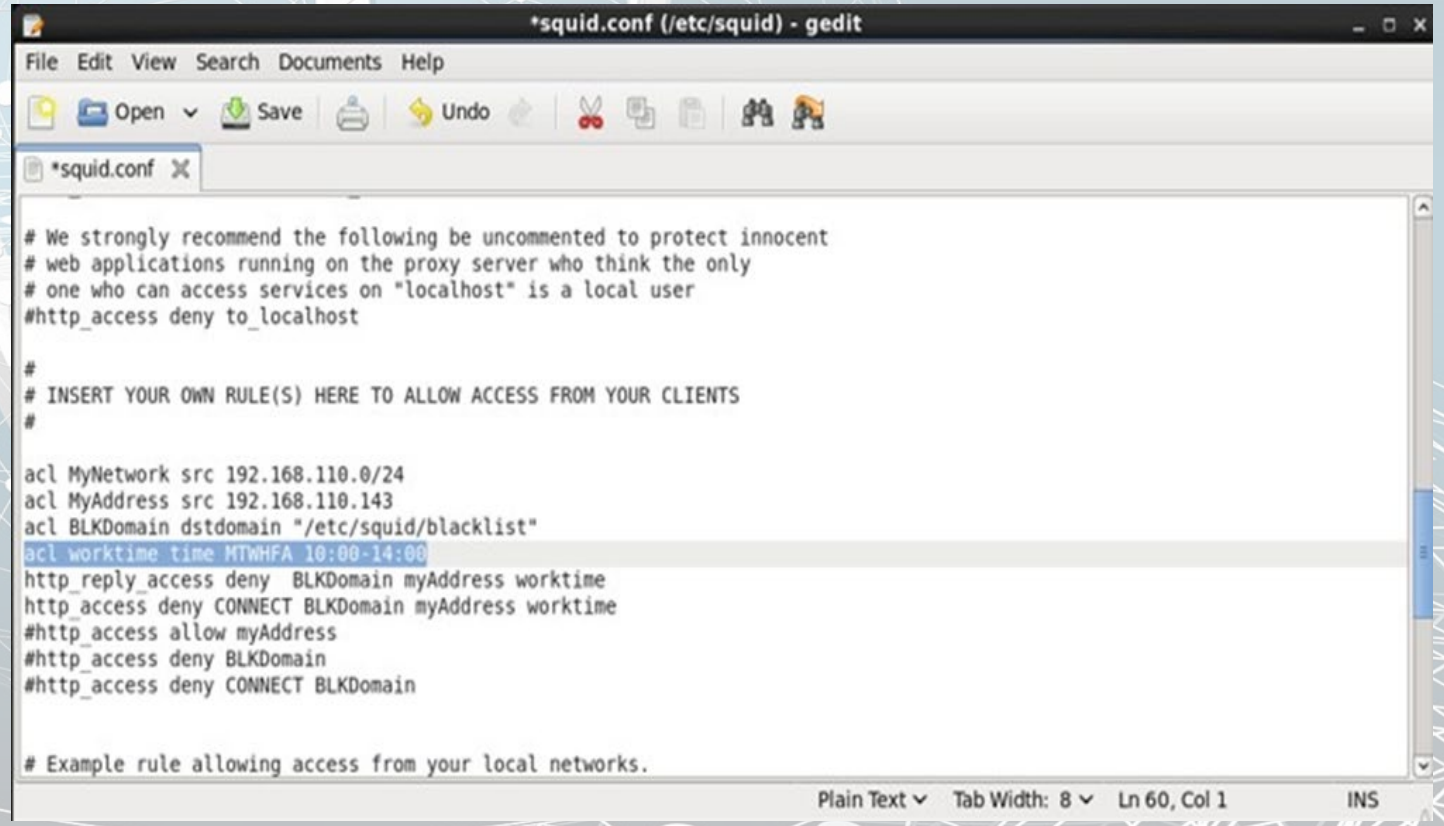


Проксі-сервер Squid

Squid (кальмар) - кешуючий проксі - сервер для протоколів HTTP, FTP, HTTPS (при відповідних налаштуваннях). Squid підтримує роботу в режимі
«прозорого проксі».
В режимі прозорості не проксіруются FTP і HTTPS - запитів.

Структура файлу є дуже простою і складається з таких параметрів:

- http_port,
- http_access,
- acl (списки контролю доступу).



Методи автентифікації в Squid

Squid щодо автентифікації подібний Web-серверу Apache і підтримує ті ж способи автентифікації, що і Apache . На сьогоднішній час існують чотири основні типи автентифікації в HTTP протоколі:

1. Basic - найперша схема, найбільш часто використовувана
2. NTLM - це перша спроба Microsoft до SSO (Single-Sign-On) єдиного входу для ресурсів локальної мережі
3. Digest - вона ж дайджет аутентифікація. Трохи краща з боку захищеності ніж базова
4. Negotiate (інша назва SPNEGO) - вона ж покоління Kerberos SPN - друга спроба Microsoft реалізації SSO

До кожної схеми автентифікації можуть використовуватися скільки завгодно різних зовнішніх модулів, аж до використання і самописних скриптів bash. Зазвичай при установці Squid встановлюються всі необхідні модулі згідно підтримуваних схем автентифікації.

Приклади сучасних брандмауерів

- Программно-аппаратный межсетевой экран CISCO PIX FIREWALL Брандмауер Cisco PIX забезпечує багаторівневий захист з багатим набором інтегрованих можливостей безпеки, включаючи адаптивний алгоритм безпеки та глибокий аналіз мережевих і прикладних протоколів за допомогою глибокої перевірки пакетів.
- Программный межсетевой экран CISCO IOS FIREWALL Програмне забезпечення Cisco IOS Firewall – це державний брандмауер, інтегрований в операційну систему Cisco IOS і підтримується на широкому спектрі моделей маршрутизаторів Cisco: 800, 1600, 1700, 1800, 2500, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7400, 7500, 7600.

Тенденції розвитку брандмауерів

Сучасні брандмауери істотно відрізняються від класичних прототипів початку 1990-х років. Якщо раніше брандмауер призначався тільки для розмежування доступу між інтернетом і внутрішньою мережею, то сьогодні з'явилися нові сфери його застосування:

- сегментація мережі з різними вимогами до безпеки;
- захист дата-центру;
- захист серверів додатків і т.д.

Тенденції:

- Використання технології Deep Packet Inspection
- брандмауери додатків – вузькоспеціалізовані рішення, які орієнтувалися на захист окремих додатків або сервісів на прикладному рівні еталонної моделі OSI
- виконувати глибокий аналіз вмісту трафіку, підключаючи ряд додаткових підсистем запобігання IPS (Intrusion Prevention), антивірусного захисту, контролю контенту і т.д.
- централізоване управління, перевірка різних мережевих і прикладних протоколів, підтримка NAT, інтеграція з різними серверами аутентифікації, фільтрація URL і т.д.
- брандмауери для захисту широко поширених веб-додатків електронної комерції
- тісна інтеграція з іншими рішеннями інформаційної безпеки

Питання для самоконтролю

1. Сформулюйте поняття «брандмауер»
2. Поясніть суть фільтрації інформаційного потоку брандмауером.
3. Які параметри можна використовувати в якості критеріїв для аналізу інформаційного потоку?
4. Які рішення приймаються при тлумаченні правил фільтрації інформаційного потоку?
5. Які існують функції медіації та програми медіації Міністерства енергетики США? Перелічіть функції, які може виконувати програмне забезпечення для посередництва.
6. Які додаткові можливості має брандмауер? Поясніть трансляцію внутрішньої мережевої адреси для пакетів вихідних повідомлень.
7. Опишіть особливості роботи екрануючого маршрутизатора (пакетного фільтра).
8. Охарактеризуйте особливості функціонування міжмережевих екранів експертного рівня. Як відбувається фільтрація пакетів зі збереженням стану?
9. Вкажіть переваги апаратної та програмної версії брандмауерів.
10. Сформулюйте принципи формування політики міжмережевої взаємодії, що реалізується системою брандмауер.
11. Які основні схеми підключення брандмауера? Опишіть, як схема працює із захищеними приватними та незахищеними відкритими підмережами.
12. Розкажіть про тенденції подальшого розвитку брандмауерів.

БЕЗПЕКА МОБІЛЬНИХ ТА БЕЗДРОТОВИХ МЕРЕЖ

Особливості забезпечення безпеки інформації в системах мобільного зв'язку стандарту GSM

У стандарті GSM термін «безпека» розуміють як виключення несанкціонованого використання системи і забезпечення конфіденційності переговорів мобільних абонентів. Визначено такі механізми безпеки в стандарті GSM:

- автентифікація;
- конфіденційність передачі даних;
- конфіденційність абонента;
- конфіденційність напрямів з'єднання абонентів.

Рекомендації щодо забезпечення інформаційної безпеки в мережах GSM

Стандарт	Режим безпеки	Механізм безпеки
GSM 02.09	Аспекти конфіденційності	Визначає характеристики безпеки, вживані в мережах. Регламентується їх застосування в мобільних станціях і мережах
GSM 03.20	Конфіденційність, пов'язана з функціями мережі	Визначає функції, необхідні для забезпечення характеристик безпеки, що розглядаються в Рекомендаціях GSM 02.09
GSM 03.21	Алгоритми забезпечення конфіденційності	Визначає криптографічні алгоритми в системі зв'язку
GSM 02.17	Модулі достовірності абонентів (SIM)	Визначає основні характеристики модуля SIM

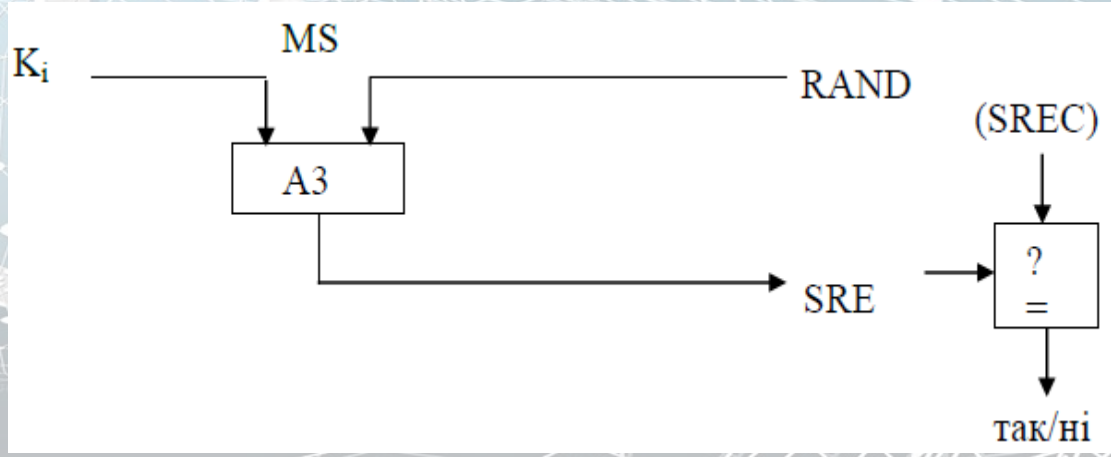
Механізми автентифікації

Для виключення несанкціонованого використання ресурсів системи в стандарті GSM реалізуються механізми автентифікації – перевірки достовірності абонента.

Кожен мобільний абонент на час користування системою зв'язку одержує стандартний модуль достовірності абонента (SIM-карту), який містить:

- міжнародний ідентифікаційний номер мобільного абонента (IMSI);
- свій індивідуальний ключ автентифікації (Ki);
- алгоритм автентифікації (A).

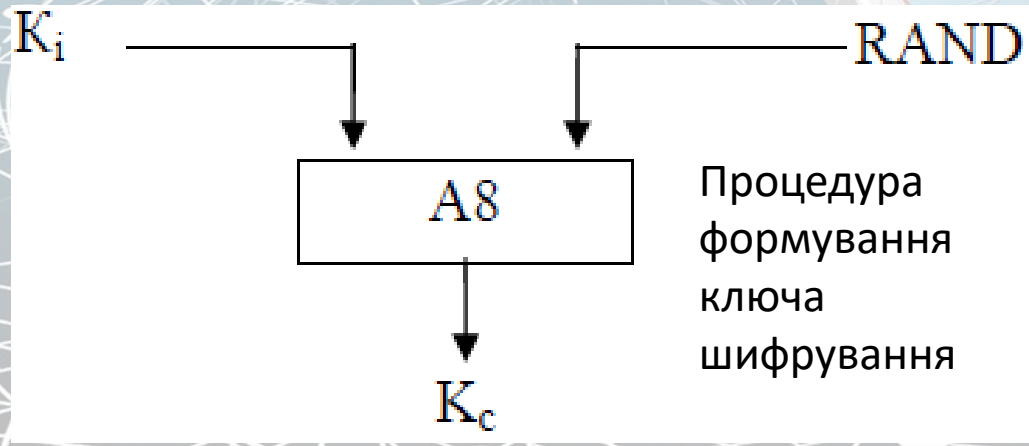
Мережа передає випадковий номер (RAND) на мобільну станцію. Мобільна станція визначає значення відгуку (SRES), використовуючи RAND, Ki і алгоритм A3 :
SRES = Ki[RAND].



Конфіденційність передачі мовної інформації

Після прийому випадкового номера RAND мобільна станція обчислює, окрім відгуку SRES, також і ключ шифрування (Кс), використовуючи RAND, Кі і алгоритм А8 (рис.): Кс = Кі [RAND].

Ключ шифрування Кс не передається радіоканалом. Як мобільна станція, так і мережа обчислюють ключ шифрування, який використовується іншими мобільними абонентами. На користь забезпечення безпеки обчислення Кс відбувається в SIM.



Процедура формування ключа шифрування



Процедура встановлення режиму шифрування

Принципи виконання алгоритмів сімейства A5/x (1)

Сімейство алгоритмів A5 є потоковими шифрами, побудованими на регістрах зсуву з лінійним зворотним зв'язком.

Алгоритм A5/1 має таку структуру:

- три регістри (R1, R2, R3) мають довжини 19, 22 і 23 біт;
- багаточлени зворотних зв'язків обчислюються за формулами для регістрів R1, R2 і R3 відповідно:

$$x^{18} + x^{17} + x^{16} + x^{13} + 1$$

$$x^{21} + x^{20} + 1$$

$$x^{22} + x^{21} + x^{20} + x^{7} + 1$$

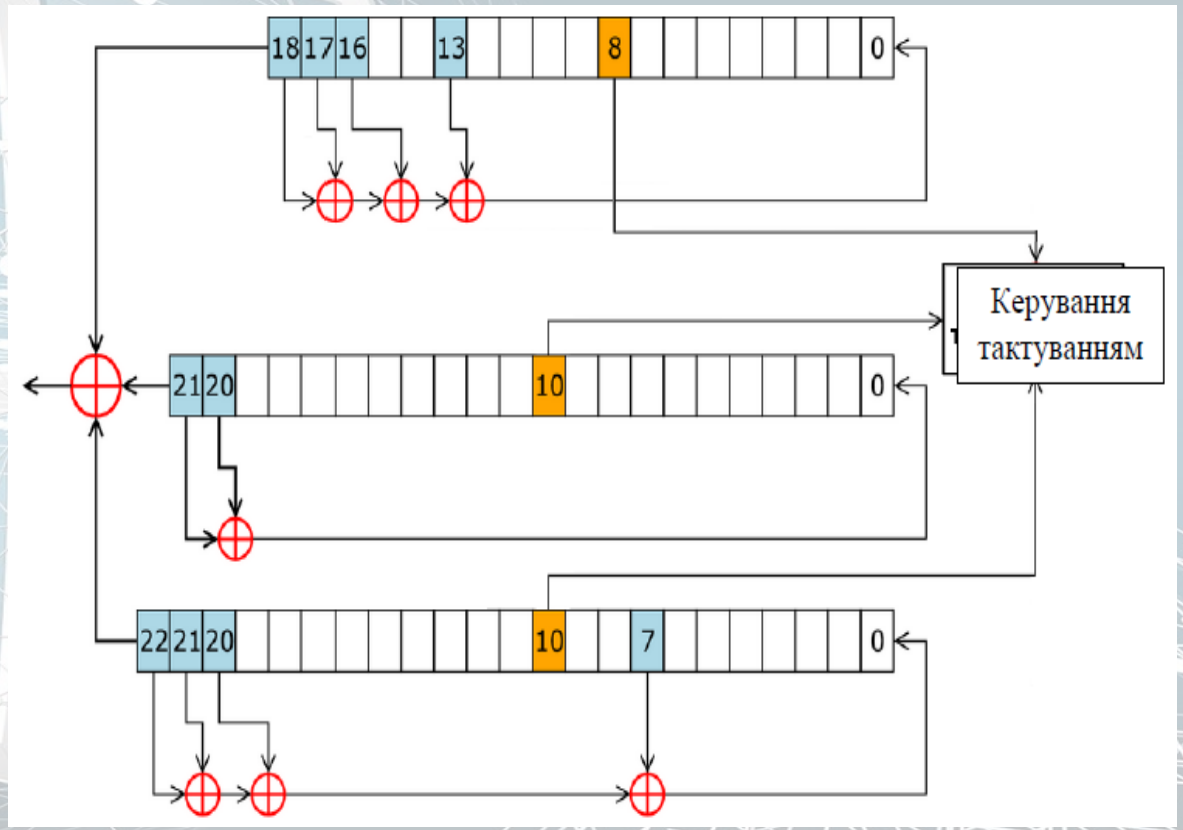
- блок керування тактуванням. Керування тактуванням здійснюється таким чином: у кожному регістрі є біти синхронізації –: 8 (R1), 10 (R2), 10 (R3). Обчислюється функція за формулою

  F = x & y | x & z | y & z

  де & – булево AND, | – булево OR, x, y та z – біти синхронізації R1, R2 і R3 відповідно.

Зсуваються тільки ті регістри, у яких біт синхронізації рівний F. Тобто, фактично, здійснюється зсув регістрів, сінхробіт яких належить більшості.

Вихідний біт системи – результат операції XOR над вихідними бітами регістрів. Структурна схема алгоритму A5/1 зображена на рис.



Структурна схема алгоритму A5/1

Принципи виконання алгоритмів сімейства A5/x (2)

Передача даних здійснюється в структурованому вигляді – з розбиттям на кадри (114 біт). При ініціалізації алгоритму, на його вхід надходять сесійний ключ (64 біта), сформований A8, і номер кадру (22 біта). Далі послідовно виконуються наступні дії:

1. Ініціалізація:

- 64 такти без керування зсувами регістрів, при яких молодші біти складаються з відповідним бітом сесійного ключа;
- аналогічні 22 такти, тільки підсумовування проводиться з номером кадру;
- 100 тактів з керуванням зсувами регістрів, але без генерації послідовності.

2. 228 (114 + 114) тактів робочі, відбувається шифрування переданого кадру (перші 114 біт) і розшифрування (останні 114 біт) того, що приймається.

3. Далі ініціалізація проводиться наново, використовується новий номер кадру.

Передача даних здійснюється в структурованому вигляді – з розбиттям на кадри (114 біт). При ініціалізації алгоритму, на його вхід надходять сесійний ключ (64 біта), сформований A8, і номер кадру (22 біта). Далі послідовно виконуються наступні дії:

1. Ініціалізація:

- 64 такти без керування зсувами регістрів, при яких молодші біти складаються з відповідним бітом сесійного ключа;
- аналогічні 22 такти, тільки підсумовування проводиться з номером кадру;
- 100 тактів з керуванням зсувами регістрів, але без генерації послідовності.

2. 228 (114 + 114) тактів робочі, відбувається шифрування переданого кадру (перші 114 біт) і розшифрування (останні 114 біт) того, що приймається.

3. Далі ініціалізація проводиться наново, використовується новий номер кадру.

Принципи виконання алгоритмів сімейства A5/x (3)

В алгоритм A5/2 доданий ще один регістр на 17 біт (R4), що керує рухом інших. Структурна схема алгоритму A5/2 зображена на рис.

Зміни структури такі:

- додано регістр R4 завдовжки 17 біт;
- багаточлен зворотного зв'язку для R4 обчислюється за формулою

$$x^{16} + x^{11} + 1,$$

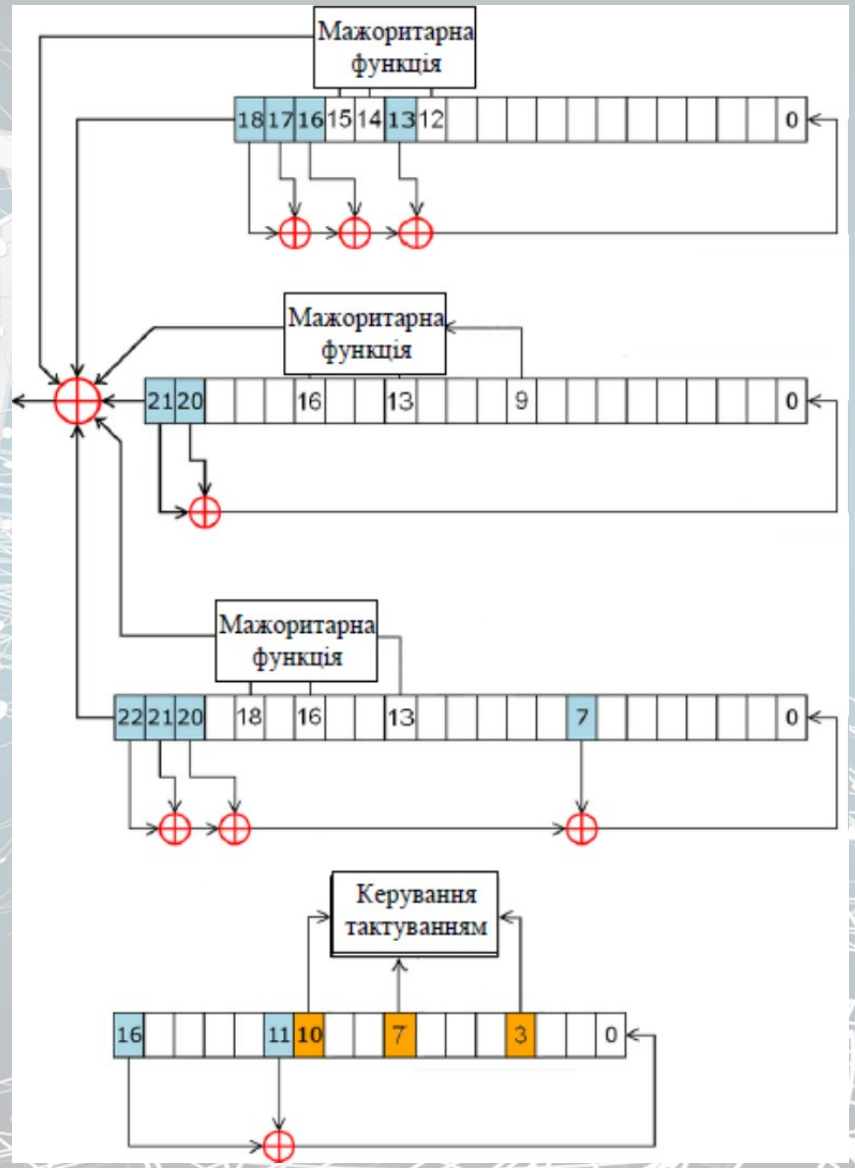
- керування тактуванням здійснюється з допомогою R4 таким чином:

1. У R4 біти 3, 7, 10 є бітами синхронізації.
2. Обчислюється мажоритарна функція за формулою 4.4, де x, y і z – біти синхронізації R4(3), R4(7) і R4(10) відповідно.
3. R1 здійснює зсув, якщо R4(10) = F.
4. R2 здійснює зсув, якщо R4(3) = F.
5. R3 здійснює зсув, якщо R4(7) = F;

- вихідний біт системи – результат операції XOR над старшими бітами регістрів і мажоритарних функцій від певних бітів регістрів:
  1) для R1 – 12, 14, 15;
  2) для R2 – 9, 13, 16;
  3) для R3 – 13, 16, 18.

Зміни у функціонуванні не такі істотні і стосуються тільки ініціалізації:

- 64 + 22 такти заповнюються сесійним ключем і номером кадру також R4;
- 1 такт R4(3), R4(7) і R4(10) заповнюються 1;
- 99 тактів з керуванням зрушеннями регістрів, але без генерації послідовності.



Порівняльний аналіз криптостійкості алгоритмів A5/1 і A5/2

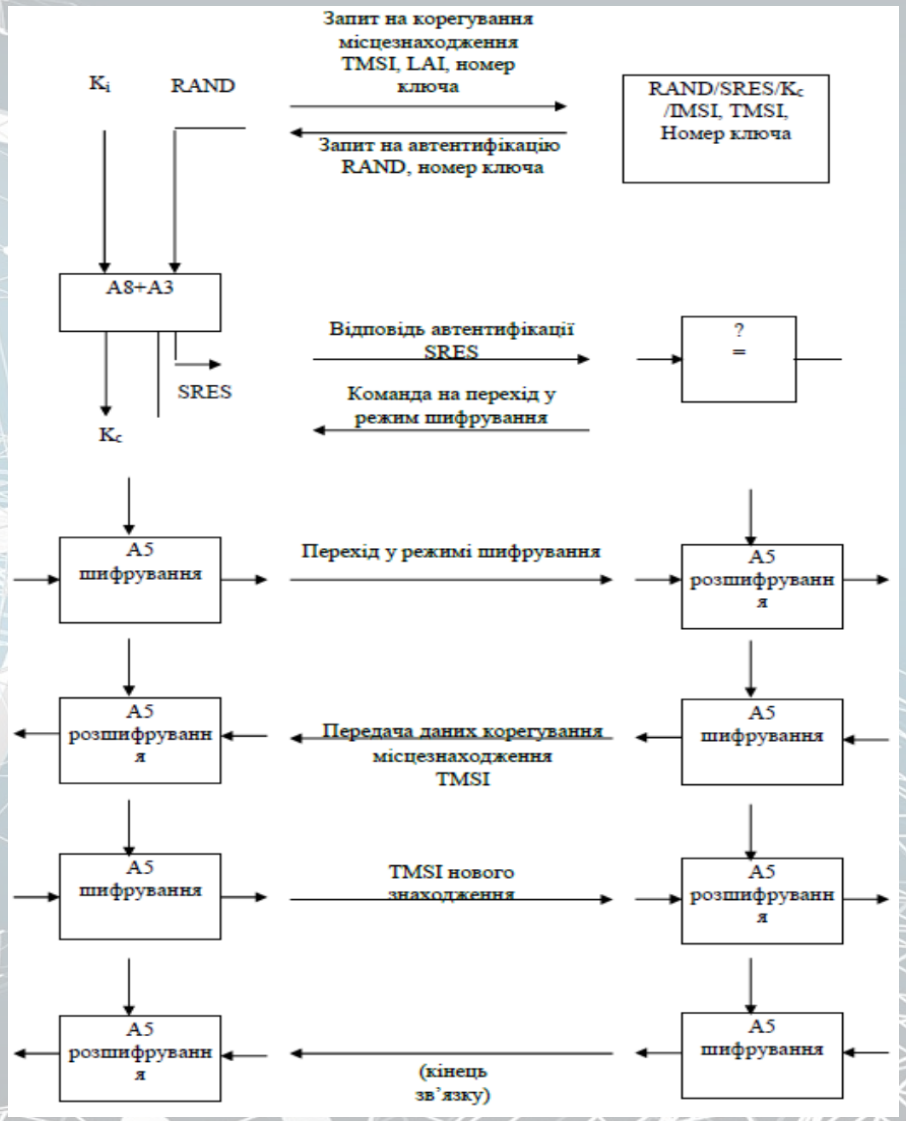
- порівнюючи криптостійкість алгоритмів A5/1 і A5/2, можна зробити висновок, що алгоритм A5/1 є стійкішим, оскільки для його злому у будь-якому випадку необхідно мінімум дві хвилини, а для злому A5/2 – декілька секунд.
- алгоритми забезпечення конфіденційності акустичної інформації, автентифікації, генерації сеансового ключа в стандарті GSM на сьогодні є уразливими до багатьох видів атак.
- Оскільки переговори між двома мобільними станціями ведуться через базову станцію і центр комутації, у обслуговуючого персоналу є можливість доступу до ключової інформації. Таким чином, GSM-зв'язок украй не рекомендується використовувати в сферах, де циркулює таємна інформація.

Забезпечення конфіденційності абонента

Для виключення визначення (ідентифікації) абонента шляхом перехоплення повідомлень, переданих радіоканалом, кожному абоненту системи зв'язку присвоюється «тимчасове посвідчення особи» – тимчасовий міжнародний ідентифікаційний номер користувача (TMSI), який дійсний тільки в межах зони розташування (LA). В іншій зоні розташування йому присвоюється інший TMSI. Якщо абоненту ще не присвоєний тимчасовий номер (наприклад, при першому включенні мобільної станції), ідентифікація проводиться через міжнародний ідентифікаційний номер (IMSI).

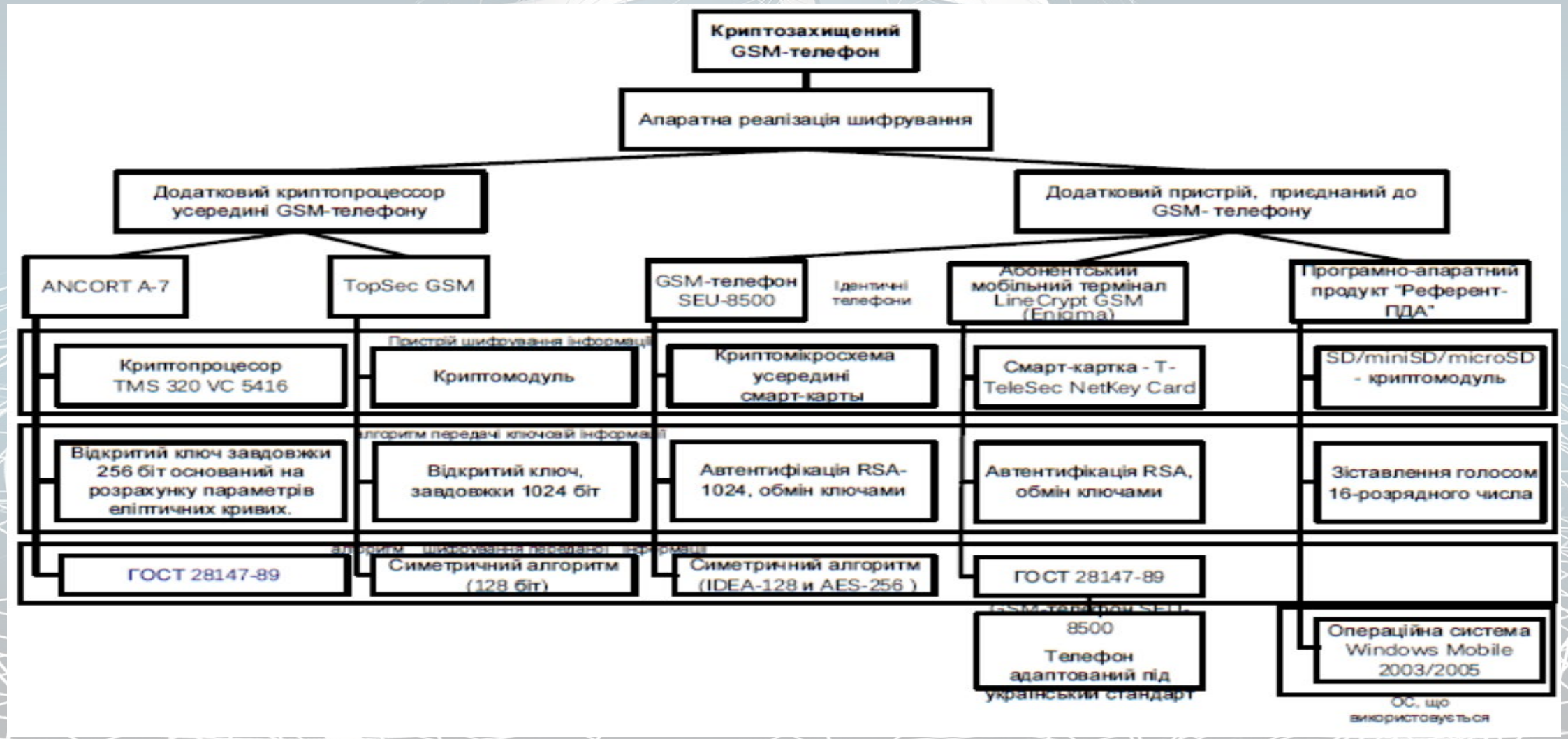
Після закінчення процедури автентифікації і початку режиму шифрування тимчасовий ідентифікаційний номер – TMSI передається на мобільну станцію тільки в зашифрованому вигляді. Цей TMSI використовуватиметься при всіх подальших доступах до системи. Якщо мобільна станція переходить у нову область розташування, то її TMSI повинен передаватися разом з ідентифікаційним номером зони (LAI), в якій TMSI був присвоєний абоненту.

При виконанні процедури корегування місцезнаходження каналами керування здійснюється двосторонній обмін між MS і BTS-службовими повідомленнями, що містять тимчасові номери абонентів TMSI. В цьому випадку в радіоканалі необхідно забезпечити захист інформації про перейменування TMSI і їх належності конкретному абоненту.



Процедура корегування місцезнаходження

Класифікація сучасних програмно-апаратних засобів захисту інформації стандарту GSM



Криптофони з додатковим криптопроцесором усередині GSM-телефону

В теперішній час найбільш поширеним криптофоном з додатковим криптопроцесором усередині GSM-телефону є криптосмартфон ANCORT A-7.

Особливості ANCORT A-7:

- Шифрування SMS і E-mail.
- Виключення можливості атаки «людина посередині».
- Захист від вірусів, які дозволяють прослуховувати телефон абонента, за допомогою будь-якого іншого телефону або спеціалізованого комп'ютера.
- Захист від незаявлених можливостей.
- ANCORT A-7 захищений від пристроїв, що дозволяють прослуховувати стандартні GSM–телефони.
- Захист від прослухування інформації в результаті втрати, розкрадання, отримання тимчасового доступу.
- Низький час затримки в крипторежимі.

Криптофони з додатковим чипом усередині GSM-телефону

- TopSecGSM – мобільний телефон із захистом від перехоплення телефонних переговорів.
- Шифрована мова передається прозорим каналом передачі даних мережі GSM. Висока безпека досягається комбінацією двох алгоритмів: асиметричного алгоритму з довжиною ключа 1024 біт для ключової угоди і симетричного алгоритму з довжиною ключа 128 біт для шифрування голосу. Режим криптозахисту має опціональне включення. При включеному режимі криптозахисту ініціалізується цифровий виклик і в межах 15 с відбувається обмін ключами.
- Спеціальне програмне забезпечення TopSec GSM дозволяє створювати закриті групи користувачів.
- При конфіденційному зв'язку відбувається стиснення мовного сигналу за допомогою Half-Rate GSM кодера.
- TopSec GSM забезпечує шифрування голосу на ділянці абонент-абонент у мережах стільникового зв'язку GSM, працюючих у діапазонах частот 900 МГц і 1800 МГц.

GSM-телефон SEU-8500

- Шифрування здійснюється в режимі реального часу за допомогою алгоритмів IDEA з довжиною ключа 128 біт і AES з довжиною ключа 256 біт. Передача ключів шифрування здійснюється протягом сеансу установки з'єднання, як частина процедури автентифікації передавальної сторони.
- Генерація ключів шифрування здійснюється за допомогою сертифікованого генератора випадкових чисел у мікросхемі смарт-карти.
- Секретний ключ знаходиться в смарт-карті, і прорахувати його неможливо.

LineCrypt GSM (Enigma)

- Enigma дозволяє встановити захищений голосовий виклик у мережі стільникового зв'язку загального користування із здійсненням безпосереднього шифрування між двома абонентами, що ведуть переговори.
- У терміналі використовується європейський криптографічний алгоритм IDEA, при якому ключ є індивідуальним для кожної розмови і генерується під час процесу обміну на початку кожного захищеного виклику.
- В кінці виклику ці ключі знищуються, і при наступному виклику цей процес виконується наново. Крім того, для забезпечення додаткового захисту інформації, кожен термінал Enigma має індивідуальний цифровий сертифікат.

Додатковий пристрій, що виконує функцію шифрування, та приєднується до звичайного GSM-телефону

- Програмно-апаратний продукт “Референт-PDA” розроблений для пристроїв типу смартфон, що працюють під керуванням операційної системи Windows Mobile 2003/2005.
- Основною відмінністю виробу від аналогів є використання низькошвидкісного каналу передачі даних (до 1600 бод), що дозволяє працювати при слабкому GSM–сигналі (у місцях поганого прийому), в роумінгу, при використанні різних операторів і т. ін.
- У процесі встановлення з'єднання проводиться обмін спеціальною інформацією для взаємної автентифікації пристроїв і формування сеансового ключа.

Особливості захисту інформації в системах мобільного зв'язку стандарту IS-95

- Стандарт IS-95 забезпечує високий ступінь безпеки переданих повідомлень і даних про абонентів.
- Безпека зв'язку забезпечується також застосуванням процедур автентифікації і шифрування повідомлень.
- У стандарті IS-95 реалізовано процедуру автентифікації, відповідну стандарту IS-54B. Шифрування повідомлень, переданих каналами зв'язку, здійснюється також з використанням процедур стандарту IS-54B.
- У стандарті IS-95 реалізовано режим «приватний характер зв'язку», що забезпечується використанням секретної маски у вигляді довгого коду. Цей процес також аналогічний процесу формування маски у вигляді довгого коду, описаного в стандарті IS-54B.

Особливості захисту інформації в прямому каналі зв'язку



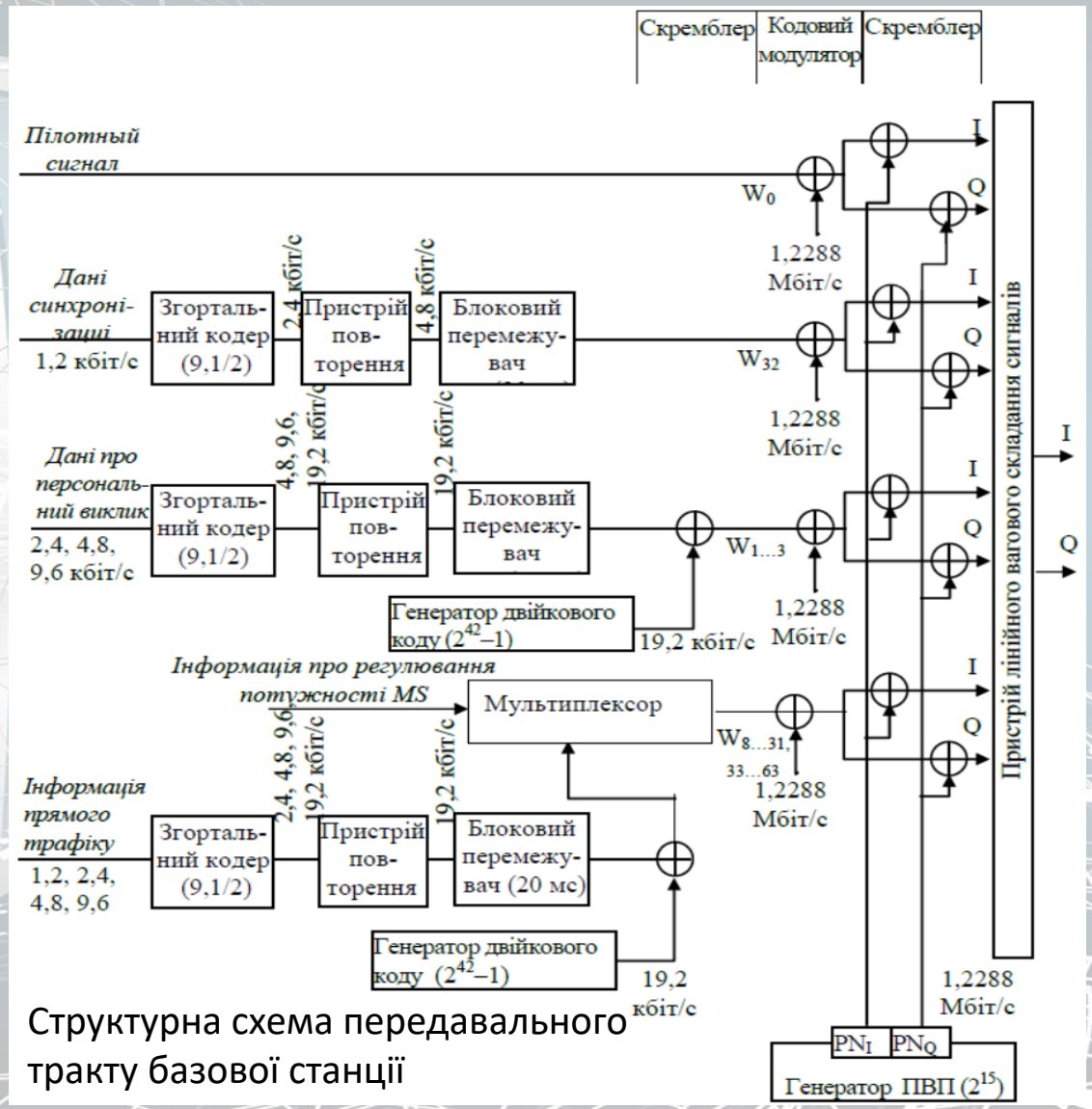
Структура прямого каналу зв'язку системи cdmaOne

Структура маски довгого коду каналу прямого трафіку

Преамбула	Серійний номер		
1100011000	Кодовий номер 8 біт	Резервні біти 6 біт	Порядковий номер 18 біт

Структура маски довгого коду каналу персонального виклику

Преамбула	Резервні біти	Номер каналу персонального виклику	Резервні біти	Індекс часового зсуву ПВП пілот-сигналу
1100011000	00000	XXX	000000000000	XXXXXXXXX

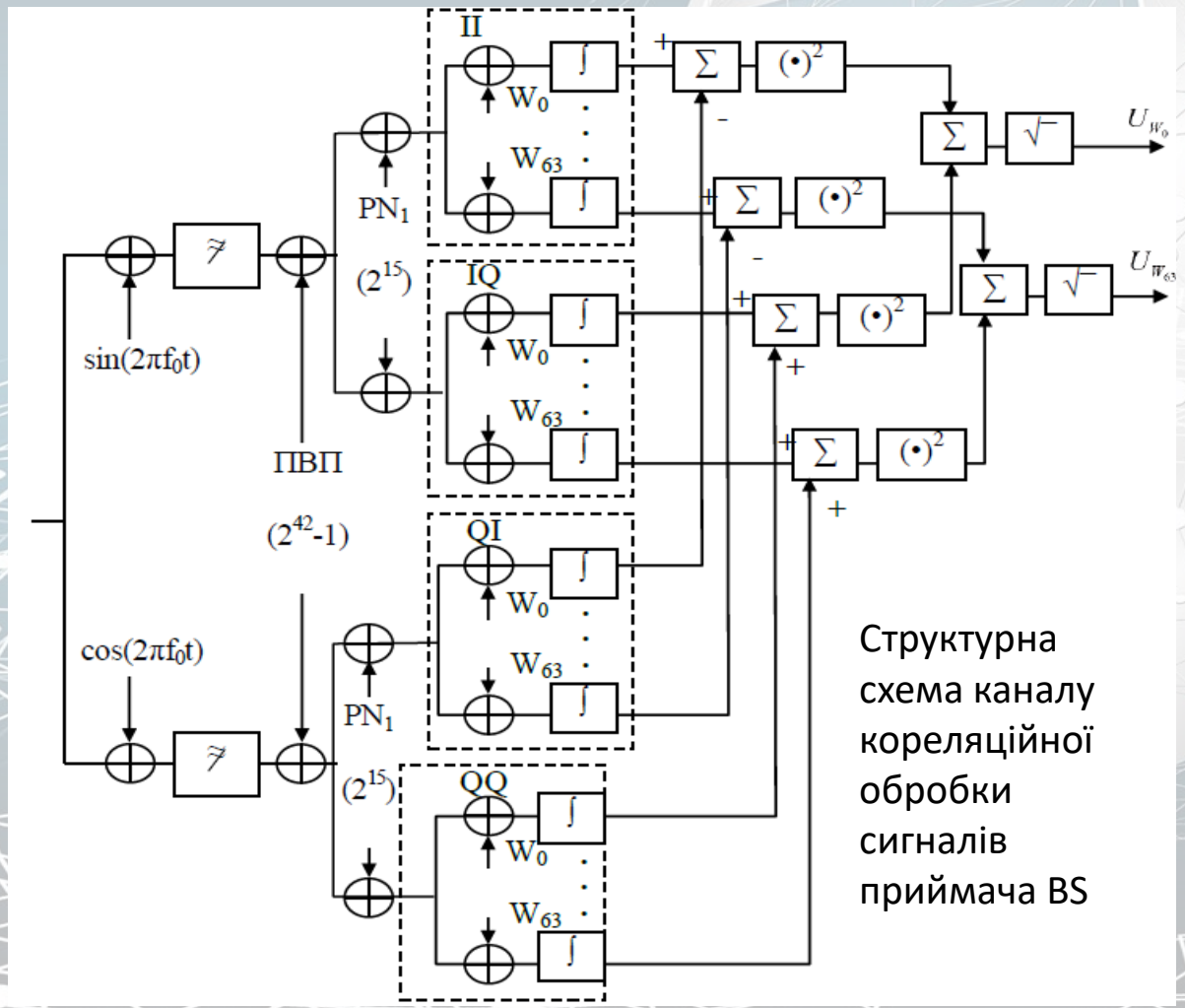


Структурна схема передавального тракту базової станції

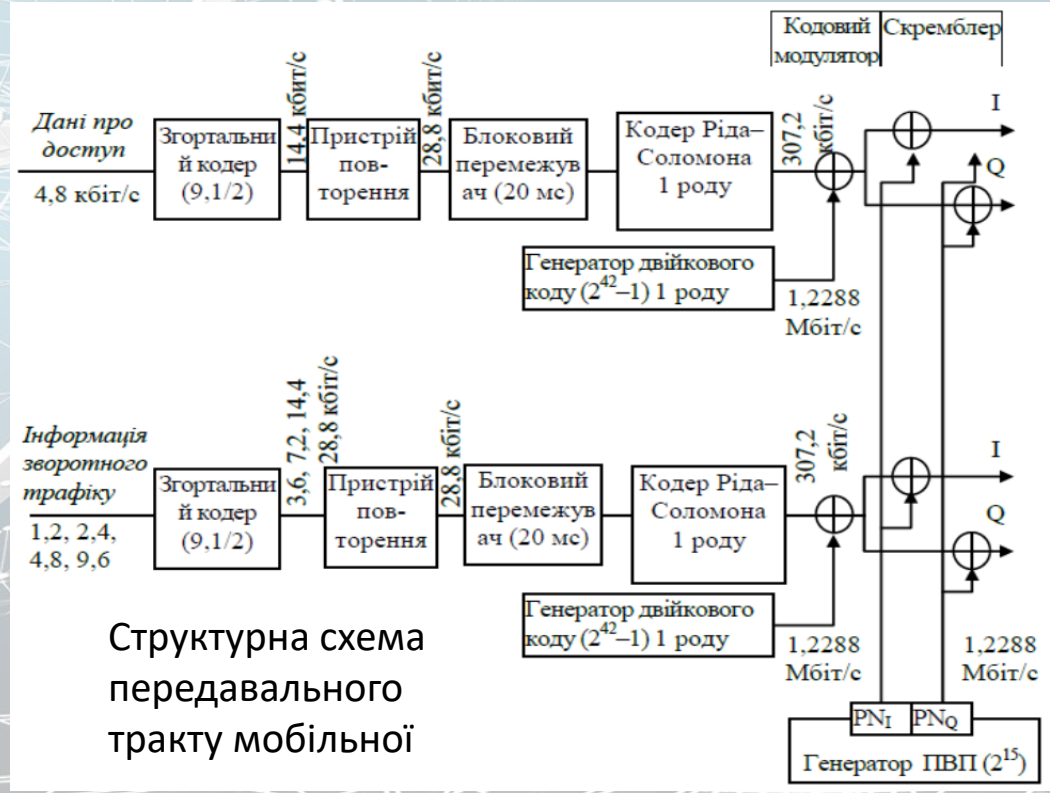
Особливості захисту інформації в зворотному каналі зв'язку

Структура зворотного каналу зв'язку системи cdmaOne





Структурна схема каналу кореляційної обробки сигналів приймача BS



Структурна схема передавального тракту мобільної

Безпека бездротових з'єднань (WLAN)

У бездротових локальних мережах головним чином використовується група стандартів технології 802.11x (a, b, g і т.д.). Ці стандарти дозволяють з'єднувати робочі станції, або мобільні пристрої каналами із пропускною здатністю до декількох Гбіт/с із використанням бездротової точки доступу, що підключається до кабельної мережі або прямо до іншої робочої станції.

Стандарти передбачають обмін автентифікаційними даними, а також шифрування інформації.

Стандарт 802.11x визначає протокол WPA і WPA2 для захисту інформації при її передачі через WLAN. WPA і WPA2 передбачає забезпечення трьох основних аспектів:

- Автентифікація.
- Конфіденційність.
- Цілісність.

WPA і WPA2 (1)

WPA і WPA2 (Wi-Fi Protected Access) – являє собою оновлену програму сертифікації пристроїв бездротового зв'язку. Технологія WPA прийшла на заміну технології захисту бездротової Wi-Fi мережі WEP. Плюсами WPA є посилена безпека даних і більш жорсткий контроль доступу до бездротових мереж. Вагомою характеристикою є сумісність між безліччю бездротових пристроїв як на апаратному рівні, так і на програмному. На даний момент WPA і WPA2 розробляються й просуваються організацією Wi-Fi Alliance.

В WPA забезпечена підтримка стандартів 802.1X, а також протоколу EAP (Extensible Authentication Protocol, розширюваний протокол автентифікації). Варто помітити, що в WPA2 підтримується шифрування у відповідності зі стандартом AES (Advanced Encryption Standard, удосконалений стандарт шифрування), що має ряд переваг над використовуваним в WEP RC4, наприклад набагато більше стійкий криптоалгоритм.

Більш вагомим аспектом при впровадженні WPA є можливість роботи технології на існуючому апаратному забезпеченні Wi-Fi.

Деякі відмінні риси WPA:

- удосконалена схема шифрування RC4;
- обов'язкова автентифікація з використанням EAP;
- Система централізованого керування безпекою, можливість використання в діючих корпоративних політиках безпеки.

WPA і WPA2 (2)

Автентифікація користувачів

- Wi-Fi Alliance дає наступну формулу для визначення суті WPA: WPA = 802.1X + EAP + TKIP + MIC
- Видно, що WPA, по суті, є сумою декількох технологій
- WPA використовується Розширюваний протокол автентифікації (EAP) як основа для механізму автентифікації користувачів.
- Неодмінною умовою автентифікації є пред'явлення користувачем свідчення (або інакше мандат), що підтверджує його право на доступ у мережу. Для цього права користувач проходить перевірку за спеціальною базою зареєстрованих користувачів.
- Слід зазначити, що WPA має спрощений режим. Він одержав назву Pre-Shared Key (WPA-PSK).

WPA і WPA2 (3)

Шифрування

- Ключова проблема WEP полягає у використанні занадто схожих ключів для різних пакетів даних.
- TKIP, MIC і 802.1X (частини рівняння WPA) внесли свою лепту в посилення шифрування даних мереж, що використовують WPA.
- Протокол TKIP (Temporal Key Integrity Protocol) – це метод шифрування. Протокол TKIP забезпечує попакетне шифрування, що включає перевірку цілісності повідомлень і механізм повторного шифрування.
- Іншим важливим механізмом є перевірка цілісності повідомлень (Message Integrity Check, MIC)
- механізми шифрування, які використовуються для WPA і WPA-PSK, є ідентичними. Єдина відмінність WPA-PSK полягає в тому, що автентифікація виробляється з використанням пароля, а не по сертифікату користувача.

WPA2

- WPA2 визначається стандартом IEEE 802.11i, прийнятим у червні 2004 року, і покликаний замінити WPA. У ньому реалізоване CCMP і шифрування AES, за рахунок чого WPA2 став більше захищеним, чим свій попередник. З 13 березня 2006 року підтримка WPA2 є обов'язковою умовою для всіх сертифікованих Wi-Fi пристроїв.
- У режимі WPA-PSK/WPA 2-PSK і TKIP або AES використовується загальний ключ (PSK) довжиною 8 – 63 символу.

Автентифікація в WLAN

- Автентифікація є ключовим компонентом системи безпеки WLAN.
- Ідентифікатор набору служб (SSID) – це 32-бітний рядок, використовуваний як мережеве ім'я. Щоб зв'язати робочу станцію із точкою доступу, обидві системи повинні мати той самий SSID. Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися із точкою доступу й з'єднатися з мережею. На жаль, SSID поширюється багатьма точками доступу. Це означає, що будь-яка робоча станція, що перебуває в режимі очікування, може одержати SSID і додати саму себе у відповідну мережу. Деякі точки доступу можна налаштувати на заборону поширення SSID. Однак, якщо дана конфігурація не буде супроводжуватися відповідними мірами безпеки передачі даних, SSID як і раніше можна буде визначити за допомогою прослуховування трафіку.
- Деякі точки доступу дозволяють використовувати MAC-адреси авторизованих робочих станцій для автентифікації (це можливість, передбачена постачальником, тому вона не включена в специфікацію). MAC-адреса повідомляється точці доступу адміністратором, що додає MAC-адресу в список дозволених пристроїв. На жаль, MAC-адреси повинні передаватися у відкритому виді; у противному випадку мережа функціонувати не буде. Якщо зловмисник прослуховує трафік, він може визначати авторизовані MAC-адреси й налаштувати свою власну систему на використання однієї із цих MAC-адрес для установки з'єднання з AP.

Протокол 802.1X: контроль доступу в мережу по портах

Протокол 802.1X розроблений як надбудова для всіх протоколів контролю доступу 2 рівнів, включаючи Ethernet і WLAN. Протокол призначений для забезпечення узагальненого механізму автентифікації при доступі в мережу й передбачає наступний набір елементів:

- Автентифікатор. Мережний пристрій, що здійснює пошук інших об'єктів для автентифікації; для WLAN це може бути AP.
- Здобувач. Об'єкт, якому потрібен доступ. У випадку з WLAN це може бути робоча станція.
- Сервер автентифікації. Джерело служб автентифікації. 802.1X дозволяє централізацію цієї функції, тому даний сервер є, наприклад, сервером RADIUS.
- Мережева точка доступу. Точка приєднання робочої станції до мережі. По суті, це порт на комутаторі або концентраторі. У бездротовій технології вона є зв'язком між робочої станції й точкою доступу.
- Процес доступу через порт (PAE). PAE – це процес, що виконує протоколи автентифікації. PAE є як в автентифікатора, так і в здобувача.
- Розширюваний протокол автентифікації (EAP). Протокол EAP (визначений у стандарті RFC 2284) являє собою протокол, використовуваний при обміні автентифікаційними даними. Поверх EAP можуть працювати й інші протоколи автентифікації більш високого рівня.

Питання безпеки бездротових з'єднань

- Виявлення WLAN
  Виявити WLAN дуже легко. Дійсно, саме для цієї мети був розроблений ряд засобів. Однієї з таких утиліт є NetStumber (http://www.netstumber.com/); вона працює в операційних системах сімейства Windows і може використовуватися спільно із супутниковим навігатором (ресивером глобальної системи позиціонування, GPS) для виявлення бездротових мереж WLAN. Дана утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній WPA/WPA2.
- Прослуховування
  Найбільш очевидним ризиком, що представляється для організації, що використовує бездротову мережу, є можливість проникнення зловмисника у внутрішню мережу компанії. Навіть ті організації, у яких використовується WPA/WPA2, є уразливими до даного типу прослуховування. Такі засоби, як WPA/WPA2Crack, вимагають обробки декількох мільйонів пакетів, перш ніж зможуть бути визначені ключі шифрування.
- Активні атаки
  Основний ризик, пов'язаний з бездротовими мережами: зловмисник може успішно перебороти периметр мережного захисту організації. В більшості організацій використовується деякий метод автентифікації перед наданням доступу до серверів і файлів. Однак якщо на системах не встановлені потрібні відновлення, у зловмисника з'являється можливість виявити ці уразливості, якими він зможе скористатися для виконання несанкціонованих дій.
  Замість проведення внутрішніх атак зловмисник може використовувати мережеве з'єднання для атаки ззовні. Таким чином, організація стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему.
- Юридичні питання

Реалізація безпеки бездротових мереж

- Безпека точки доступу. В ідеальному випадку точка доступу дозволяє вказати ключ WPA/WPA2. По можливості використовуйте HTTPS для керування точкою доступу й запобігайте доступу зловмисника за допомогою використання високонадійних паролів. Останнє, що необхідно взяти до уваги при розгляді точок доступу, – їхнє розташування.
- Безпека передачі даних. Незважаючи на серйозні уразливості, що є присутнім в WPA/WPA2, необхідно використовувати цей протокол. Більша частина VPN-продуктів передбачає надійні алгоритми шифрування, у яких відсутні недоліки, властиві WPA/WPA2.
- Безпека робочої станції. Захист робочих станцій у мережі WLAN не відрізняється від захисту переносних комп'ютерів, розташованих в іншому місці. Необхідно встановити відповідне антивірусне ПЗ. Якщо ризик великий, на робочих станціях варто застосувати персональні міжмережеві екрани.
- Безпека сайту. WLAN необхідно розгортати в окремих сегментах мережі й встановити міжмережевий екран між мережею WLAN і внутрішньою мережею організації. Варто встановити в WLAN систему виявлення вторгнень для виявлення несанкціонованих відвідувачів. Стандарт 802.1X передбачає більш надійну автентифікацію, ніж SSID або MAC-адреса, однак він не захищений від перехоплення сеансу з'єднання. Нелегальні й несанкціоновані точки доступу також являють собою проблему, що організації повинні дозволяти з метою запобігання неприємностей.

Приклад реалізації бездротової локальної мережі

- Почніть із того, що розпишіть на папері суть проблеми. Визначте, які служби повинні бути доступні співробітникам на території організації, а також тих, хто може працювати в мережі, перебуваючи в їдальні або в приміщенні для відпочинку.
- Визначте ризики, що представляються для організації через використання WLAN. Чи буде сигнал бездротової мережі доступний поза територією організації? Як розв'язати питання підключення до мережі відвідувачів і позаштатних співробітників?
- Після визначення погроз варто почати визначення контрзаходів, які можуть знизити ризики до контрольованого рівня. Не слід розглядати лише технологічні рішення. Візьміть до уваги також питання, пов'язані з керуванням і виконанням різних операцій.
- Якщо у вас є доступ до точки доступу й бездротовий мережний адаптер, спробуйте застосувати розроблені рішення.

Контрольні запитання

1. Назвіть основні механізми безпеки в стандарті GSM.
2. Що входить до складу стандартного модуля достовірності абонента (SIM-карти)?
3. Що використовується для забезпечення конфіденційності переданої радіоканалом інформації?
4. У чому суть алгоритму шифрування A5/1?
5. Порівняльний аналіз криптостійкості алгоритмів A5/1 і A5/2.
6. Що таке тимчасовий міжнародний ідентифікаційний номер користувача (TMSI)?
7. Що входить до складу криптофонів з додатковим криптопроцесором усередині GSM-телефону?
8. Які особливості захисту інформації в системах мобільного зв'язку стандарту IS-95?
9. Назвіть особливості захисту інформації в прямому каналі зв'язку.
10. Які додаткові пристрої, що виконують функцію шифрування, та приєднуються до звичайного GSM-телефону, ви знаєте?
11. Які стандарти та протоколи використовуються для захисту безпроводових мереж?

ВІРТУАЛЬНІ БЕЗПЕЧНІ ТЕХНОЛОГІЇ VPN

Концепція побудови

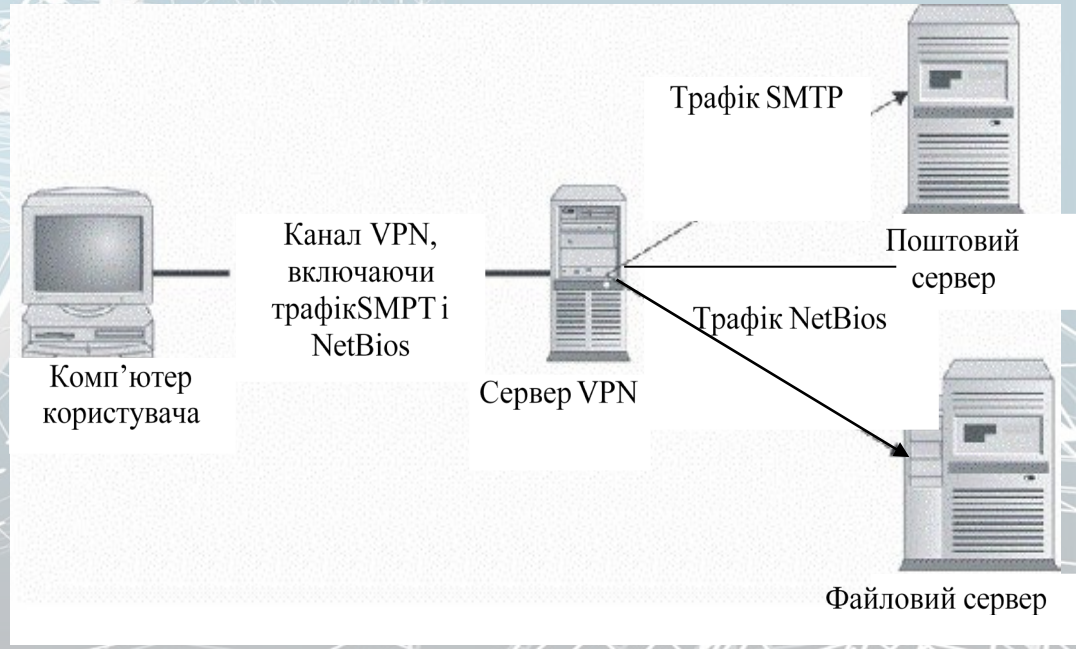
Приватні мережі використовуються організаціями для з'єднання з віддаленими сайтами й з іншими організаціями. Приватні мережі складаються з каналів зв'язку, орендованих у різних телефонних компаній і постачальників послуг Інтернету.

Приватні мережі мають безліч переваг:

- інформація зберігається в секреті;
- віддалені сайти можуть здійснювати обмін інформацією негайно;
- віддалені користувачі не відчувають себе ізольованими від системи, до якої вони здійснюють доступ.

Віртуальні приватні мережі володіють декількома характеристиками:

- трафік шифрується для забезпечення захисту від прослуховування;
- здійснюється автентифікація віддаленого сайту;
- віртуальні приватні мережі забезпечують підтримку безлічі протоколів;
- з'єднання забезпечує зв'язок тільки між двома конкретними абонентами.



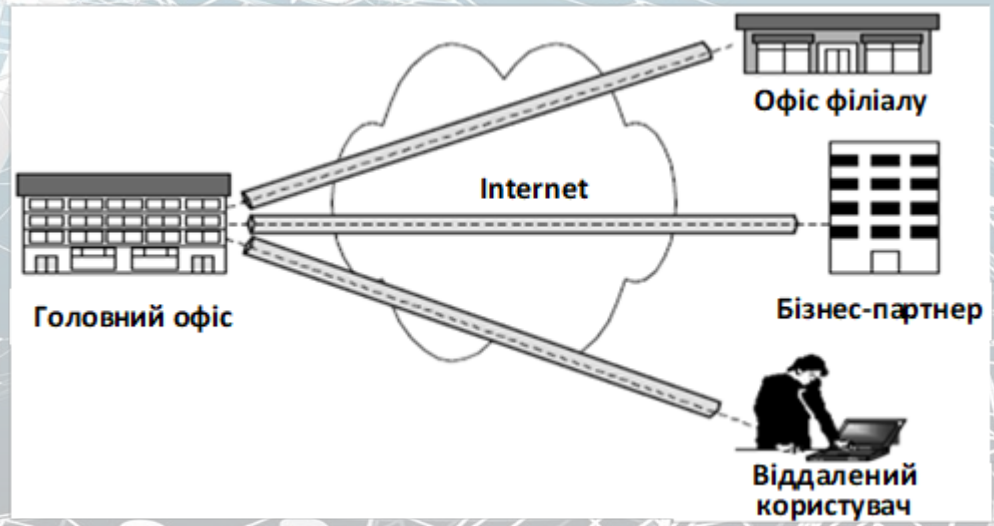
Основні поняття та функції (1)

При підключенні корпоративної локальної мережі до відкритої мережі виділяють два основних типи загроз безпеці:

- несанкціонований доступ до внутрішніх ресурсів корпоративної локальної мережі, отриманий зловмисником в результаті несанкціонованого доступу до цієї мережі;
- Несанкціонований доступ до корпоративних даних при передачі по відкритій мережі.

Забезпечення безпеки інформаційної взаємодії між локальними мережами та окремими комп'ютерами за допомогою відкритих мереж, зокрема через мережу Інтернет, можливе шляхом ефективного вирішення таких завдань:

- захист локальних мереж і окремих комп'ютерів, підключених до відкритих каналів зв'язку, від несанкціонованих дій із зовнішнього середовища;
- захист інформації в процесі її передачі по відкритих каналах зв'язку.



Основні поняття та функції (2)

VPN-тунель – це з'єднання, що здійснюється через відкриту мережу, по якій передаються криптографічно захищені пакети віртуальних мережевих повідомлень. Захист інформації при передачі через VPN-тунель базується на наступних функціях:

- аутентифікація взаємодіючих сторін;
- криптографічне замикання (шифрування) даних, що передаються;
- перевірка достовірності та цілісності переданої інформації.

VPN-клієнт – це програмний або апаратно-апаратний комплекс, який зазвичай виконується на базі персонального комп'ютера.

VPN-сервер – це встановлений на комп'ютері програмний або апаратно-апаратний комплекс, який виконує функції сервера.

Шлюз безпеки — це мережевий пристрій, який підключається до двох мереж, який виконує функції шифрування та автентифікації для кількох хостів, розташованих за ним.

Основні поняття та функції (3)

Суть тунелювання полягає в інкапсуляції, тобто «упаковці» переданої частини даних разом з сервісними полями в нову «оболонку». У цьому випадку пакет протоколу нижчого рівня розміщується в полі даних пакета протоколу вищого рівня або еквівалента.

Особливістю тунелювання є те, що ця технологія дозволяє шифрувати вихідний пакет повністю разом із заголовком, а не лише його полем даних. Оригінальний пакет із зашифрованим заголовком не може бути використаний для передачі по мережі. Тому для захисту вихідного пакета використовується інкапсуляція та тунелювання. Вихідний пакет шифрується повністю разом із заголовком, а потім цей зашифрований пакет поміщається в інший зовнішній пакет з відкритим заголовком. Для передачі даних по відкритій мережі використовуються відкриті поля заголовка зовнішнього пакета.

Після прибуття в кінцеву точку захищеного каналу внутрішній пакет джерела витягується із зовнішнього пакета, розшифровується, а його відновлений заголовок використовується для подальшої передачі по внутрішній мережі

Нова IP-адреса Заголовок	Джерело: IP Заголовок	Дані
	Оригінальна упаковка	

Приклад пакета, підготовленого до тунелювання

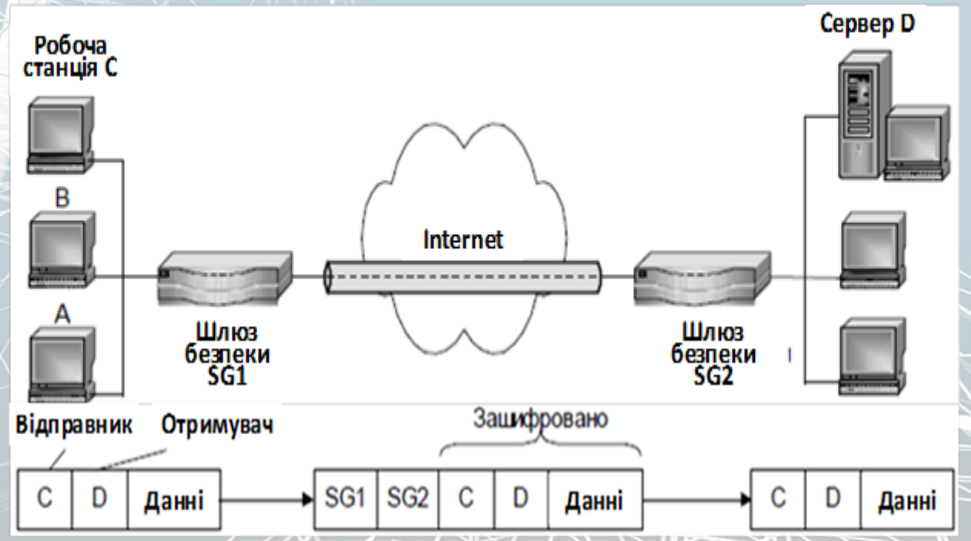


Схема віртуального захищеного тунелю

Основні поняття та функції (4)

VPN-тунелі можуть бути створені для різних типів кінцевих користувачів – як локальна локальна мережа (Local Area Network) зі шлюзом безпеки, так і окремі комп'ютери віддалених і мобільних користувачів. Щоб створити віртуальну приватну мережу для великого підприємства, вам потрібні VPN-шлюзи, VPN-сервери та VPN-клієнти. VPN-шлюзи доцільно використовувати для захисту локальних мереж підприємства, VPN-сервери і VPN-клієнти використовуються для організації безпечних з'єднань віддалених і мобільних користувачів з корпоративною мережею через мережу Інтернет.
Стандартна технологія функціонування VPN складається з чотирьох ключових компонентів:

- Сервер VPN.
- Алгоритми шифрування.
- Система автентифікації.
- Протокол VPN.

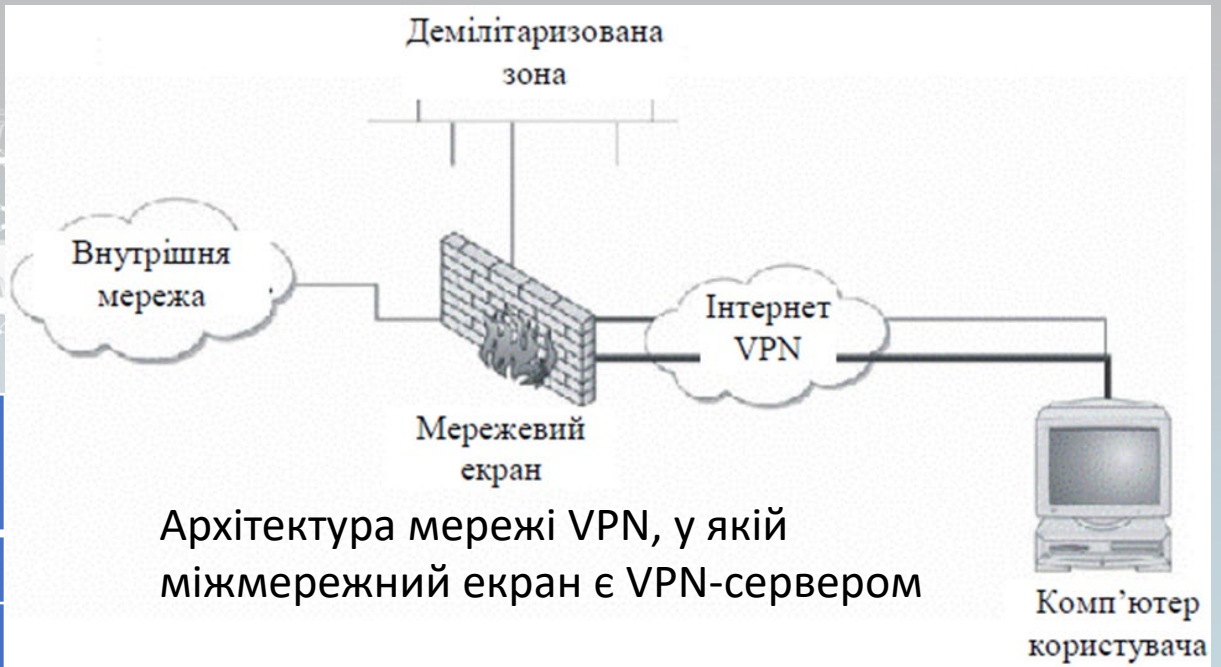
Ці компоненти реалізують відповідність вимогам по безпеці, продуктивності й здатності до взаємодії.

- Кількість часу, протягом якого необхідно забезпечувати захист інформації.
- Число одночасних з'єднань користувачів.
- Очікувані типи з'єднань користувачів (співробітники, що працюють віддалено або перебувають у поїздці).
- Число з'єднань із віддаленим сервером.
- Типи мереж VPN, яким знадобиться з'єднання.
- Очікуваний обсяг вхідного й вихідного трафіку на віддалених вузлах.
- Політика безпеки, що визначає налаштування безпеки.

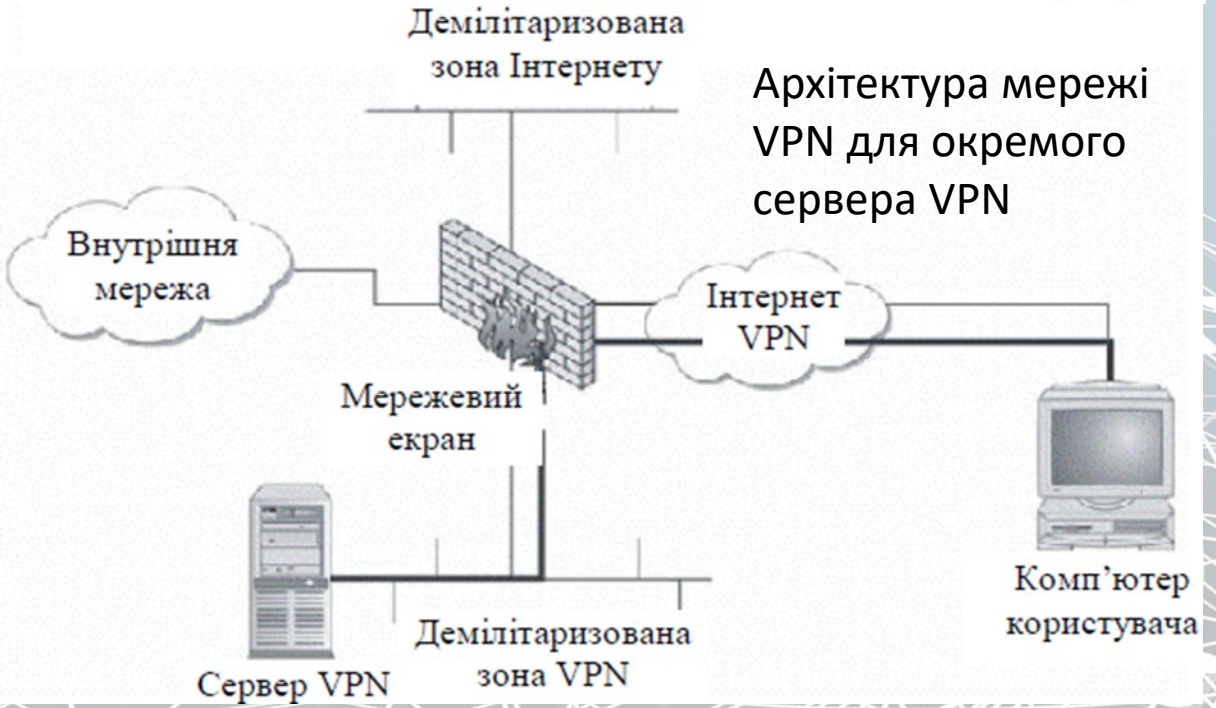
Сервер VPN

Правила політики міжмережевого екрана, що включають демілітаризовану зону VPN

Номер правила	Вихідний IP	Кінцевий IP	Служба	Дія
1	Будь-який	VPN-сервер	Служба VPN	Прийняття.
2	VPN-сервер	Внутрішня мережа	Будь-який	Прийняття
3	Будь-який	VPN-сервер	Будь-який	Відхилення
4	Будь-який	Веб-сервер	HTTP	Прийняття
5	Будь-який	Поштовий сервер	SMTP	Прийняття
6	Поштовий сервер	Будь-який	SMTP	Прийняття
7	Внутрішня мережа	Будь-який	HTTP, HTTPS, FTP, telnet, SSH	Прийняття
8	Внутрішня DNS	Будь-який	DNS	Прийняття
9	Будь-який	Будь-який	Будь-який	Скидання



Архітектура мережі VPN, у якій міжмережний екран є VPN-сервером



Архітектура мережі VPN для окремого сервера VPN

Компоненти VPN

Алгоритми шифрування

- Алгоритм шифрування, використовуваний в VPN, повинен бути стандартним потужним алгоритмом. Виникає питання: яка ж система шифрування найкраща? Взагалі, всі стандартні й потужні алгоритми можуть ефективно використовуватися при побудові VPN.

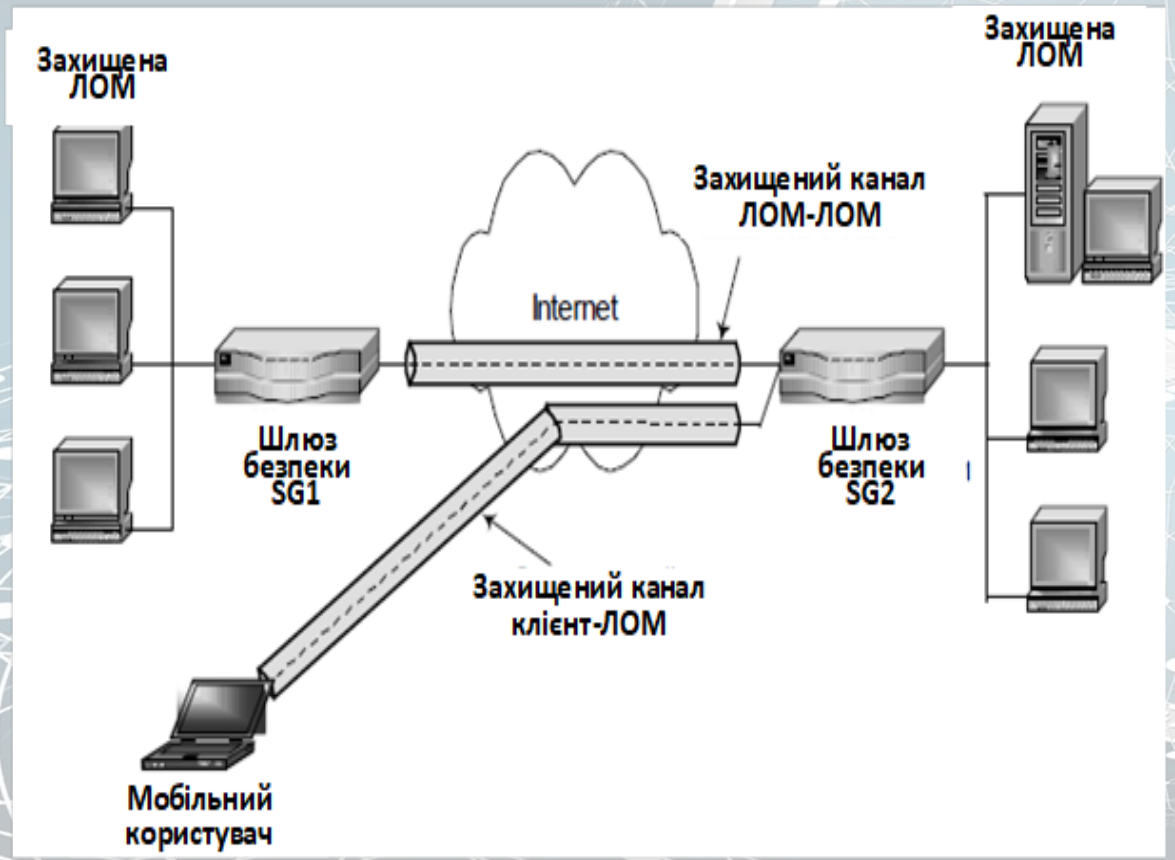
Система автентифікації

- Користувачі можуть проходити автентифікацію з використанням того, що вони знають, того, що в них є або за допомогою даних про те, ким вони є. Гарною комбінацією засобів автентифікації є смарт-карти в парі з персональним ідентифікаційним номером або паролем.

Протокол VPN

- Протокол VPN визначає, яким чином система VPN взаємодіє з іншими системами в Інтернеті, а також рівень захищеності трафіку.

Варіанти побудови віртуальних захищених каналів



При проектуванні VPN зазвичай розглядають дві основні схеми (рис.):

- віртуальний захищений канал між локальними мережами (канал LAN-LAN);
- віртуальний захищений канал між хостом і локальною мережею (канал клієнт-LAN).

Перша схема підключення дозволяє замінити дорогі виділені лінії між окремими офісами і створити завжди доступні захищені канали між ними. У цьому випадку шлюз безпеки служить інтерфейсом між тунелем і локальною мережею, при цьому користувачі локальної мережі використовують тунель для зв'язку один з одним. Багато компаній використовують цей тип VPN як заміну або доповнення до існуючих WAN-з'єднань, таких як Frame Relay.

Друга схема захищеного VPN-каналу призначена для встановлення з'єднань з віддаленими або мобільними користувачами. Створення тунелю ініціює клієнт (віддалений користувач). Для зв'язку зі шлюзом, який захищає віддалену мережу, він запускає на своєму комп'ютері спеціальне клієнтське програмне забезпечення. Цей тип VPN замінює комутоване з'єднання та може використовуватися разом із традиційними методами віддаленого доступу.

Інструменти безпеки VPN

У контексті завдань VPN критерії безпеки даних можна визначити таким чином:

- Конфіденційність – гарантія того, що в процесі передачі даних по захищених каналах VPN ці дані можуть бути відомі тільки законному відправнику і одержувачу;
- Цілісність – це запорука збереження даних, що передаються під час проходження захищеним каналом VPN. Будь-які спроби змінити, знищити або створити нові дані будуть виявлені і стануть відомими легальним користувачам;
- Доступність є гарантією того, що засоби, які виконують функції VPN, постійно доступні законним користувачам. Доступність VPN-інструментів – це комплексний показник, який залежить від низки факторів: надійності впровадження, якості сервісу та ступеня захисту самого інструменту від зовнішніх атак.

Для забезпечення безпеки даних, що передаються у віртуальних захищених мережах, повинні бути вирішені такі основні завдання мережевої безпеки:

- взаємна аутентифікація абонентів при встановленні з'єднання;
- забезпечення конфіденційності, цілісності та достовірності інформації, що передається;
- авторизація та управління доступом;
- охорона периметра мережі та виявлення вторгнень;
- Управління мережевою безпекою.

Завдання мережевої безпеки

Процедура аутентифікації дозволяє законним користувачам увійти в систему та запобігає доступу небажаних осіб до мережі. Сучасні засоби ідентифікації та аутентифікації повинні відповідати двом умовам:

- Дотримуйтесь єдиного входу
- бути стійким до мережевих загроз (пасивне і активне прослуховування мережі).

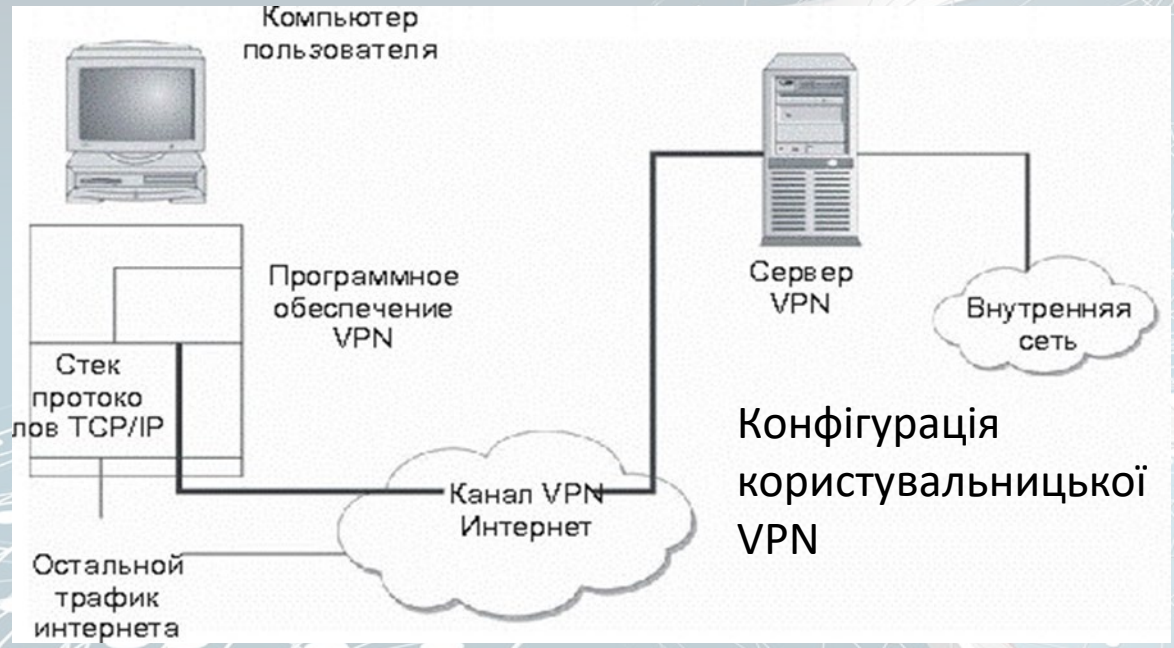
Завданням забезпечення конфіденційності інформації є захист переданих даних від несанкціонованого зчитування і копіювання. Основним засобом забезпечення конфіденційності інформації є шифрування.

Система авторизації надає легальним користувачам не тільки певні права доступу до каталогів, файлів і принтерів, а й регулює доступ користувача до шифрування пакетів, цифрового підпису та певних VPN-пристроїв.

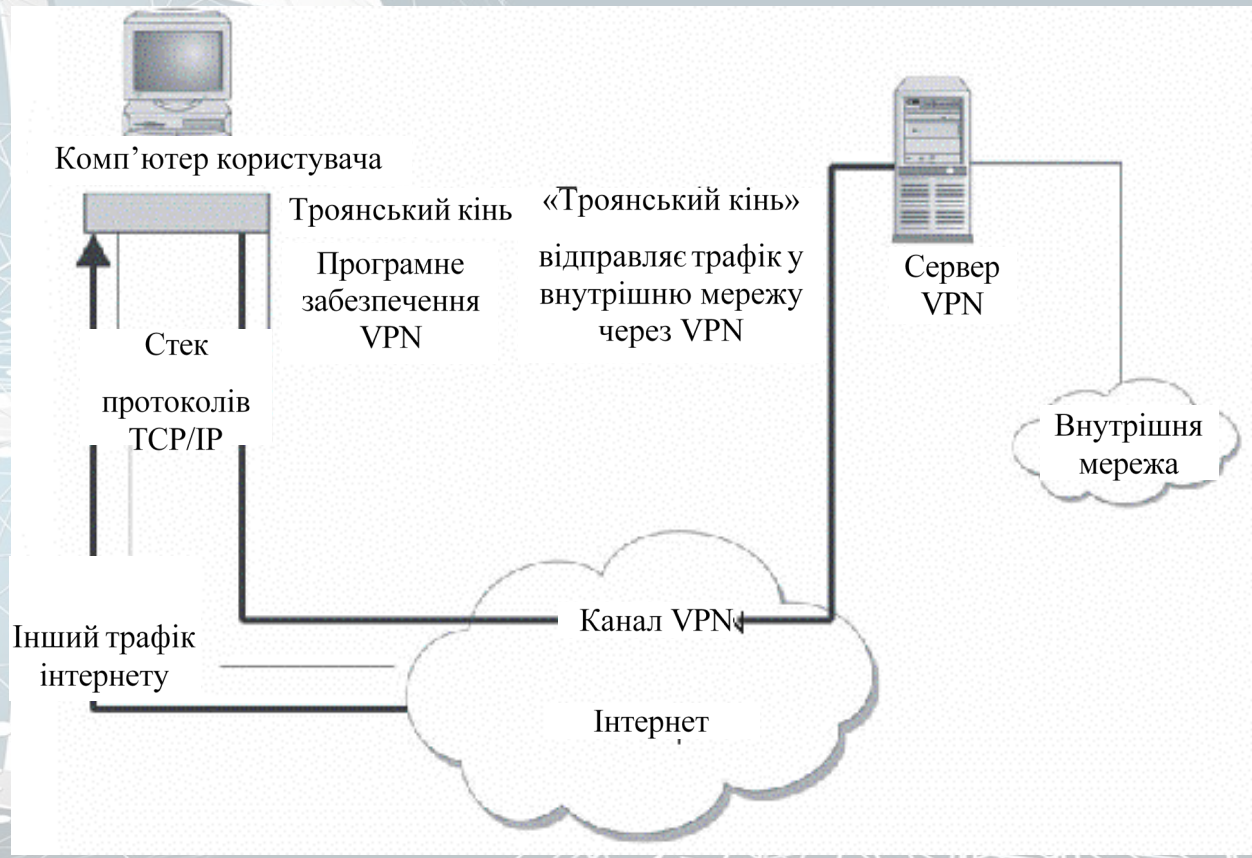
Використання інструментів безпеки, таких як брандмауери, системи виявлення вторгнень, системи аудиту безпеки та антивірусні пакети, забезпечує систематичний захист даних, що переміщуються по мережі.

VPN дозволяють компаніям визначати, який рівень управління мережею вони повинні зберегти і які функції слід передати постачальникам послуг. Багато компаній вважають за краще здійснювати повний контроль над розгортанням і роботою своїх VPN і, відповідно, хочуть мати комплексну систему управління мережею, засновану на політиці безпеки компанії.

Розгортання користувальницьких віртуальних приватних мереж



Конфігурація користувальницької VPN



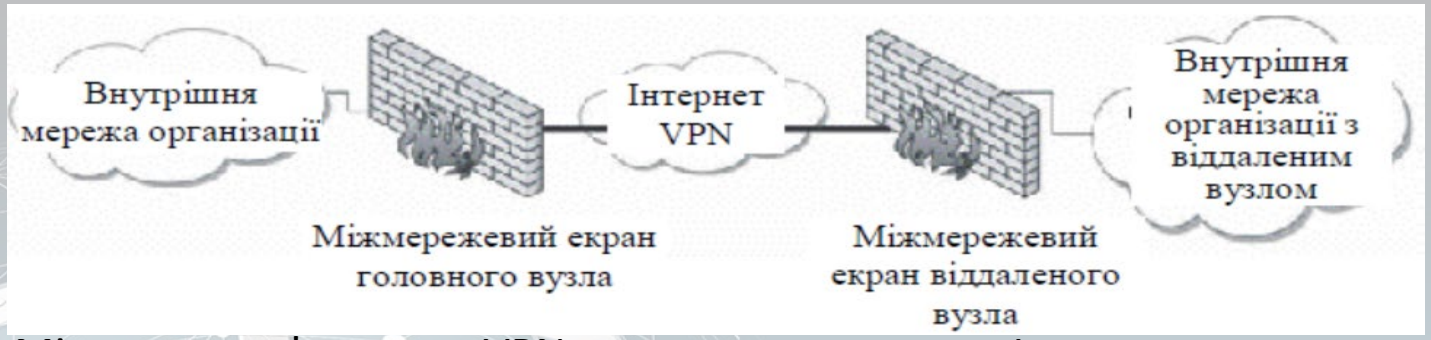
Використання "троянського коня" для проникнення у внутрішню мережу організації

Користувальницькі VPN володіють двома основними перевагами:

- Співробітники, що перебувають у відрядженні, можуть здійснювати доступ до електронної пошти, файлів і внутрішніх систем у будь-який час.
- Співробітники, що працюють дома, можуть здійснювати доступ до служб мережі, як і співробітники, що працюють в організації, без оренди дорогих виділених каналів.

Розгортання вузлових мереж VPN

Вузлові віртуальні приватні мережі використовуються організаціями для підключення до віддалених вузлів без застосування дорогих виділених каналів або для з'єднання двох різних організацій, між якими потрібен зв'язок для здійснення інформаційного обміну, пов'язаного з діяльністю цих організацій. Як правило, VPN з'єднує один міжмережевий екран або прикордонний маршрутизатор з іншим аналогічним пристроєм (рис.)



Міжвузлове з'єднання VPN, що проходить через Інтернет



Вузлова VPN може викликати конфлікти, пов'язані з адресацією



Вузлова VPN використовує NAT для запобігання конфліктів адресації

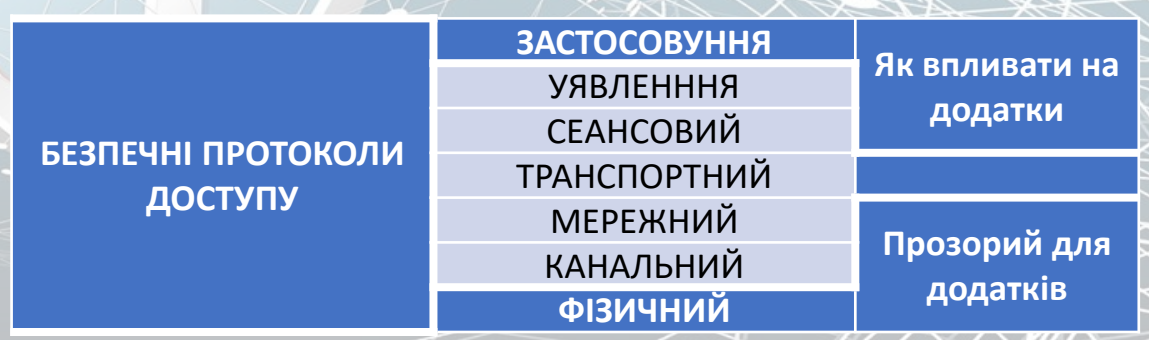
Класифікація VPN (1)

Існують різні варіанти класифікації VPN. Найчастіше використовуються такі три класифікаційні ознаки:

- операційний рівень моделі OSI;
- архітектура технічного рішення VPN;
- спосіб технічної реалізації VPN.

Класифікація VPN за операційним рівнем моделі OSI. Виходячи з операційного рівня моделі OSI, виділяють такі групи VPN:

- VPN на рівні каналу;
- VPN на мережевому рівні;
- VPN на рівні сеансу.



Класифікація VPN (2)

Класифікація VPN за архітектурою технічних рішень. За архітектурою технічного рішення прийнято виділяти три основні типи віртуальних приватних мереж:

- Внутрішні VPN
- VPN з віддаленим доступом;
- VPN для бізнесу.

Класифікація VPN за технічною реалізацією. Конфігурація та характеристики віртуальної приватної мережі багато в чому визначаються типом використовуваних VPN-пристроїв. За способом технічної реалізації виділяють наступні групи VPN:

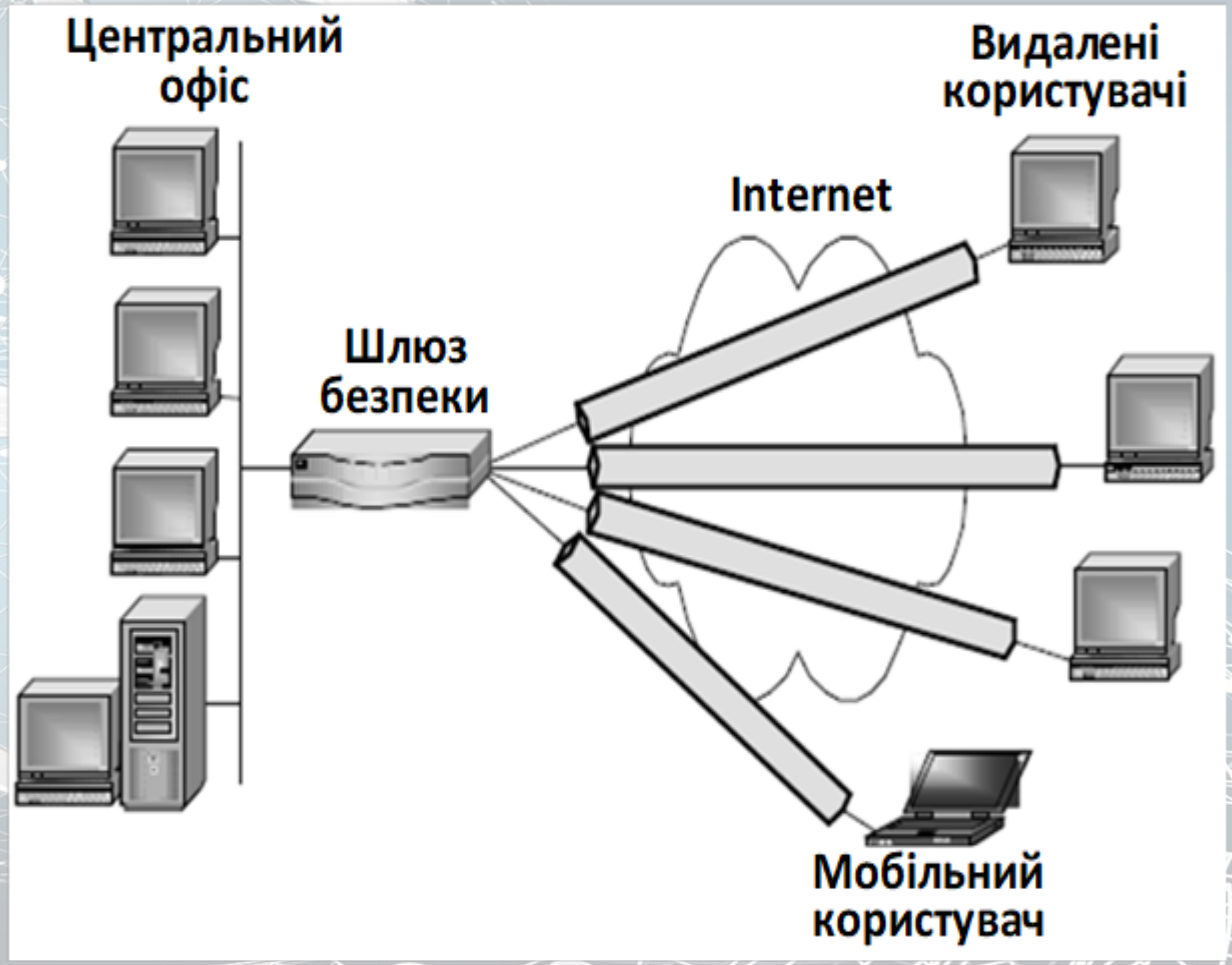
- VPN на базі маршрутизатора;
- VPN на базі брандмауера;
- Програмні VPN
- VPN на базі спеціалізованого обладнання з вбудованими процесорами шифрування.

VPN для віддаленого доступу

VPN з віддаленим доступом (рис.) отримали широке визнання завдяки значному зниженню щомісячних витрат на комутовані та виділені лінії. Принцип їх роботи простий: користувачі встановлюють з'єднання з місцевою точкою доступу WAN, а потім тунелюють свої дзвінки через Інтернет, уникаючи міжміських і міжнародних зборів або виставляючи рахунки за безкоштовні міжміські номери. Потім всі дзвінки концентруються на відповідних вузлах і передаються в корпоративні мережі.

Перехід на VPN з віддаленим доступом має ряд переваг, зокрема:

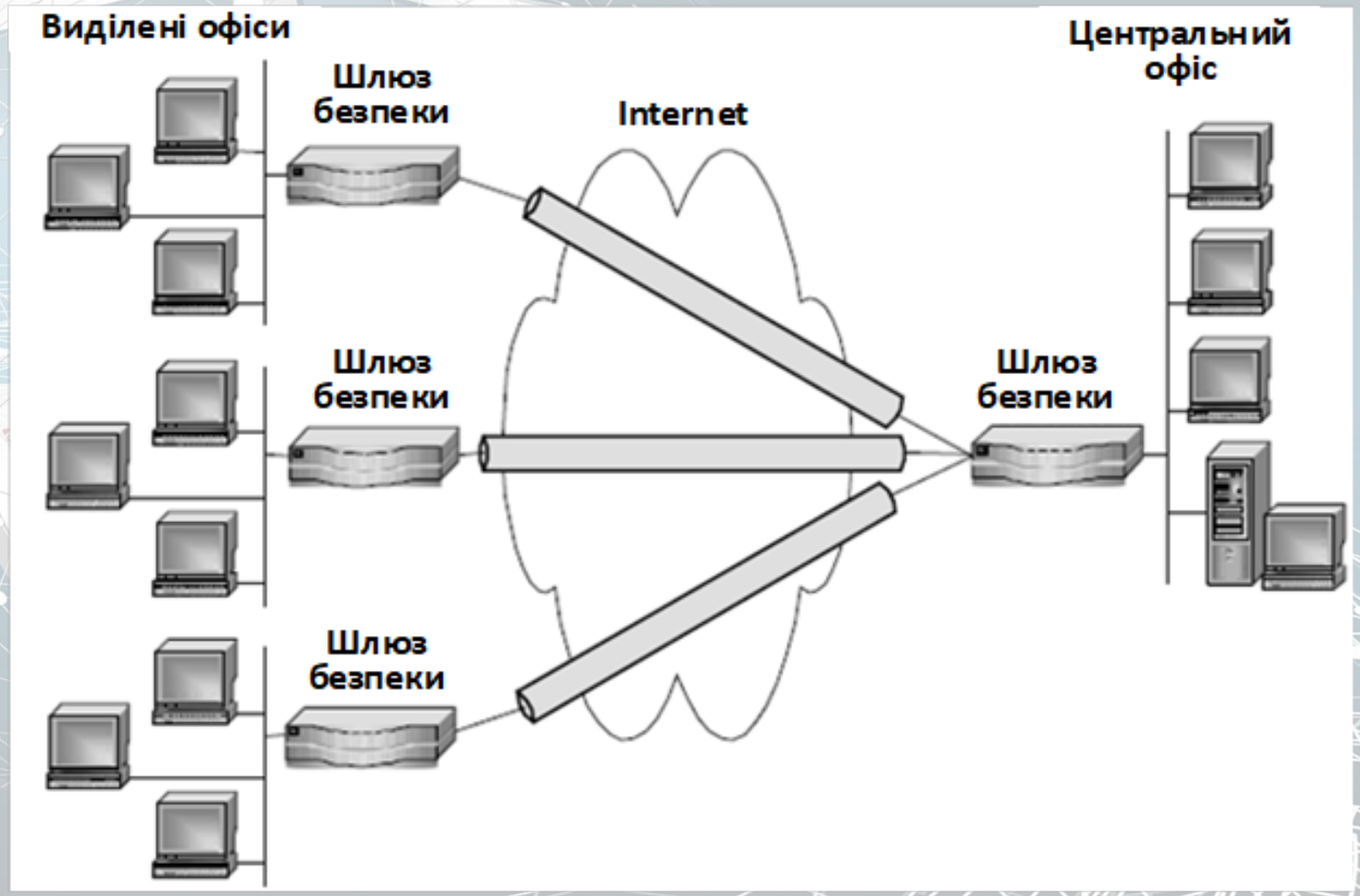
- Ефективна система аутентифікації для віддалених та мобільних користувачів, яка забезпечується надійною процедурою аутентифікації;
- Висока масштабованість і простота розгортання для нових користувачів, доданих до мережі.
- Зосередження уваги компанії на основних корпоративних бізнес-цілях замість того, щоб зосереджуватися на мережевих операціях.



Внутрішньокорпоративний VPN

Внутрішні корпоративні VPN використовуються для організації безпечного зв'язку між відділами всередині підприємства або між групою підприємств, об'єднаних корпоративними мережами зв'язку. Переваги:

- Використовуйте потужні протоколи криптографічного шифрування даних для захисту конфіденційної інформації.
- Надійність критично важливих додатків, таких як автоматизовані системи продажів і системи управління базами даних
- Гнучкість управління для більш ефективного пристосування до швидко зростаючої кількості нових користувачів, нових офісів і нових програмних додатків.

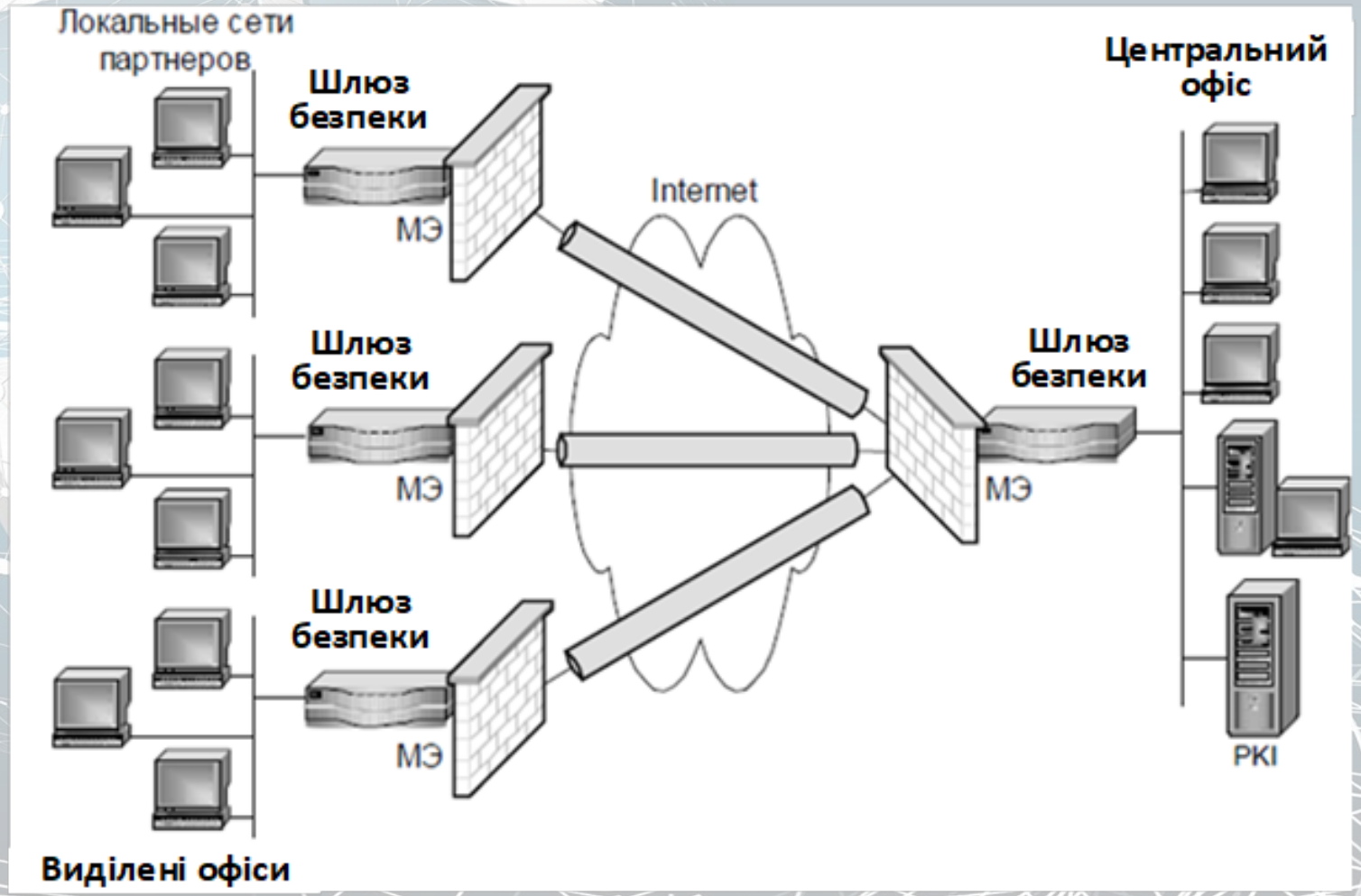


Міжкорпоративні VPN

Міжкорпоративні VPN використовуються для організації ефективної взаємодії та безпечного обміну інформацією зі стратегічними бізнес-партнерами, включаючи іноземних, великих постачальників, великих замовників, змовників тощо .

Екстранет - це мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії в мережу іншої, тим самим підвищуючи надійність зв'язку, що підтримується в ході ділових відносин.

З'єднання Extranet-VPN розгортаються з використанням тієї ж архітектури та протоколів, що використовуються в реалізаціях intranet-VPN та VPN віддаленого доступу. Основна відмінність полягає в тому, що дозвіл на доступ, який надається користувачам VPN в екстранет, прив'язаний до мережі їхнього партнера



Основні типи технічної реалізації VPN

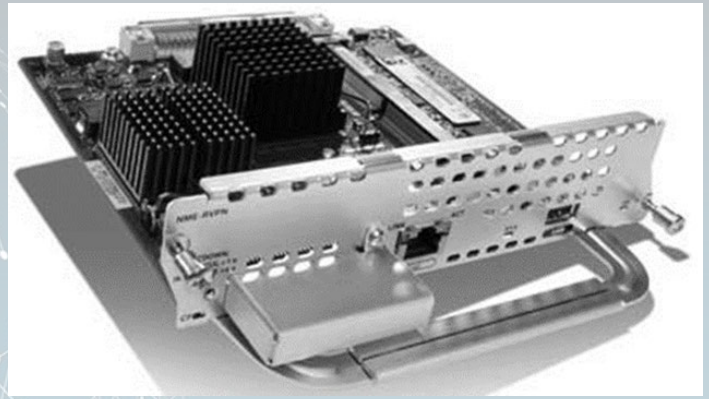
Для побудови VPN можуть використовуватися інструменти мережевого захисту наступних категорій:

- Сервери віддаленого доступу, які дозволяють створювати безпечні тунелі на канальному рівні еталонної моделі взаємодії з мережею OSI.
- Маршрутизатори з вбудованими функціями VPN, які підтримують протоколи VPN з'єднання OSI та мережевого рівня.
- брандмауери, можливо, включають сервери віддаленого доступу та дозволяють створювати VPN на рівнях зв'язку, мережі та сеансу моделі OSI;
- автономне програмне забезпечення, що дозволяє створювати VPN переважно на рівні мережі та сеансу моделі OSI;
- спеціалізоване обладнання, орієнтоване на формування захищених тунелів на канальному та мережевому рівнях моделі OSI.

За способом технічної реалізації виділяють такі групи VPN:

- VPN на базі маршрутизатора;
- VPN на базі брандмауера;
- Програмні VPN
- VPN на базі спеціалізованого обладнання
- веб-системи.

Сучасні VPN-продукти. S-Terra CSP



Повний набір функцій мережевої безпеки CSP VPN забезпечує:

- захист окремих користувачів;
- захист сервера;
- захист окремих мереж;
- захист спеціалізованих пристроїв

Продукти CSP VPN надають базовий функціонал сучасного VPN-пристрою:

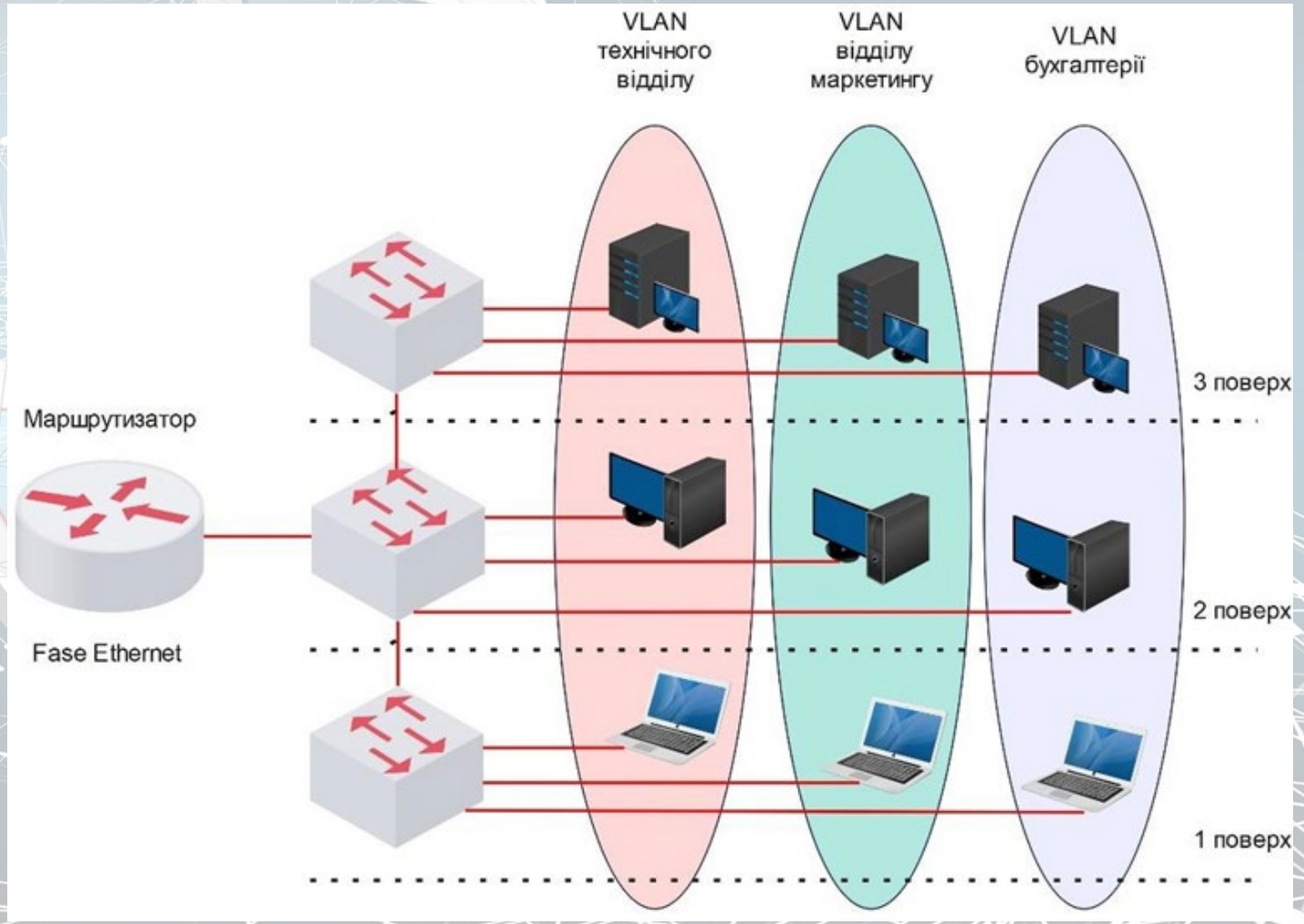
- шифрування (конфіденційність) та EDS (цілісність, аутентичність) IP-пакетів, цілісність потоку пакетів;
- Маскування топології мережі шляхом інкапсуляції трафіку в захищений тунель
- прозорість для NAT (підтримка інкапсуляції ESP-пакета в UDP);
- аутентифікація хоста і користувача, контроль доступу на рівні комп'ютерів, користувачів і додатків, інтегрований брандмауер 4-го класу (CSP VPN Gate відповідає вимогам, що пред'являються до брандмауера по 4-му класу безпеки);
- Забезпечте надійність за допомогою балансування навантаження в схемі резервування
- N + 1 (протокол виявлення мертвих пірів);
- уніфікація політики безпеки для мобільних та внутрішніх користувачів (динамічна настройка корпоративних IP-адрес для віддалених користувачів всередині VPN);
- збереження класифікації трафіку для захищених пакетів, пріоритетна обробка голосового та відео трафіку (підтримка QoS), відсутність втрати пакетів при регенерації сесійного ключа (Smooth IKE Re-keying);
- Гнучке, централізоване та засноване на подіях ведення журналу з вторинною обробкою на основі протоколу Syslog.

Питання для самоконтролю

1. Що таке віртуальні безпечні VPN?
2. Сформулюйте концепцію побудови віртуальних безпечних VPN-мереж.
3. Поясніть такі поняття: віртуальний захищений тунель, тунелювання та інкапсуляція.
4. Надайте детальні визначення пристроїв, таких як VPN-клієнт, VPN-сервер і шлюз безпеки VPN.
5. Поясніть особливості будови та функціонування двох основних схем віртуальних захищених каналів.
6. Які функції виконує ініціатор тунелю та термінатор тунелю?
7. Які методи використовуються для захисту VPN?
8. Класифікуйте VPN за моделлю сумісності відкритих систем OSI.
9. Які основні архітектури VPN? Надайте пояснення до кожного з трьох основних варіантів.
10. Вкажіть основні типи технічних реалізацій VPN та надайте пояснення до кожного з них.
11. Які російські компанії зараз випускають VPN-продукти?
12. Порівняйте можливості та основні характеристики VPN-продуктів сімейства CSP VPN 3.0 від російської компанії S-Terra CSP та сімейства пристроїв мережевої безпеки ASA 5500 Series від Cisco Systems.

Призначення віртуальних локальних мереж

Технологія віртуальних локальних мереж дозволяє подолати вказане обмеження. Віртуальної локальної мережею (Virtual Local Area Network, VLAN) називається група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, хоча фізично при цьому вони можуть бути під’єднані до різних мережевих комутаторів (рис.)
Основне призначення технології VLAN полягає в полегшенні процесу створення ізольованих мереж, які потім, зазвичай, зв’язуються між собою за допомогою маршрутизаторів. Така побудова мережі створює потужні бар’єри на шляху небажаного трафіку з однієї мережі в іншу. Будь-яка велика мережа повинна включати маршрутизатори, інакше потоки помилкових кадрів, наприклад широкотрансляційних, будуть періодично «затоплювати» всю мережу через прозорі для них комутатори, приводячи її в неробочий стан.

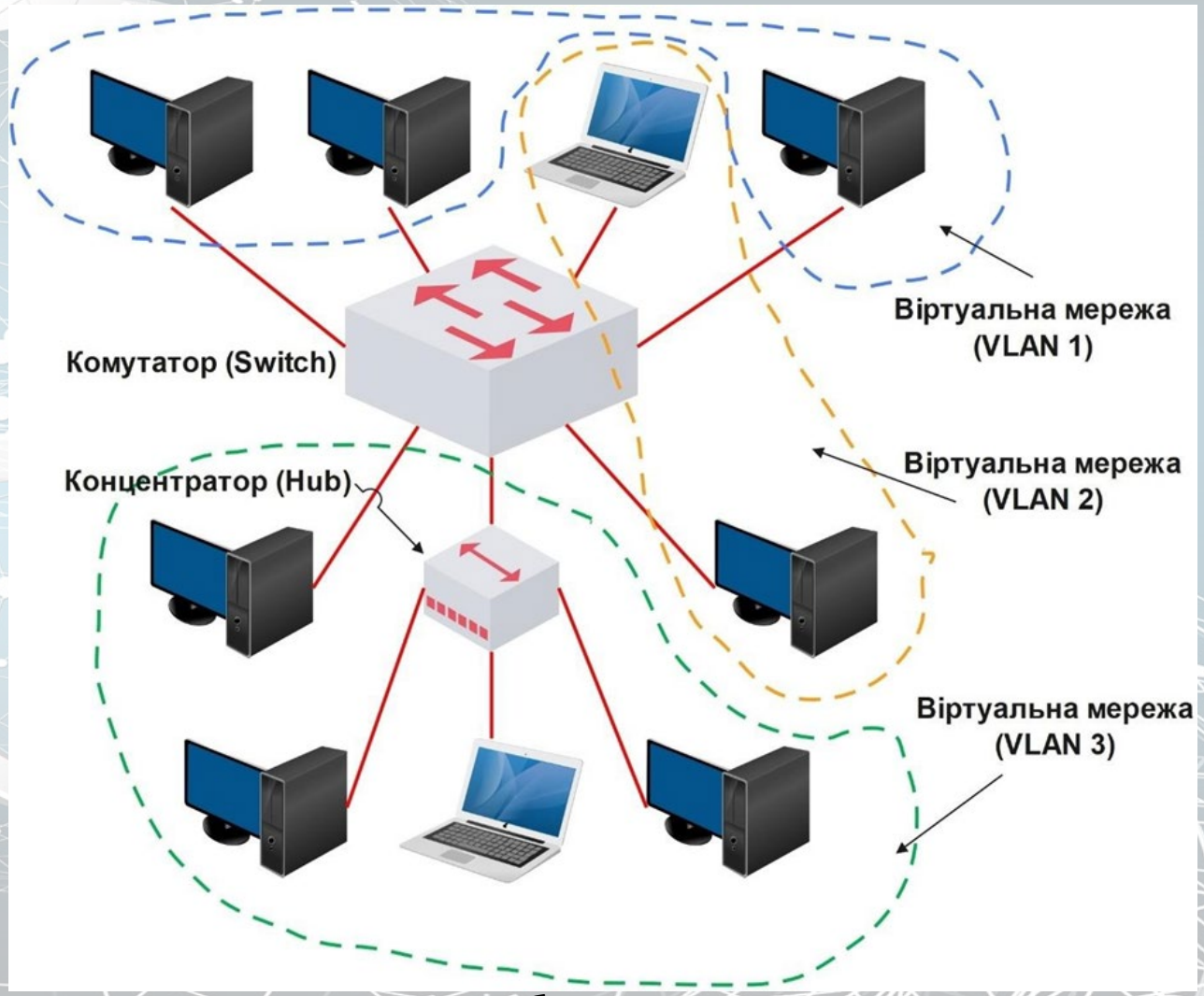


Методи побудови віртуальних мереж (1)

Існує декілька методів побудови віртуальних мереж:

- port-based VLAN – базується на приналежності портів до віртуальних мереж;
- MAC-based VLAN – базується на приналежності вузлів до різних VLAN на основі MAC-адреси;
- tag-based VLAN – базується на ідентифікаторах IEEE 802.1Q (тегах), що додаються в заголовок канального рівня.

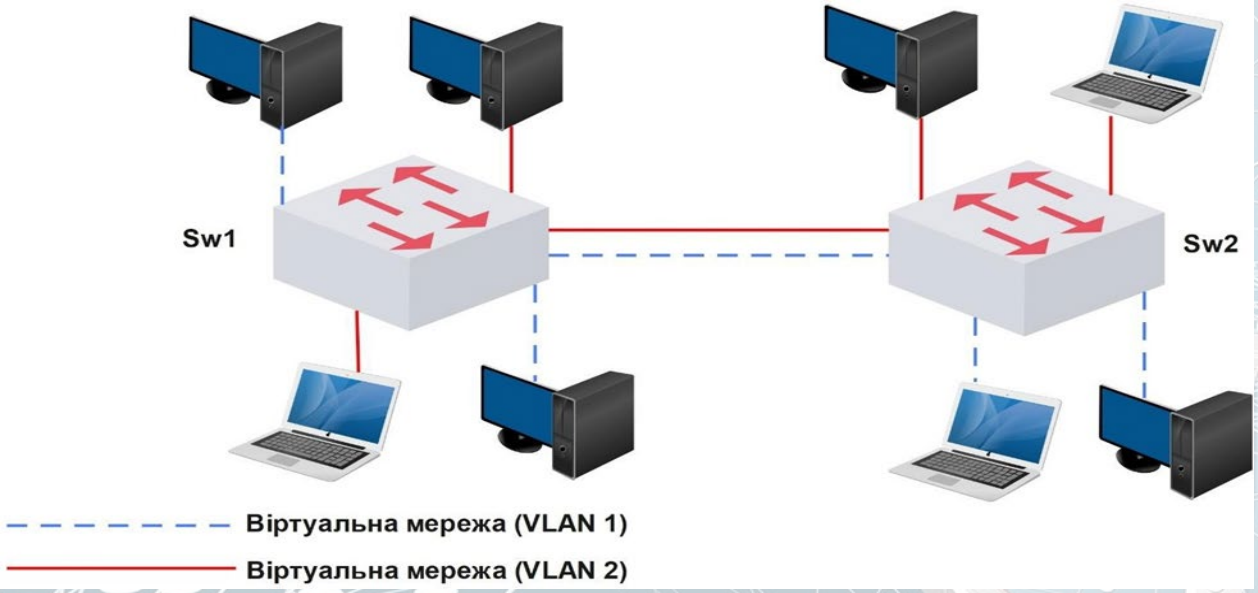
При створенні віртуальних мереж на основі одного комутатора, зазвичай використовується механізм групування портів комутатора – port-based VLAN (рис.)



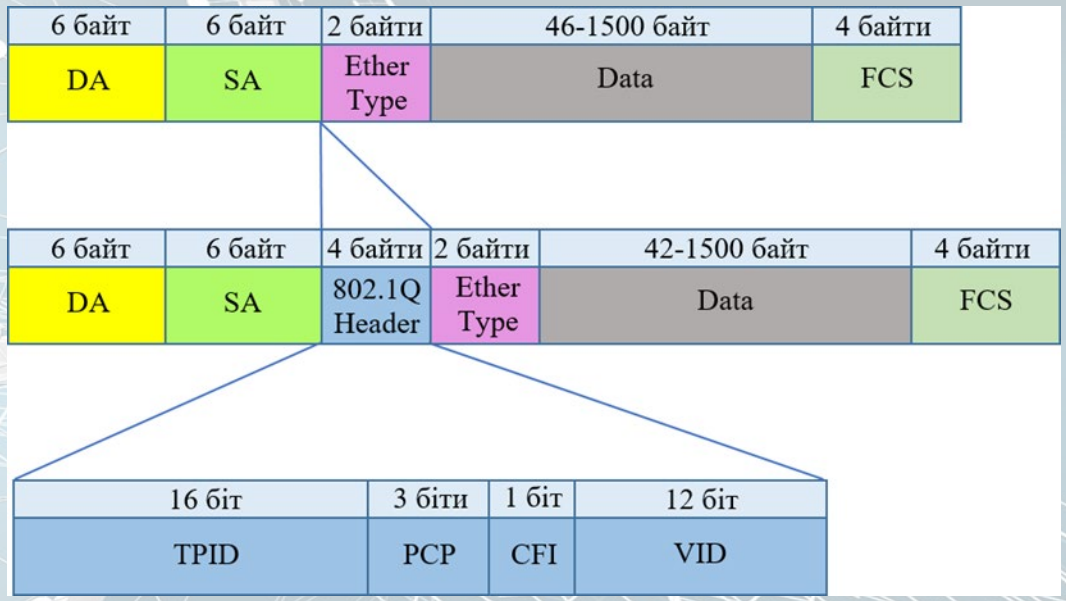
Віртуальні мережі, побудовані на одному комутаторі

Методи побудови віртуальних мереж (2)

Віртуальні мережі, побудовані на двох комутаторах за методом port-based VLAN



Додавання заголовку 802.1Q в кадр Ethernet
Поле TCI містить в собі поля PCP, CFI та VID.

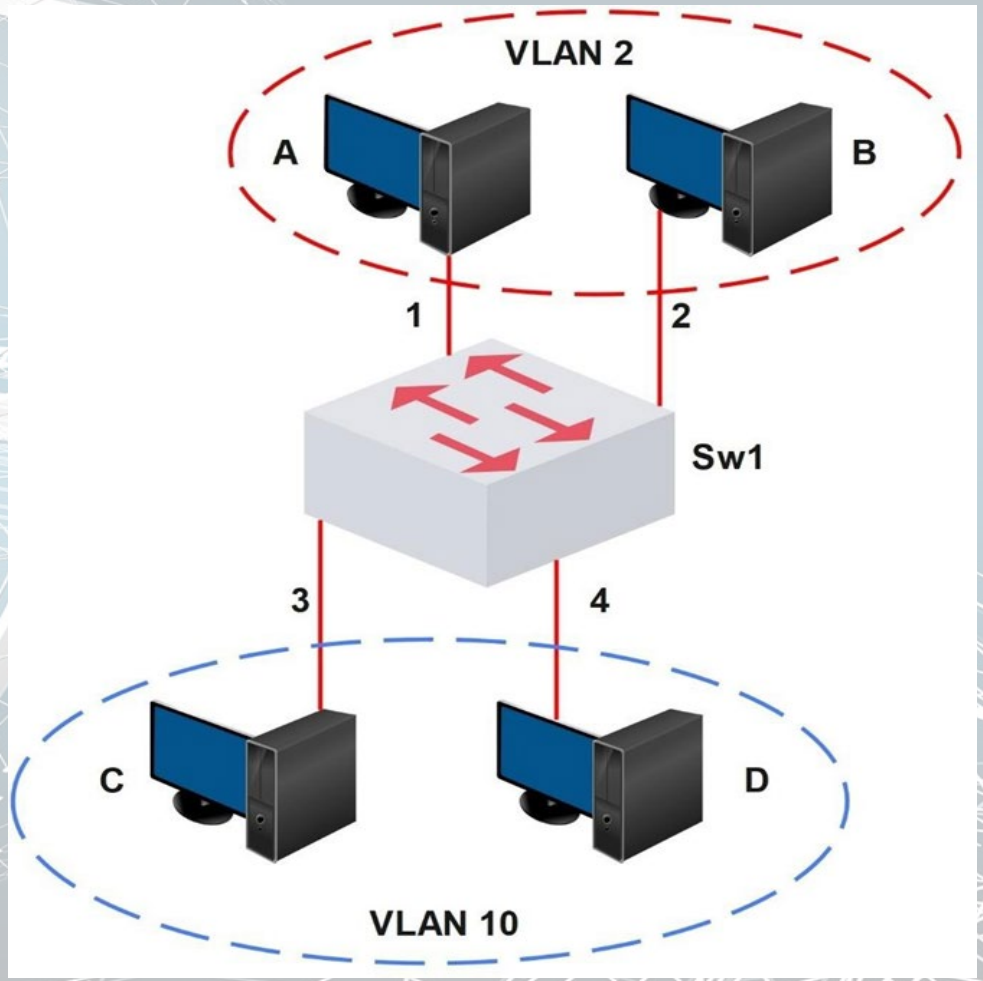


При створенні віртуальних мереж на основі одного комутатора, зазвичай використовується механізм групування портів комутатора – port-based VLAN (рис. ліворуч).

На рис.(праворуч) показану структуру тегованого кадру Ethernet. Тег віртуальної локальної мережі (32 біти) додається між MAC-адресою відправника (SA) й полем типу кадру (Ether Type). Два байти використовуються як ідентифікатор протоколу тегування (Tag Protocol Identifier, TPID), інші два байти – управляюча інформація (Tag Control Information, TCI).

Хости в різних VLAN на одному комутаторі

Усі порти комутатора вважаються нетегованими членами VLAN1. В процесі налаштування або роботи комутатора вони можуть переміщатися в інші VLAN. На комутаторі, який зображений на рис. налагоджено дві VLAN, усі порти налагоджені як нетеговані (access-порти в термінології Cisco) у відповідних VLAN.



Таблиця комутації Sw1 для VLAN2:

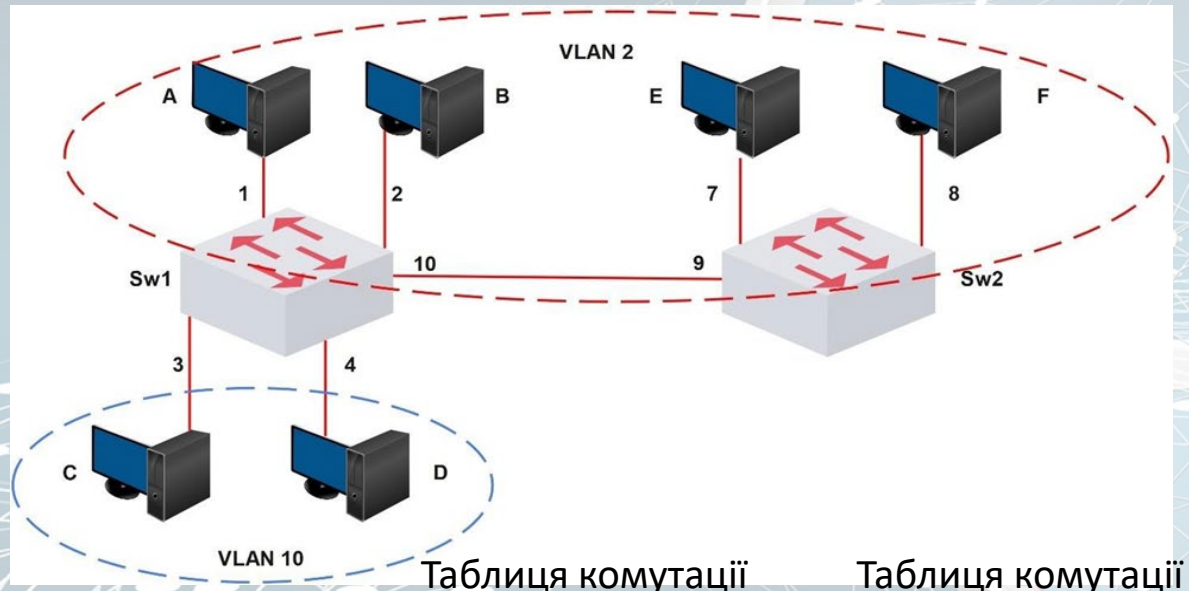
Порт комутатора	MAC-адрес хоста
1	A
2	B

Таблиця комутації Sw1 для VLAN10:

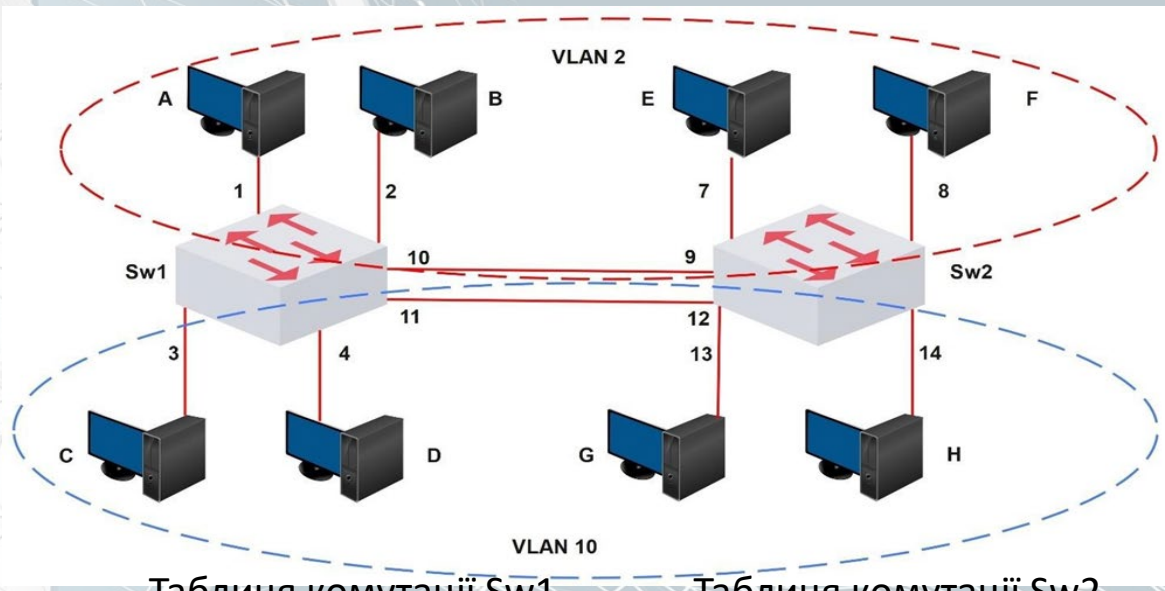
Порт комутатора	MAC-адрес хоста
3	C
4	D

Хости в різних VLAN на різних комутаторах

Хости в різних VLAN на різних комутаторах



До комутатора Sw2 додано два хоста G і H



Таблиця комутації Sw2

Порт комутатора	MAC-адрес хоста
7	E
8	F

Таблиця комутації Sw1 для VLAN2

Порт комутатора	MAC-адрес хоста
1	A
2	B
10	E
10	F

Таблиця комутації Sw2 для VLAN2:

Порт комутатора	MAC-адрес хоста
7	E
8	F
9	A
9	B

Таблиця комутації Sw1 для VLAN10

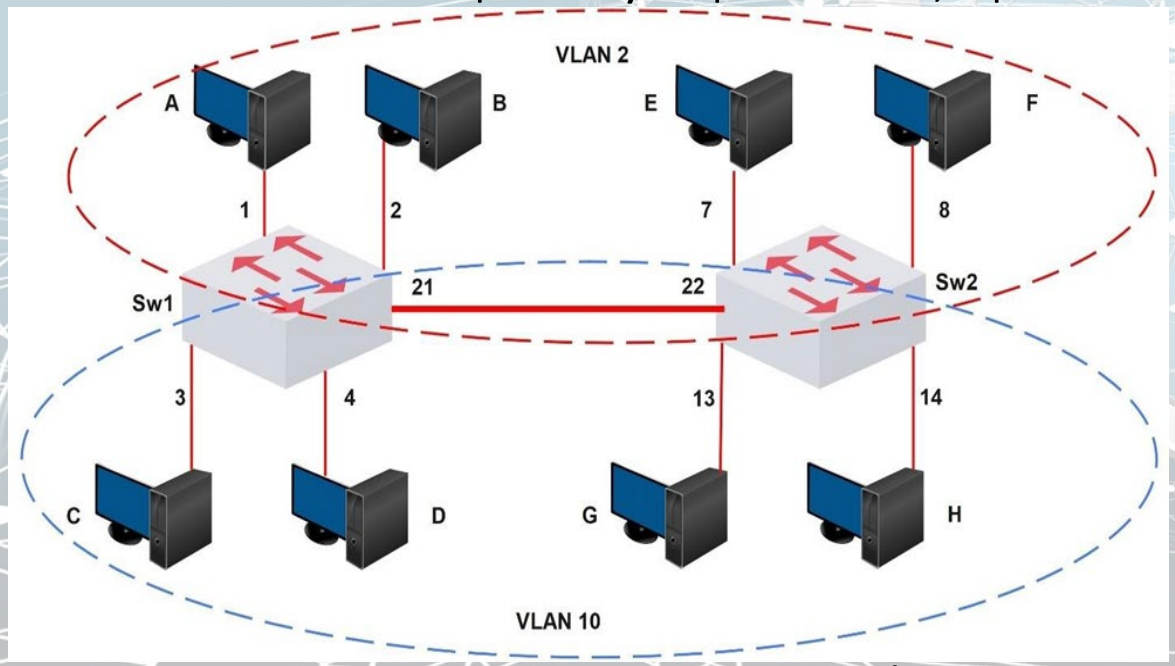
Порт комутатора	MAC-адрес хоста
3	C
4	D
11	G
11	H

Таблиця комутації Sw2 для VLAN10

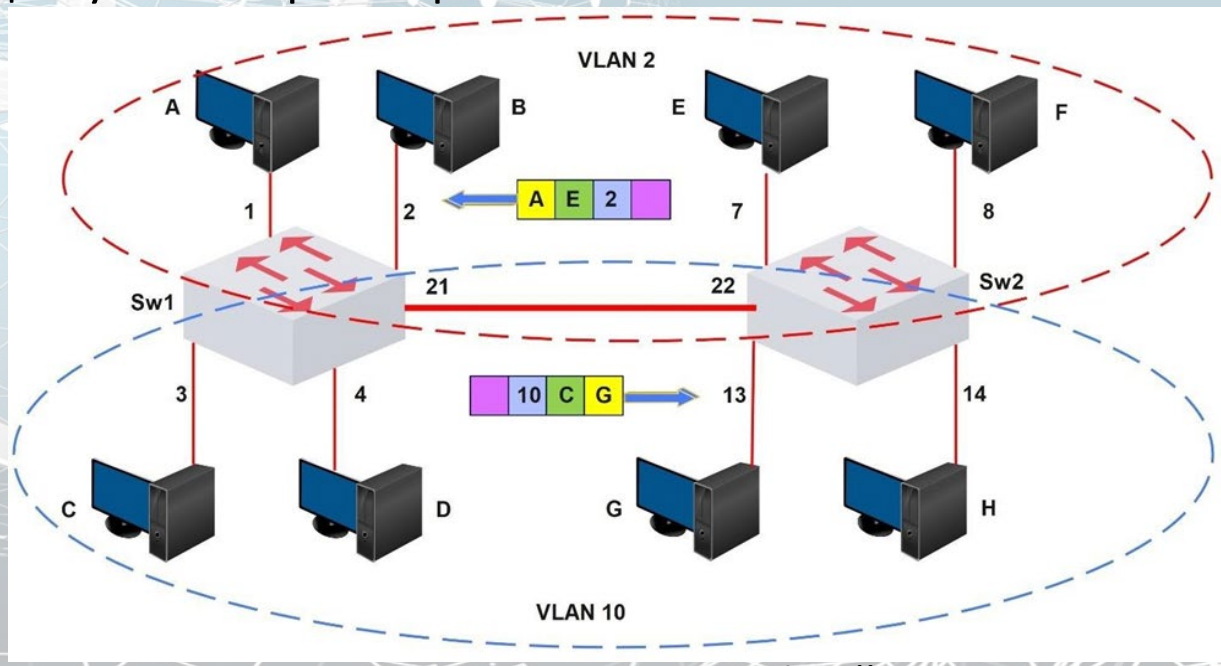
Порт комутатора	MAC-адрес хоста
13	G
14	H
12	C
12	D

Створення тегованого порту між комутаторами

- Коли кількість VLAN зростає, то розглянутий вище метод побудови віртуальних мереж стає незручним, оскільки для кожної VLAN необхідно буде додавати окремий лінк між комутаторами для того, щоб об’єднати хости в один широкотрансляційний сегмент. Для вирішення цієї проблеми використовують теговані порти (рис.ліворуч)
- Наприклад (рис. праворуч), якщо хост E передає фрейм хосту A, то комутатор Sw2 перевіряє свою таблицю комутації і бачить, що хост A доступний через порт 22.



Використання тегованих портів



Передавання тегованих фреймів

Типи VLAN

Віртуальні локальні мережі можна класифікувати за способом їх використання. Розрізняються наступні типи:

- мережа даних (Data VLAN) – використовуються для під’єднання вузлів, що генерують користувацький трафік.
- мережа, в якій знаходяться порти по замовчуванню (Default VLAN) – мережа для портів, які не визначені ні в одній VLAN. По замовчуванню – VLAN1.
- мережа для нетегованого трафіку (Native VLAN) – призначена для роботи з комутаторами, що не підтримують VLAN. По замовчуванню такою мережею є VLAN1. З міркувань безпеки рекомендується перепризначити Native VLAN на інший номер, наприклад 99.
- мережа для управління комутаторами (Management VLAN) – виділяється в цілях підвищення безпеки віддаленого управління комутаторами.
- мережа для голосових даних (Voice VLAN) – використовуються для передавання трафіку VoIP.

Налаштування VLAN на комутаторах Cisco

Якщо є необхідність створити відразу декілька віртуальних мереж, то параметром команди vlan можна їх перерахувати через кому, або вказати діапазон через дефіс – наприклад vlan 100,102,105-107.

```
Sw1#conf t
Sw1(config)#vlan 100
Sw1(config-vlan)#name test
```

Для призначення портів комутатора у віртуальні локальні мережі використовується команда режиму конфігурації порту switchport access vlan vlan-id, яка виконується після команди, що визначає режим роботи порту – switchport mode access. Приклад:

```
Sw1#conf t
Sw1(config)#in f0/1
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 100
Sw1(config-if)#
```

Для перевірки створених віртуальних мереж, можна використати команду show vlan brief.

Приклад:

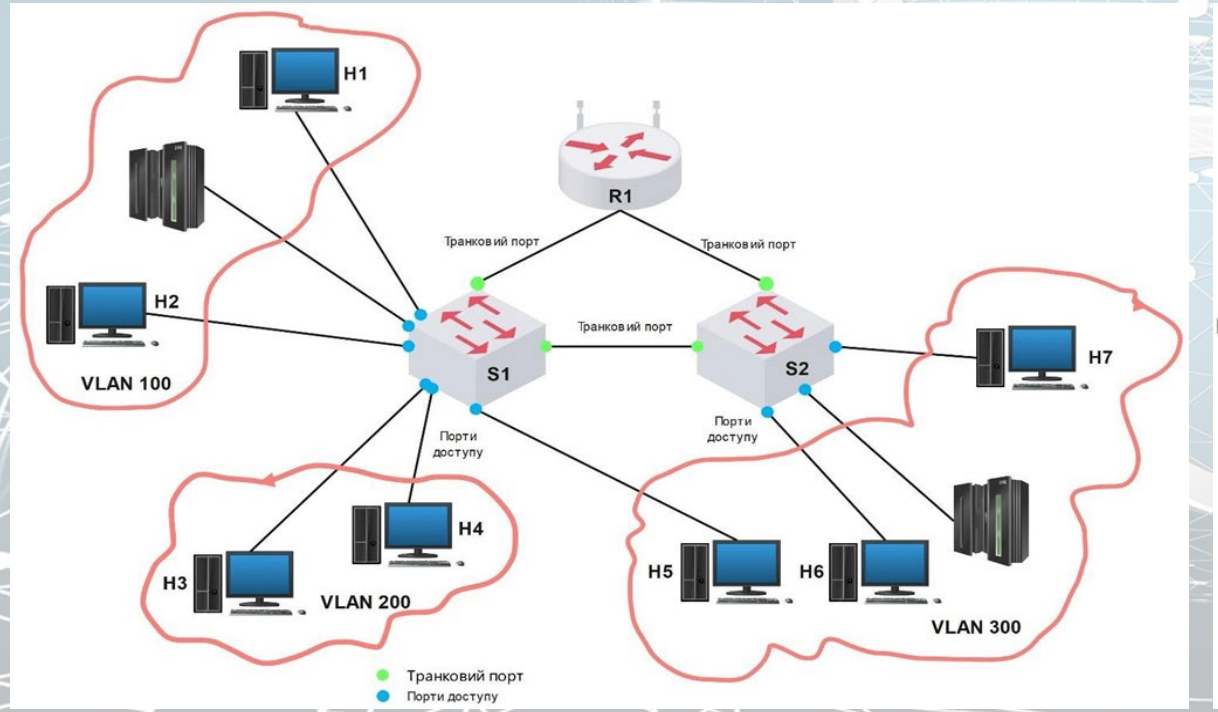
```
Sw1#sh vlan bri
VLAN Name                Status    Ports
1    default             active    Fa0/2, Fa0/3, Fa0/4, Fa0/5,
Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11,
Fa0/12, Fa0/13,
                                   Fa0/14, Fa0/15, Fa0/16,
Fa0/17, Fa0/18,
                                   Fa0/19, Fa0/20, Fa0/21,
Fa0/22, Fa0/23,
Fa0/24, Gi0/1, Gi0/2

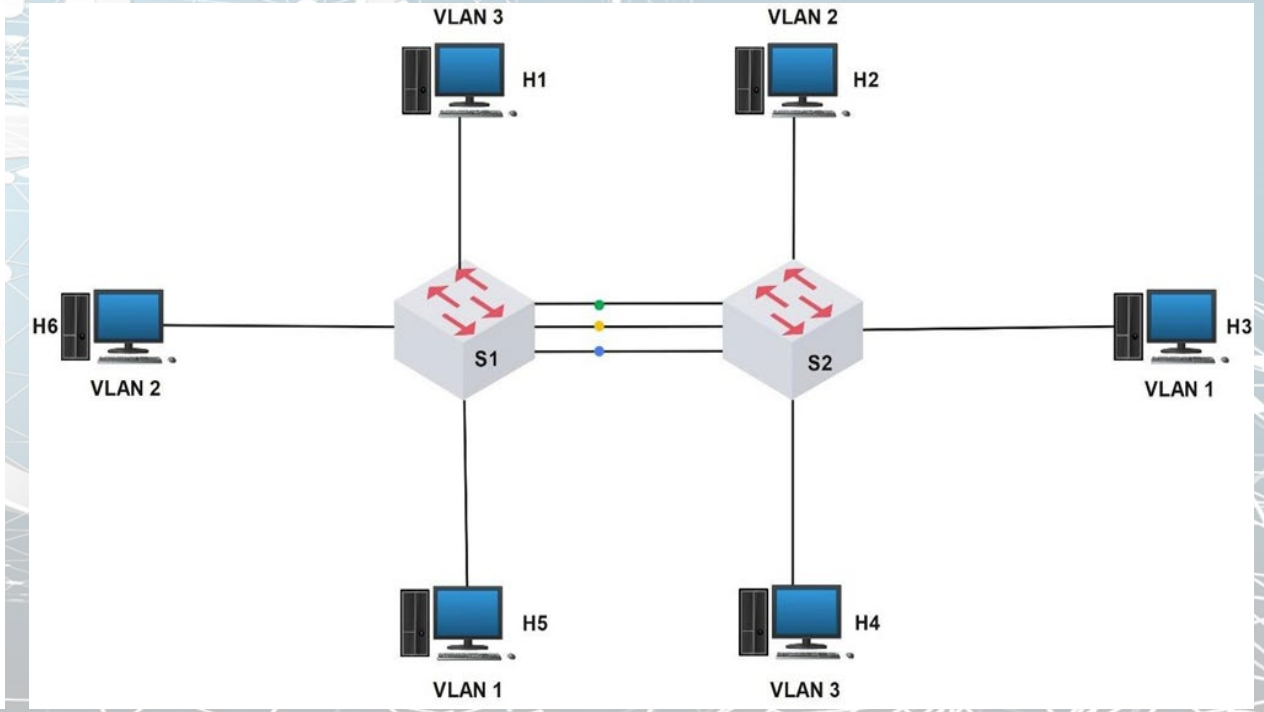
100  test                        active    Fa0/1
1002 fddi-default                act/unsup
1003 token-ring-default          act/unsup
1004 fddinet-default             act/unsup
1005 trnet-default               act/unsup
```

Транки VLAN (1)

Для портів комутатора можна задати дві різні ролі. Порт може бути визначений як порт доступу або як транковий порт (рис. ліворуч).

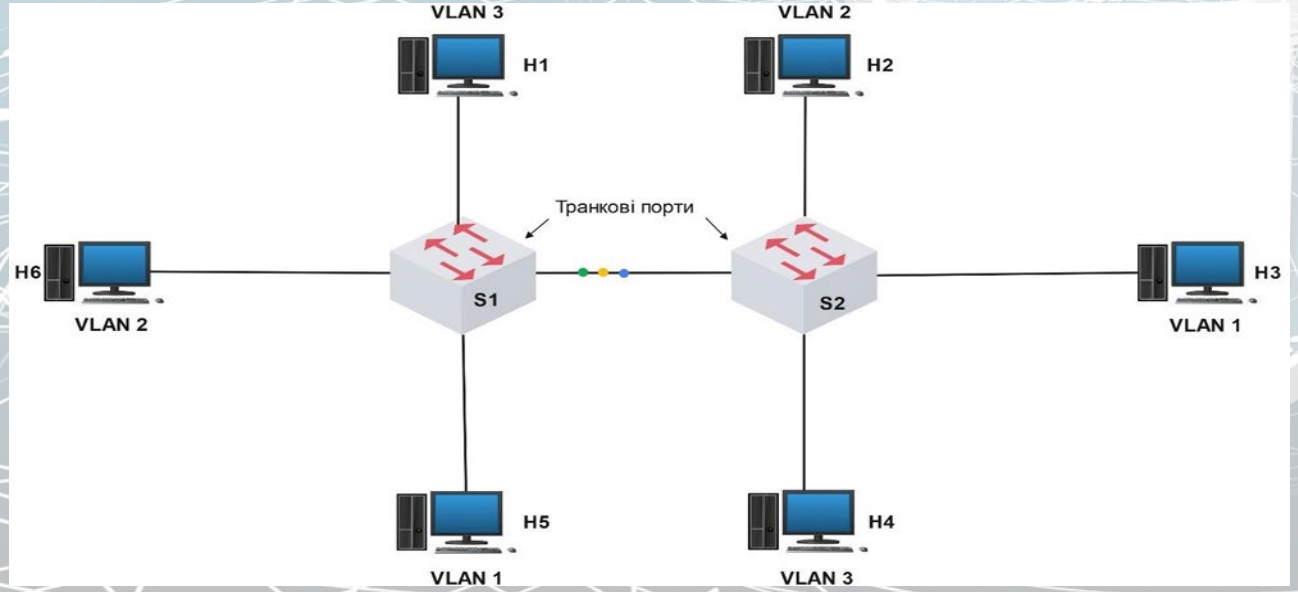
Без транкових портів для кожної VLAN потрібно було б окреме з’єднання між комутаторами. Наприклад, корпоративній мережі з трьох VLAN потрібно три канали зв’язку між комутаторами (рис. праворуч).





Транки VLAN (2)

При такій організації мережа не масштабується належним чином і дуже дорога. Транкові канали дозволяють вирішити цю проблему за рахунок передачі трафіку декількох VLAN через один канал (рис.).



По замовчуванню, порти комутатора працюють в режимі доступу. Щоб налаштувати порт комутатора в якості транкового порту, потрібно виконати наступні команди:

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}

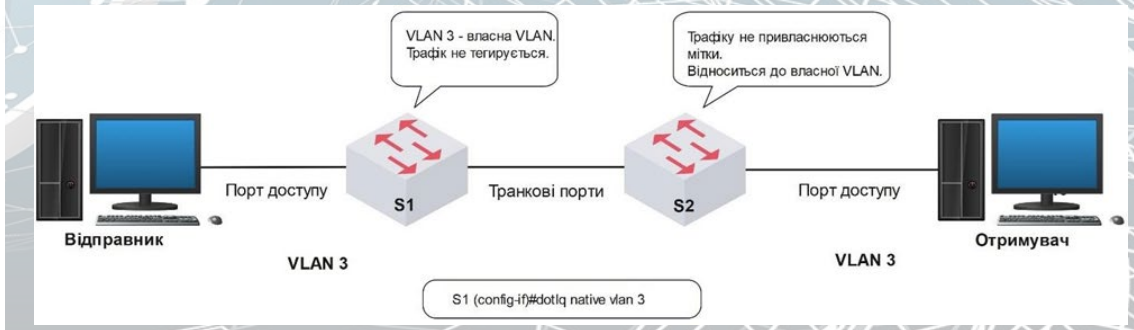
Щоб повернути транковий порт в режим доступу використовуються наступні команди:

Switch(config)#interface fa0/1

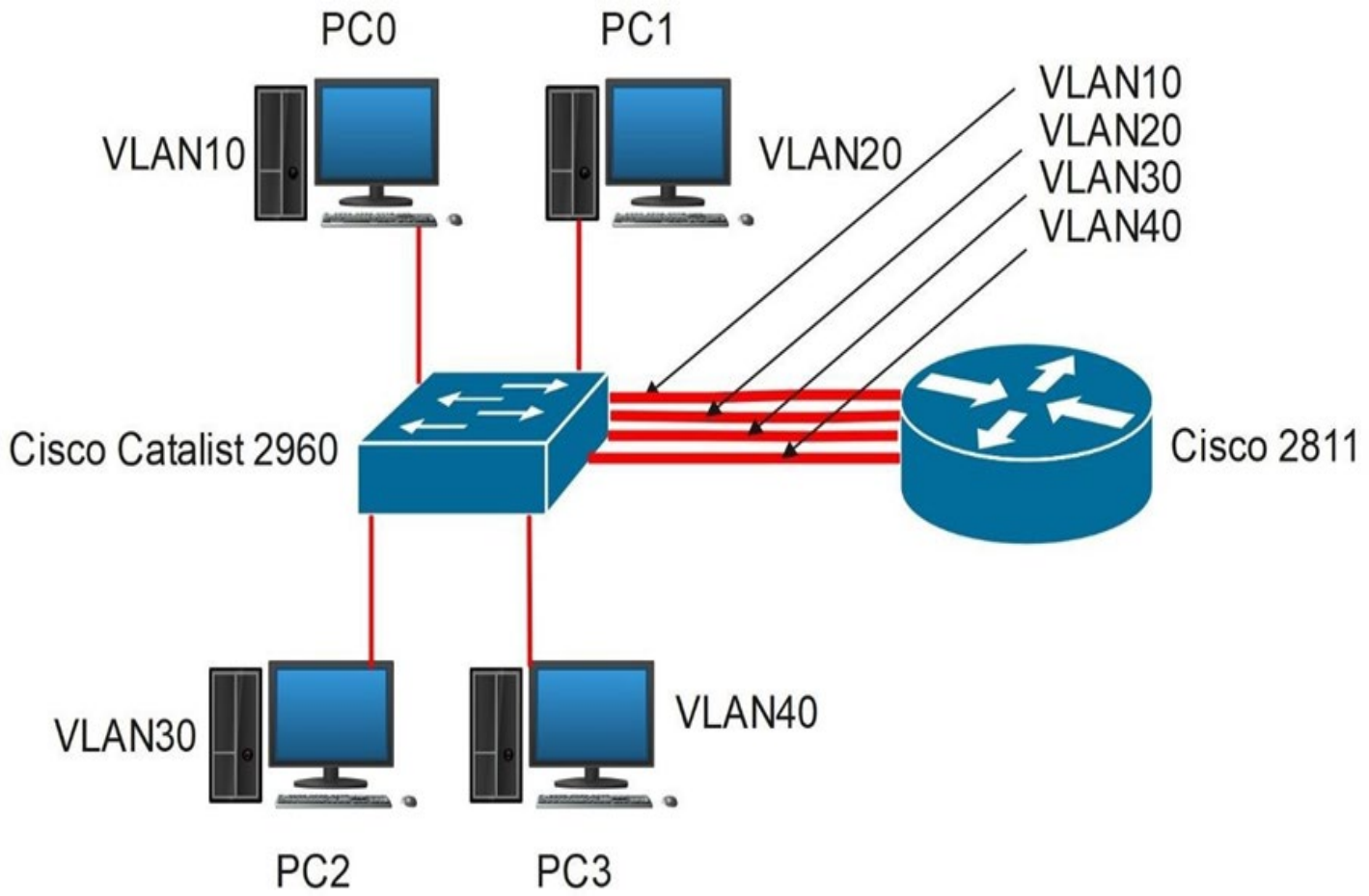
Switch(config-if)#no switchport mode trunk або

Switch(config-if)#switchport mode access

Для підтримки нетегованого трафіку використовується спеціальна VLAN, яка називається власною VLAN (native VLAN) (рис.)



Класичний метод маршрутизації між VLAN



Далі налаштовуємо інтерфейси маршрутизатора:

Router#conf t

Router(config)#int fa0/0

Router(config-if)#ip addr 10.1.1.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#int fa0/1

Router(config-if)#ip addr 10.1.2.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#int fa1/0

Router(config-if)#ip addr 10.1.3.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#int fa1/1

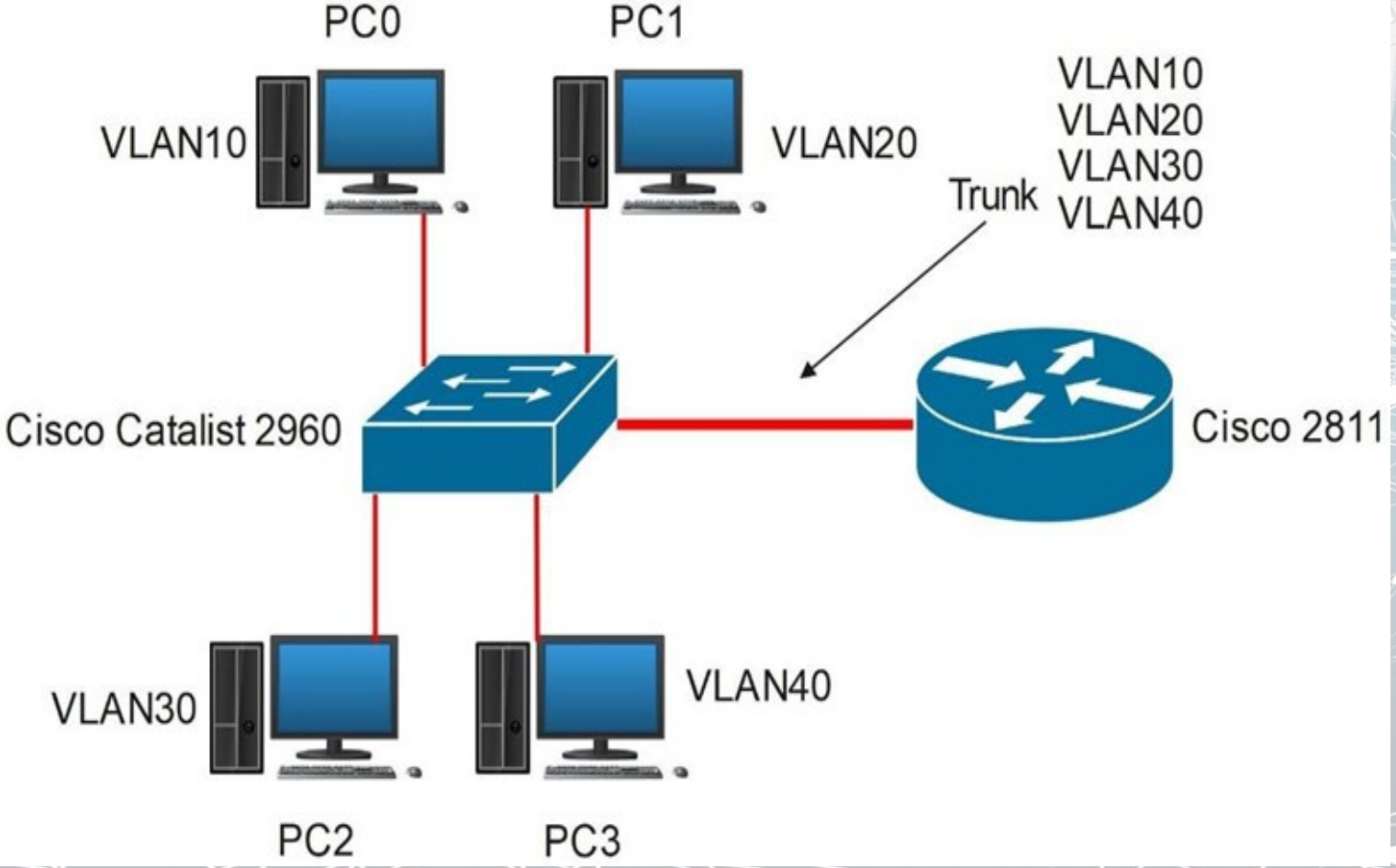
Router(config-if)#ip addr 10.1.4.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#^Z

Router#

Транковий метод маршрутизації між VLAN



Комп’ютери в даному прикладі під’єднані до портів fa0/2, fa0/3, fa0/4, fa0/5:

```
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#exit
Switch(config)#int fa 0/2
Switch(config-if)# switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/3
Switch(config-if)# switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa 0/4
Switch(config-if)# switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#int fa 0/5
Switch(config-if)# switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config-if)#
```

Пошук несправностей в конфігурації маршрутизації між VLAN

Типові помилки, що пов’язані з налаштуванням комутаторів:

- У конфігурації з окремими під’єднаннями до маршрутизатора для кожної VLAN – призначення інтерфейсу, до якого підключений маршрутизатор, у віртуальну мережу, що не відповідає налаштуванням маршрутизатора.
- У транковій конфігурації можлива ситуація, коли інтерфейс, до якого під’єднаний маршрутизатор працює в режимі доступу, а не як транк. Відповідно трафік віртуальних мереж не поступатиме до підінтерфейсів маршрутизатора.

Типові помилки, що пов’язані з налаштуванням маршрутизаторів:

- В конфігурації з окремими під’єднаннями до маршрутизатора для кожної VLAN – підключення порту маршрутизатора до порту комутатора, який не знаходиться в тій же віртуальній мережі, до складу якої повинен входити порт маршрутизатора.
- У транковій конфігурації типовою помилкою є неправильне задання номера VLAN на підінтерфейсі при його конфігуруванні.

Протокол VTP

Протокол VTP застосовується для створення, видалення, іменування VLAN і поширення інформації про віртуальні мережі усім комутаторам мережі. VTP працює тільки із звичайними (normal) VLAN – від 1 по 1005. Розширені (extended) номери VLAN не підтримуються цим протоколом.

Основні компоненти VTP:

- Домен VTP (Domain VTP) – група з’єднаних між собою комутаторів, що використовує загальне ім’я домена і конфігурацію VLAN.
- Оголошення VTP (VTP Advertisements) – кадри, за допомогою яких комутатори одного домена обмінюються інформацією між собою.
- Режими VTP – комутатори можуть бути сконфігуровані в одному з 3-х режимів участі в VTP: сервер, клієнт і прозорий (transparent).
- VTP сервер – комутатор, що має право змінювати список VLAN для свого домена. Такий комутатор зберігає інформацію про VLAN в NVRAM.
- VTP клієнт – комутатор, що відрізняється від сервера, тим, що не може вносити зміни в список VLAN. Інформація про VLAN зберігається в оперативній пам’яті, і видаляється при перезавантаженні.
- прозорий VTP – цей комутатор не бере участі в роботі домена VTP, але передає кадри VTP через свої транкові порти. Він працює тільки зі своєю локальною базою VLAN.
- Відсікання VTP (VTP Pruning) – механізм, що дозволяє зменшити область поширення інформації певних VLAN, тільки на ті комутатори, яким вона дійсно потрібна. Це дозволяє економніше використати пропускну спроможність транків.

Операції VTP. Налаштування VTP за умовчанням

Налаштування VTP, що задані по замовчуванню, дозволяють швидко та з мінімальним втручанням в конфігурацію, налаштувати комутатор для роботи в домені VTP. Побачити конфігурацію VTP можна командою show vtp status. На неналаштованому комутаторі це виглядатиме так:

```
Switch>en Switch#sh vtp status
VTP Version          2
Configuration Revision          0
Maximum VLANs supported locally          255
Number of existing VLANs      5
VTP Operating Mode            : Server
VTP Domain Name               :
VTP Pruning Mode              : Disabled
VTP V2 Mode       : Disabled
VTP Traps Generation          : Disabled
MD5 digest          : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00 Local updater ID is 0.0.0.0 (no valid interface found)
```

Основні параметри:

- VTP Version – версія протоколу VTP, усього існує 3 версії. Комутатори Catalyst 2960 підтримують 2-у версію, але по замовчуванню налаштовані на використання 1-ої версії.
- VTP V2 Mode – показує, чи використовується 2-а версія.
- Configuration Revision – 32-х бітне число, яке показує номер версії конфігурації VTP, збільшується на 1 при кожній зміні конфігурації. По замовчуванню рівне 0.
- Maximum VLANs supported locally – кількість VLAN, які підтримуються комутатором.
- Number of existing VLANs – кількість існуючих VLAN.
- VTP Operating Mode – режим участі комутатора в домені VTP.
- VTP Domain Name – ім’я домена VTP, по замовчуванню порожньо. Налаштування імені на номер версії конфігурації не впливає.

Операції VTP. Домени VTP

- Домен VTP є групою з’єднаних між собою комутаторів, що використовують загальне доменне ім’я. Комутатор може входити до складу тільки одного домена. Комутатори, які налагоджені з різними іменами домена, обмінюватися інформацією про VLAN не можуть. Також, комутатори у яких ім’я домена є порожнім, теж не можуть поширювати свою інформацію про наявні VLAN.
- Ім’я домена не обов’язково настроювати на усіх комутаторах вручну, протокол VTP поширює інформацію про ім’я у своїх оголошеннях. Комутатори, що не мають налагодженого імені, приймають його з оголошень одного налаштованого сервера

Операції VTP. Оголошення VTP

Оголошення VTP призначені для поширення інформації про конфігурацію VLAN і імені домена на комутатори, що сконфігуровані для використання VTP. Кадр VTP складається з двох частин – заголовка (VTP header) і тіла повідомлення (VTP message). Інкапсулюється він всередину кадру IEEE 802.1Q або ISL. Адреса призначення канального рівня є груповою – 01-00-0C-CC-CC-CC. Заголовок LLC SNAP вказує на протокол верхнього рівня VTP – поле PID дорівнює 2003.

Вміст заголовка VTP залежить від типу повідомлення. При цьому незалежно від типу, в заголовку містяться такі відомості:

- Ім’я домена.
- Довжина імені домена.
- Версія протоколу.
- Версія конфігурації.

У протоколі VTP є 3 типи повідомлень:

- Оголошення загальної інформації (Summary Advertisements) – таке повідомлення містить загальну інформацію VTP, наприклад ім’я домена, версію протоколу, версію конфігурації. Розсилається кожні 5 хвилин, або відразу після внесення змін до конфігурації.
- Оголошення мереж (Subset Advertisements) – ці повідомлення містять інформацію про віртуальні мережі і включають в себе інформацію про видалення, створення, зміну імені, активації, деактивації віртуальної мережі.
- Запит оголошення (Request Advertisements) – повідомлення, призначене для запиту інформації новопід’єднаним комутатором про конфігурацію VLAN. Посилається таке повідомлення, як правило, серверу VTP, який повинен відповісти попередніми двома повідомленнями. Приводом для відправки такого повідомлення служить або зміна імені домена, неспівпадання номера версії конфігурації, втрата повідомлення оголошення

Операції VTP. Режими роботи VTP

Комутатори Cisco можуть працювати в одному з трьох режимів VTP – клієнт, сервер або прозорий.

- Режим сервера – в цьому режимі комутатор може створювати, іменувати, змінювати і видаляти віртуальні мережі для свого домена. Режим сервера є режимом по замовчуванню для комутаторів Cisco. Сервер поширює свою інформацію через транкові з'єднання іншим комутаторам. Інші комутатори, отримуючи оголошення сервера, звіряють номер конфігурації зі своєю і визначають по ньому необхідність оновлення своєї конфігурації. Сервер зберігає інформацію про віртуальні мережі у своїй базі даних.
- Режим клієнта – в цьому режимі комутатор не може виконувати ніяких дій, пов'язаних зі змінами бази віртуальних мереж. Клієнт приймає інформацію про віртуальні мережі в оголошеннях від сервера і зберігає її у своїй оперативній пам'яті. Коли комутатор, що працює в режимі клієнта, вимикається або перезавантажується, уся інформація про віртуальні мережі втрачається. Після завантаження, такий комутатор просить інформацію у сервера за допомогою запиту оголошення.
- Прозорий режим – комутатор в такому режимі просто пересилає оголошення VTP через свої транкові порти, але участі в домені не бере. Прозорий комутатор має свою власну базу віртуальних мереж і оголошень про VLAN не розсилає.

Операції VTP. Відсікання VTP

- В кожній мережі присутній трафік, що розсилається усім комутаторам – це широкотрансляційні передачі і кадри з невідомим одержувачем. При використанні протоколу VTP інформація про відомі віртуальні мережі поширюється усім комутаторам домена, незалежно від логічної конфігурації мережі. Таким чином, широкотрансляційний трафік мереж, що підтримуються окремою групою комутаторів передається на усі інші, навіть якщо вузли цих мереж до них не під'єднані. Відсікання (pruning) дозволяє звільнити частину пропускної спроможності транкових з'єднань за рахунок обмеження області поширення інформації про певні віртуальні мережі тільки тими комутаторами, яким ці мережі дійсно потрібні.
- По замовчуванню, відсікання вимкнене, для його включення досить на одному з серверів домена VTP виконати команду режиму глобальної конфігурації – vtp pruning. Після включення, інформація про VLAN передаватиметься в транках тільки для тих комутаторів, у яких є порти в них. Відсікатися можуть тільки віртуальні мережі з номерами від 2 до 1001. Список мереж, що відсікаються, будується автоматично, але є можливість керувати цим списком вручну. Виконується управління цим списком в інтерфейсі конфігурації транкового порту командою switchport trunk pruning vlan

Конфігурування VTP (1)

Дії, які необхідно виконати для налаштування комутаторів, які виступатимуть в ролі серверів:

1. Спочатку необхідно переконається, що комутатори мають налаштування по замовчуванню. Зробити це можна командою show vtp status.
2. Обов'язково необхідно скинути номер конфігурації VTP. Якщо цього не зробити, може виникнути ситуація, коли наново підключений комутатор матиме версію конфігурації вищу, ніж існуюча в домені, і як результат існуюча конфігурація може бути зіпсована.
3. Для забезпечення відмовостійкості, на роль сервера VTP необхідно виділити хоча б два комутатори.
4. На одному з серверів задається ім'я домена, при цьому транкові порти мають бути сконфігуровані так, щоб через них почали поширюватися оголошення. Виконується це командою режиму глобальної конфігурації vtp domain domain-name.
5. Якщо комутатор додається до вже існуючого домена, то ім'я домена потрібно або очистити або задати вручну. При ручному налаштуванні імені слід враховувати регістр.
6. При використанні пароля VTP необхідно уважно відстежити його налаштування на усіх комутаторах. Пароль задається командою vtp password password.
7. Версія протоколу VTP також повинна співпадати на усіх комутаторах. Версія встановлюється командою vtp version number.
8. Віртуальні мережі необхідно створювати після включення VTP на сервері. Всі VLAN, що створені до цього, будуть видалені.

Приклад конфігурації:

```
 Switch> en
Switch#conf t
Switch(config)#vtp domain class
Switch(config)#vtp password cisco
Switch(config)#vtp version 1
Switch(config)#
```

Конфігурування VTP (2)

Дії, які необхідно виконати для налаштування комутаторів, які виступатимуть в ролі клієнтів:

1. Як і для сервера, переконається в тому, що є присутніми налаштування по замовчуванню.
2. Налаштувати режим VTP клієнта. Виконується командою vtp mode client. Приклад виконання:

Switch(config)#vtp mode client

3. Налаштувати транки.
4. Через деякий час після налаштування, перевірити стан VTP командою show vtp status. Переконатися, що прийнято доменне ім'я від сервера і змінився номер версії конфігурації.

Приклад:

```
Switch#sh vtp status
VTP Version                     2
Configuration Revision          4
Maximum VLANs supported locally 255
Number of existing VLANs        7
VTP Operating Mode              : Client
VTP Domain Name                 : class
VTP Pruning Mode                : Disabled
VTP V2 Mode                                 : Disabled
VTP Traps Generation            : Disabled
MD5 digest :                    0x5B 0xC0 0x3D 0x43 0xD7 0xFE 0x94 0xBE
Configuration last modified by 0.0.0.0 at 3 1-03 00:02:12
```

5. Налаштувати порти режиму доступу, вказавши в їх конфігурації номера віртуальних мереж, яким вони належать. Налаштовувати сам список VLAN немає необхідності, оскільки він має бути прийнятий він сервера.

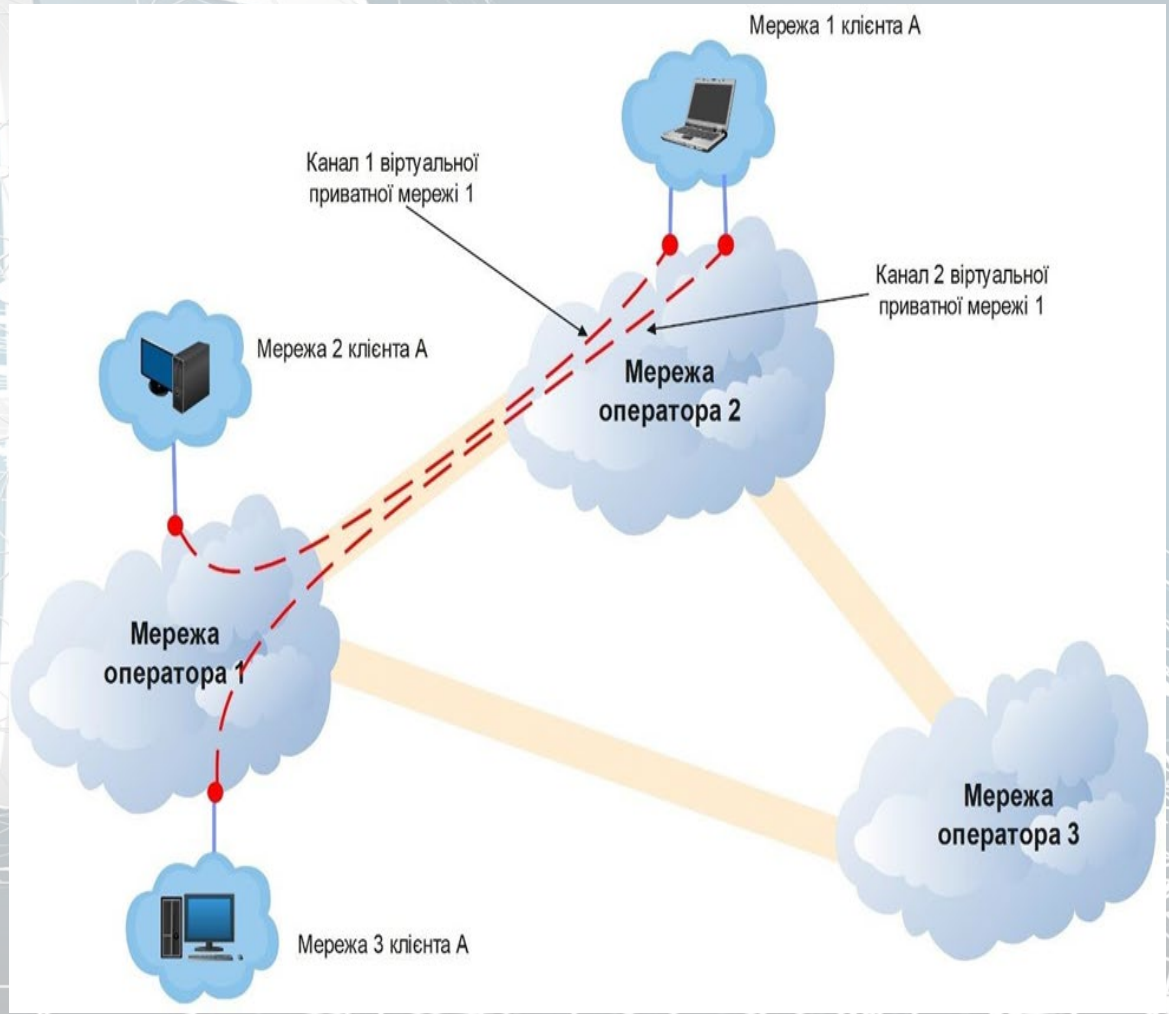
Пошук несправностей в роботі протоколу VTP

- У випадку з неспівпаданням версій протоколу VTP, комутатори не зможуть обмінюватися оголошеннями, оскільки версії 1 і 2 не сумісні. Усі комутатори в мережі повинні використати однакову версію протоколу.
- Комутатори також не зможуть обмінюватися оголошеннями у разі неспівпадання пароля VTP. По замовчуванню, комутатори не використовують пароль VTP і він не настроюється автоматично. Пароль, при необхідності, потрібно настроювати на кожному комутаторі локально.
- При помилці в імені домена комутатори не зможуть робити синхронізацію списку віртуальних мереж. Ім’я чутливе до регістру. Для того, щоб унеможливити виникнення такої помилки, призначають ім’я домена VTP тільки на одному сервері, інші клієнти і сервера повинні прийняти призначене ім’я через оголошення.
- Ще можлива ситуація – якщо усі комутатори налаштувати як клієнтів VTP, то інформація про існуючі віртуальні мережі може бути втрачена при перезавантаженні, оскільки вона зберігається в оперативній пам’яті. Для збереження інформації про віртуальні мережі потрібно хоча б один комутатор налаштувати як сервер.
- У разі, коли усі комутатори мережі налагоджені правильно, можна зіткнутися з ситуацією, яка може зіпсувати налаштування віртуальних мереж усього домена. Це ситуація з неправильними номерами версій конфігурації VTP.

Послуги віртуальних приватних мереж (1)

Найбільш цінними для власників приватних мереж є наступні їх властивості:

- Обмеження доступу до мережі на рівні транспорту: лише вузли мережі мають технічну можливість передавати свої пакети один одному. Для технології VPN забезпечити цю властивість дуже важко, оскільки пакети користувачів VPN проходять через ті ж комунікаційні пристрої і канали, що і пакети зовнішніх користувачів.
- Незалежна система адресації. У приватних мережах немає обмежень на вибір адрес – вони можуть бути будь-якими. Щоб зберегти цю властивість, мережа VPN повинна допускати адресацію вузлів з усього діапазону IP-адрес, включаючи приватні IP-адреси (рекомендовані лише для автономного використання).
- Передбачувана продуктивність. Власні лінії зв’язку гарантують заздалегідь відому пропускну спроможність між комунікаційними пристроями. Забезпечення передбачуваної пропускної спроможності в публічній мережі з комутацією пакетів може стати проблемою для сервісу VPN.
- Максимально можлива безпека. Відсутність зв’язків із зовнішнім світом захищає приватну мережу від атак ззовні і істотно знижує ймовірність «прослуховування» по трафіку шляху проходження пакетів. VPN обмежує доступ зовнішніх користувачів, тим самим виключає можливість атак ззовні, а для захисту від прослуховування застосовується шифрування.



Послуги віртуальних приватних мереж (2)

Залежно від того, адресна інформація якого рівня приймається до уваги при об’єднанні мереж клієнтів, розрізняються:

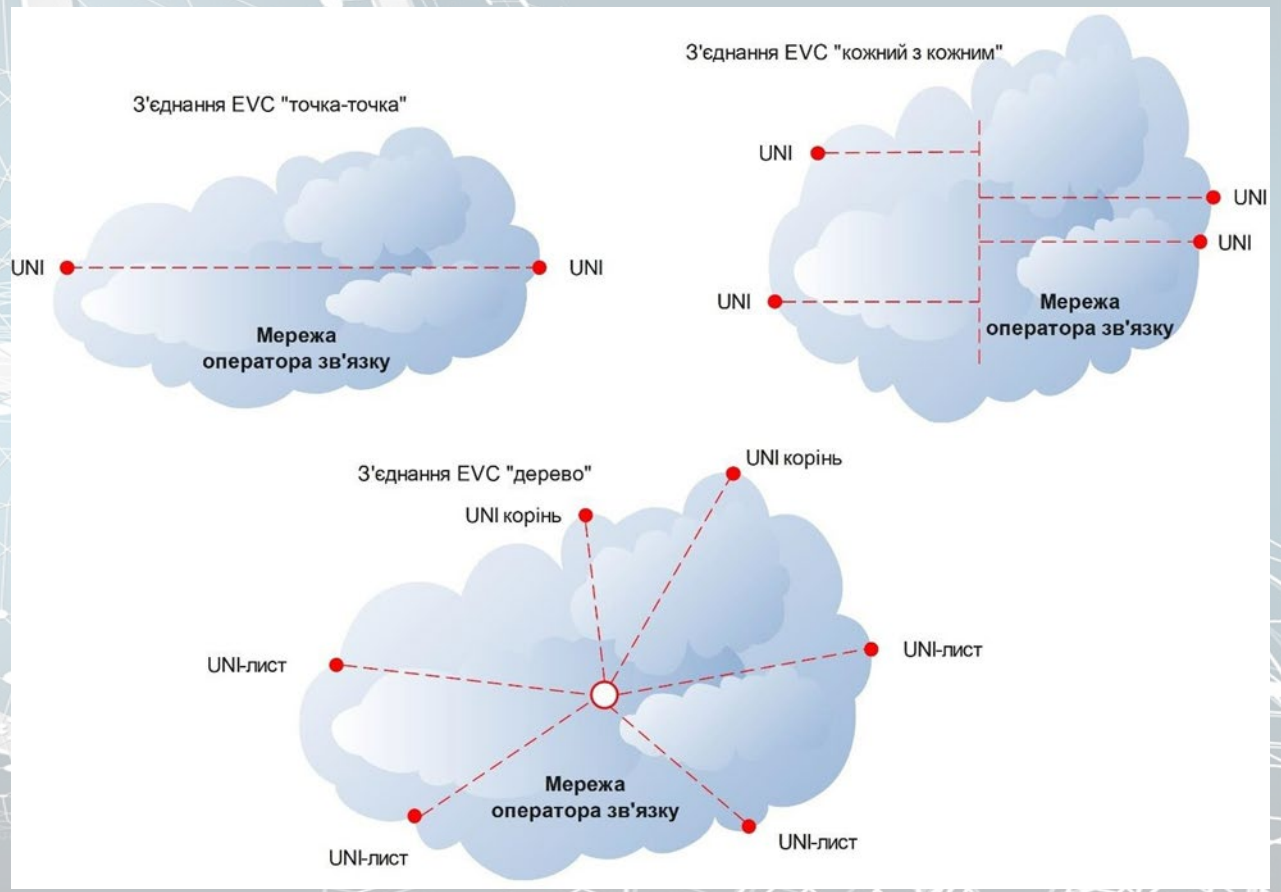
- VPN другого рівня: враховується адресна інформація другого (канального рівня) мереж клієнтів, тобто MAC-адреси і ідентифікатори VLAN;
- VPN третього рівня: враховуються IP-адреси мереж клієнтів.

Відповідно є три типи з’єднань EVC (рис):

- «точка-точка» (двоточкова топологія);
- «кожен з кожним» (повнозв’язна топологія);
- «дерево» (деревовидна топологія).

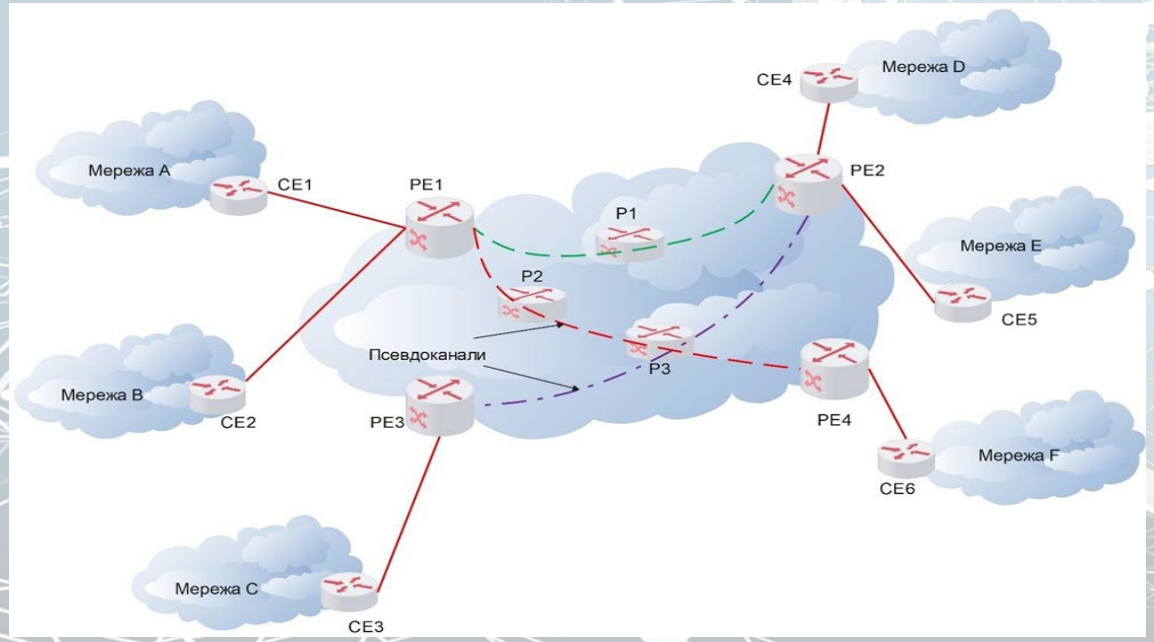
Залежно від типу використовуваного з’єднання розрізняються і типи послуг:

- E-LINE. Ця послуга з’єднує лише два користувацьких сайти через двоточкове EVC- з’єднання. Послуга E-LINE відповідає послузі виділеної лінії.
- E-LAN. Ця послуга аналогічна послузі локальної мережі, так як вона дозволяє з’єднати необмежене число користувацьких сайтів таким чином, що кожен сайт може взаємодіяти з кожним. При цьому дотримується логіка роботи локальної мережі Ethernet – кадри з невивченими і широкотрансляційними MAC-адресами передаються всім сайтам, а кадри з вивченими унікальними MAC-адресами – тільки тому сайту, в якому знаходиться кінцевий вузол з даною адресою.
- E-TREE. Специфікація цієї послуги з’явилася пізніше інших; в локальних мережах їй немає аналога. Користувацькі сайти діляться на кореневі і листові. Листові сайти можуть взаємодіяти тільки з кореневими, але не між собою. Кореневі сайти можуть взаємодіяти з листовими сайтами і один з одним.

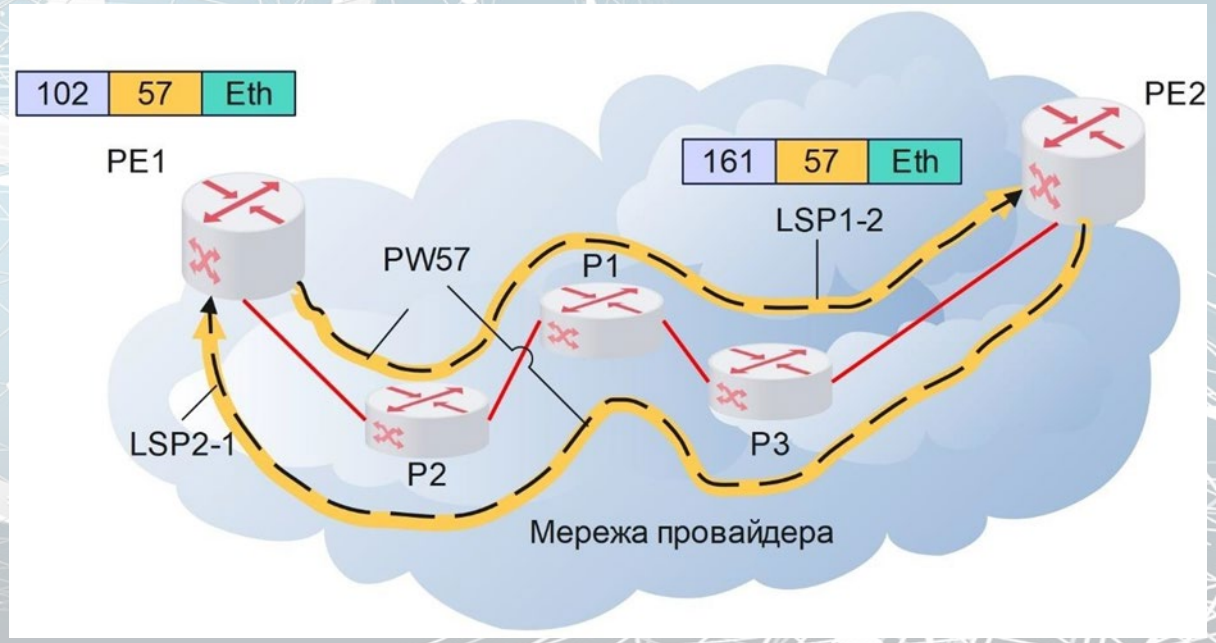


Технологія MPLS VPN рівня другого. Псевдоканали

- Для використання MPLS як внутрішньої технології провайдера при наданні послуг Ethernet VPN маршрутизатори MPLS повинні бути налаштовані спеціальним чином, а прикордонні маршрутизатори повинні, крім того, надавати користувачам інтерфейси Ethernet



Псевдоканали в мережі провайдера



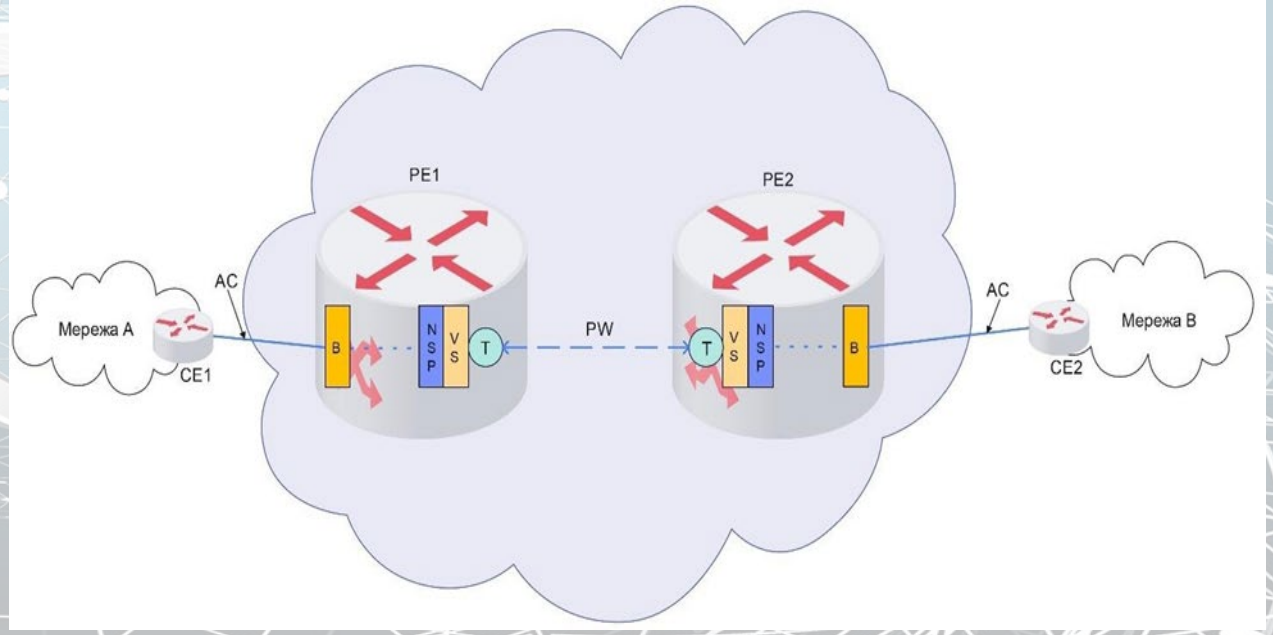
Створення псевдоканалу всередині тунелей MPLS

Технологія MPLS VPN рівня другого. Послуги VPWS

Послуги віртуальних приватних каналів (Virtual Private Wire Service, VPWS) виконують роль «глобального кабелю», прозоро поєднуючи дві локальні користувацькі мережі Ethernet через мережу оператора зв'язку. Розглянемо організацію такої послуги за допомогою псевдоканалів MPLS на прикладі (рис.).
На рисунку показані внутрішні функціональні елементи прикордонних маршрутизаторів PE1 і PE2, які емулюють послуги VPWS разом з псевдоканалом PW. Модуль B (Bridge – міст) працює
за стандартним алгоритмом IEEE 802.1D.

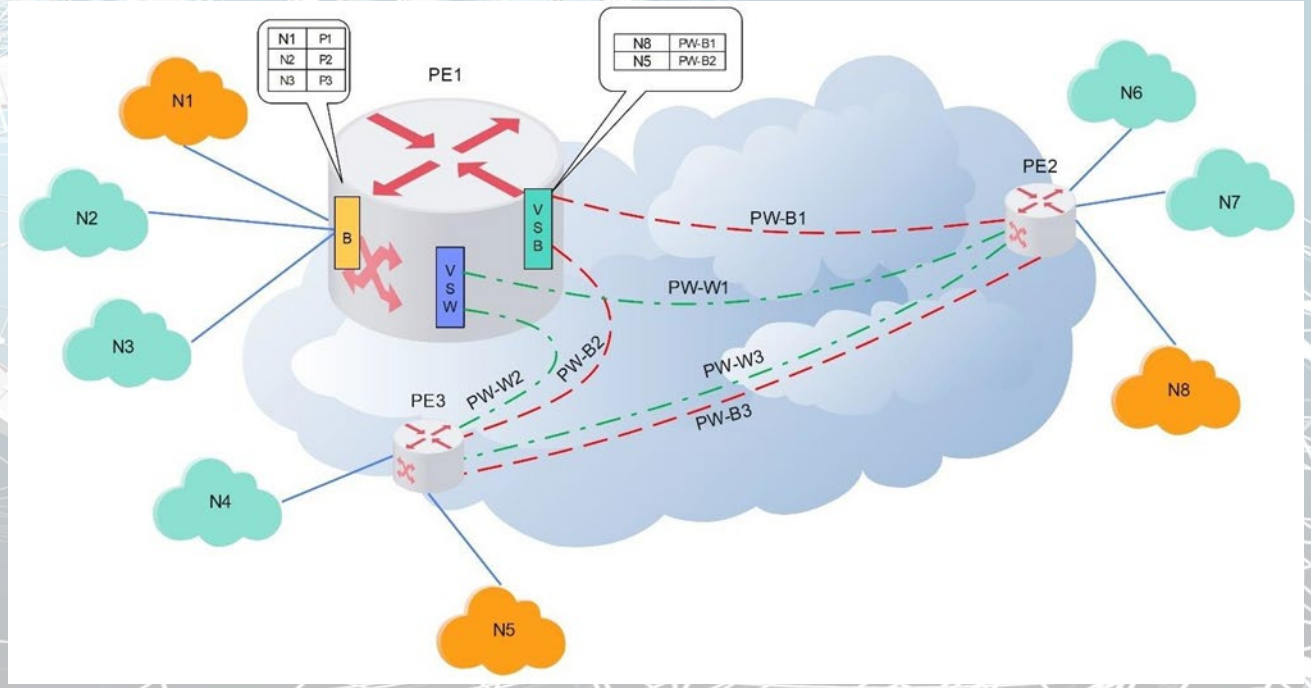
Після обробки вхідного кадру модулями NCP і VS він передається псевдоканалу. Кінцеві точки T псевдоканалу PW57 виконують дві операції:

- інкапсуляцію та деінкапсуляцію користувацьких кадрів в кадри MPLS;
- мультиплексування і демультиплексування псевдоканалів в тунелі MPLS.



Технологія MPLS VPN рівня другого. Послуги VPLS

- Послуги віртуальної приватної локальної мережі (Virtual LAN Service Private, VPLS) відповідають визначенню послуг E-LAN MEF, причому як варіанту з урахуванням ідентифікаторів VLAN користувачів EVPLAN, так і варіанту без їх урахування EPLAN.
- На рис. 3.6 показаний приклад мережі провайдера, що емулює два сервіси VPLS. Користувацькі мережі N1, N5 і N8 відносяться до VPLS сервісу «А», а мережі N2, N3, N4, N6 і N7 – до сервісу «В». Відповідно набір псевдоканалів PW- B1, PW-B2 і PW-B3 об’єднує прикордонні маршрутизатори, до яких під’єднані мережі сервісу «А» VPLS, а набір псевдоканалів PW-W1, PW-W2 і PW-W3 - маршрутизатори, до яких під’єднані мережі сервісу «В»VPLS (в прикладі це одні і ті ж прикордонні маршрутизатори PE1, PE2 і PE3, але якби мережі N4 не існувало, то псевдоканали PW-W2 і PW-W3 були б не потрібні).



Технологія MPLS VPN третього рівня

У цьому типі VPN користувацькі мережі (звані також сайтами) об’єднуються на основі адресної інформації третього рівня, тобто IP-адрес (а не MAC-адрес і ідентифікаторів VLAN, як в MPLS VPN другого рівня). При цьому IP-адреси можуть бути як публічними, так і приватними, в останньому випадку вони повинні бути унікальними в межах однієї віртуальної мережі.

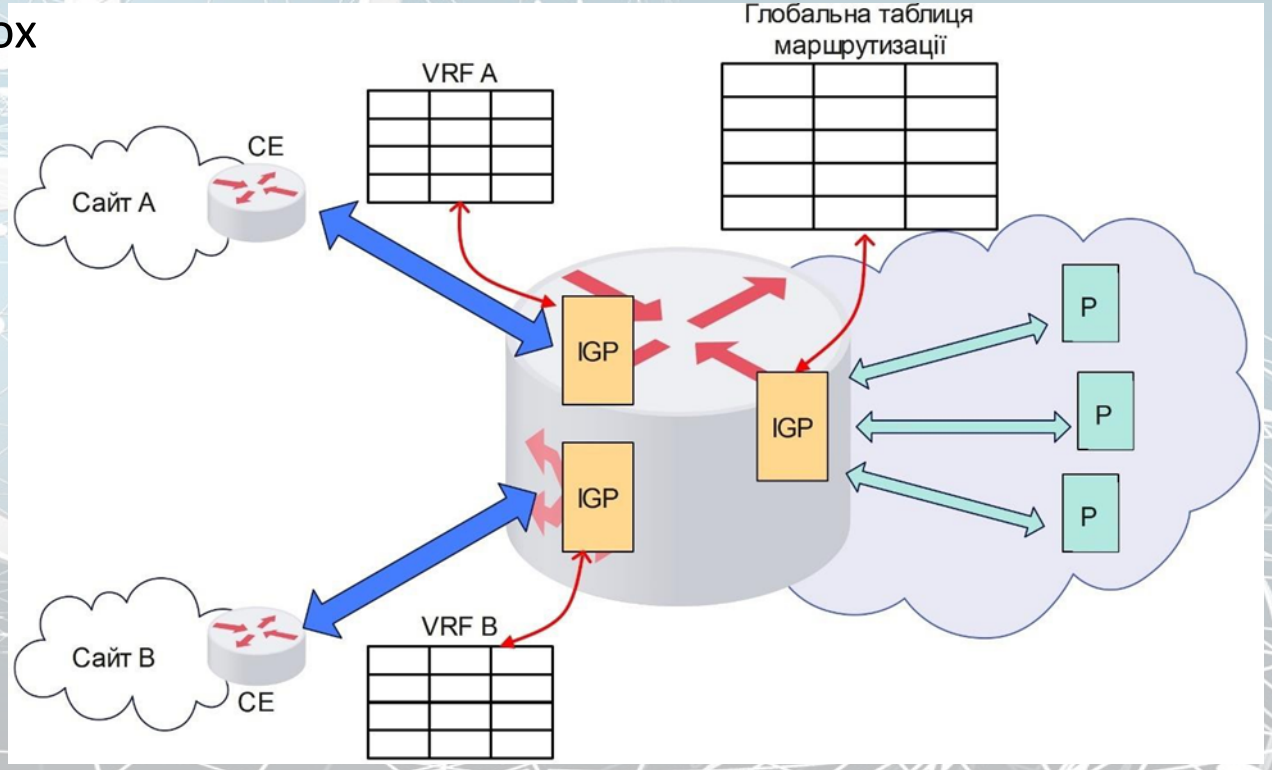
У той же час між MPLS VPN третього рівня і другого рівня є багато спільного:

- послуги надаються провайдером за допомогою мережі IP/MPLS;
- прикордонні маршрутизатори PE виконують всю роботу з підтримки VPN;
- внутрішні маршрутизатори провайдера P потрібні лише для передачі MPLS пакетів між прикордонними маршрутизаторами PE; вони не знають про існування VPN;
- для передачі інформації про належність пакета до певної мережі VPN використовується мітка MPLS другого рівня.

Технологія MPLS VPN третього рівня (1). Розмежування маршрутної інформації

Протоколи маршрутизації повинні бути сповіщені про те, з яких інтерфейсів і від кого вони мають право приймати оголошення і на які інтерфейси і кому їх поширювати.

На рис. показаний маршрутизатор PE, на якому встановлені кілька протоколів класу IGP. Один з них налаштований для прийому і поширення маршрутних оголошень лише з трьох внутрішніх інтерфейсів, які пов'язують цей маршрутизатор PE з маршрутизаторами P. Два інших протоколу IGP обробляють маршрутну інформацію від сайтів клієнтів.



Розмежування маршрутів різних клієнтів забезпечує установка на маршрутизаторах PE окремої копії протоколу маршрутизації на кожен інтерфейс, до якого під'єднаний сайт клієнта. Цей протокол приймає і передає клієнтські маршрутні оголошення тільки з одного визначеного для нього інтерфейсу, не пересилаючи їх ні на внутрішні інтерфейси, через які PE пов'язаний з маршрутизаторами P, ні на інтерфейси, до яких під'єднані сайти інших клієнтів.

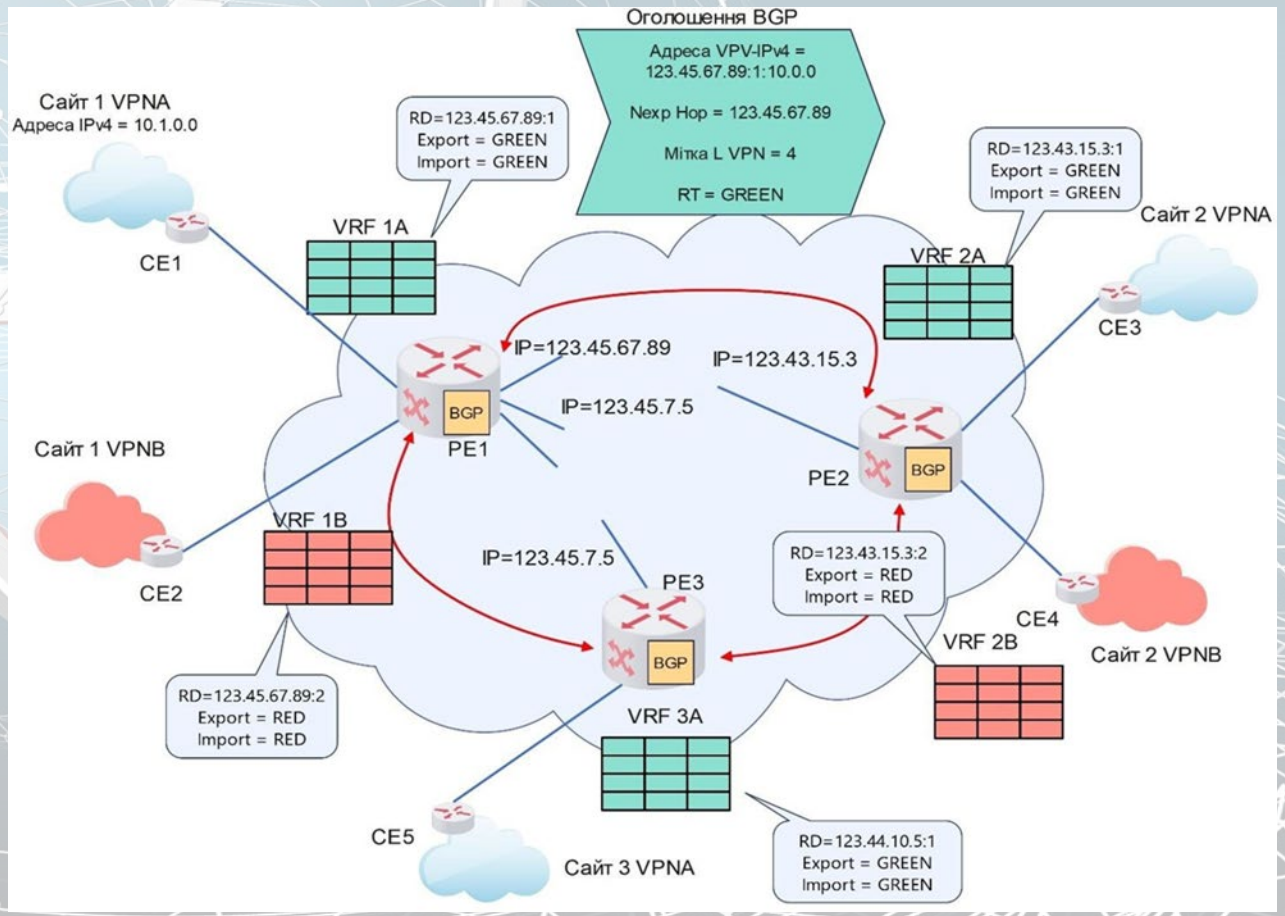
Технологія MPLS VPN третього рівня (2)

Обмін маршрутною інформацією

- Механізмом, за допомогою якого сайти однієї мережі VPN обмінюються маршрутною інформацією, є багатопротокольне розширення для BGP (Multiprotocol extensions for BGP, MP-BGP). За допомогою цього протоколу прикордонні маршрутизатори PE організовують взаємні сеанси і в рамках цих сеансів обмінюються маршрутною інформацією зі своїх таблиць VRF.

Незалежність адресних просторів сайтів

- Використання в різних мережах VPN одного і того ж адресного простору створює проблему для маршрутизаторів PE. Протокол BGP спочатку був розроблений в припущенні, що всі адреси , якими він маніпулює, по-перше, відносяться до сімейства адрес IPv4, по-друге, однозначно ідентифікують вузли мережі, тобто є глобально унікальними в межах всієї мережі.
- На рис. показано, як вхідний маршрутизатор PE1 додає розрізнювач маршрутів 123.45.67.89:1 (123.45.67.89 – це глобальна адреса інтерфейсу маршрутизатора PE, а 1 – призначений адміністратором номер) до всіх адрес з префіксом 10.1/16, які він отримує від маршрутизатора CE сайту 1 в VPN A, і пересилає ці на два маршрути на два інших вихідних маршрутизатора PE. Аналогічно, маршрутизатор PE1 додає розрізнювач маршрутів 123.45.67.89:2 до адрес з префіксом 10.1/16 в маршрутах, які він отримує від маршрутизатора CE сайту 1 в VPN B, і передає сформовані маршрути на інші два маршрутизатора PE.

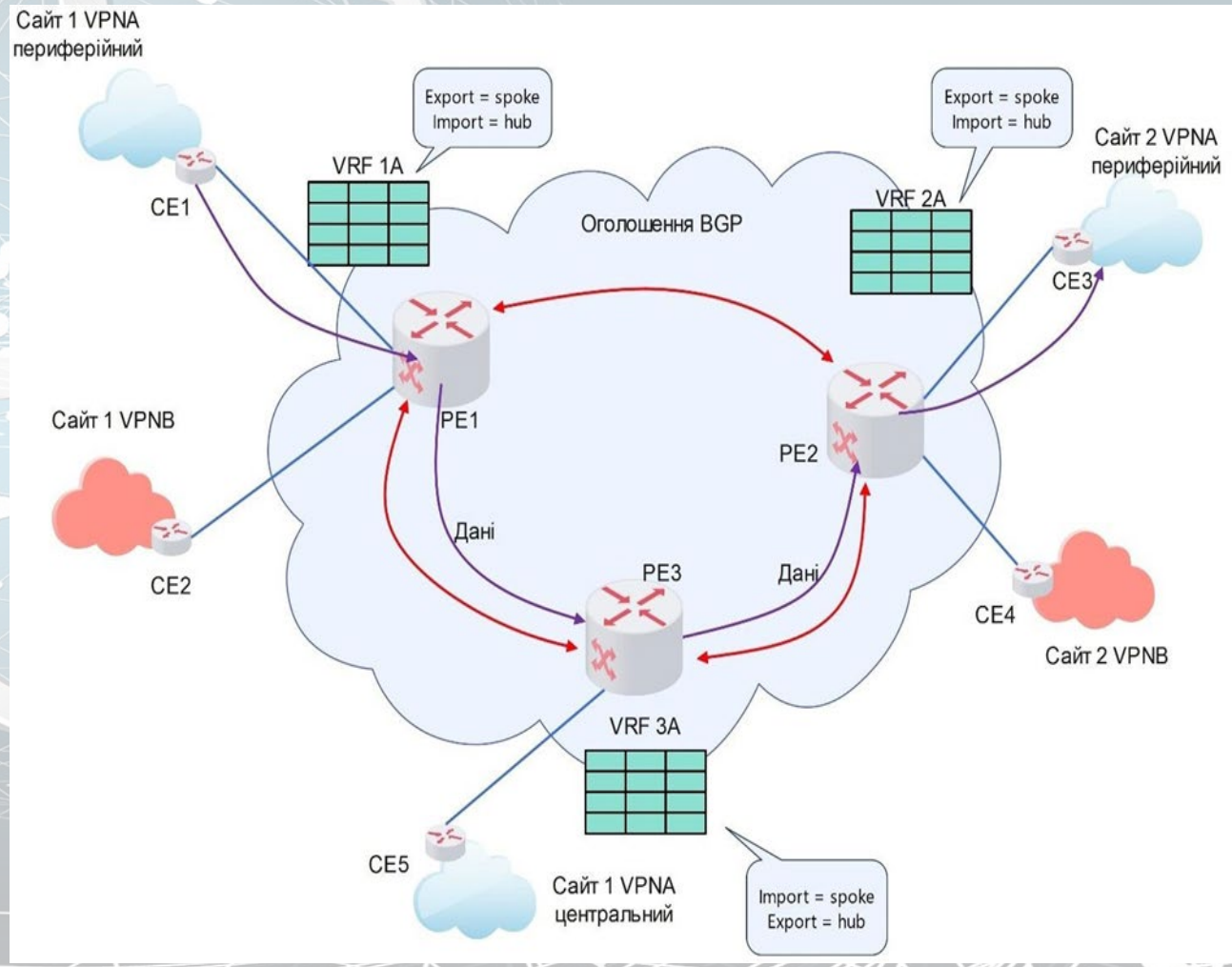


Конфігурування VPN топології

MPLS VPN третього рівня дозволяють створювати різні топології зв’язків між сайтами однієї і тієї ж мережі VPN. Цією властивістю мережі VPN даного типу відрізняються від мереж MPLS VPN другого рівня, в яких сайти однієї і тієї ж мережі VPN завжди досяжні один для одного.

При отриманні оголошень MP-BGP вступає в дію політика імпорту маршрутів; як і політика експорту, вона задається при конфігуруванні кожної таблиці VRE.

Задання одного і того ж значення для політики експорту та імпорту для всіх таблиць VRF певної мережі VPN призводить до повнозв’язної топології – кожен сайт пересилає пакети безпосередньо того сайту, в якому знаходиться мережа призначення. Саме цей випадок для VPN A і VPN B показаний на рис., так як таблиці VRF сайтів цих мереж VPN сконфігуровані з однаковими значеннями політики експорту та імпорту: значенням GREEN для VPN A і значенням RED для VPN B.



VPN на основі шифрування

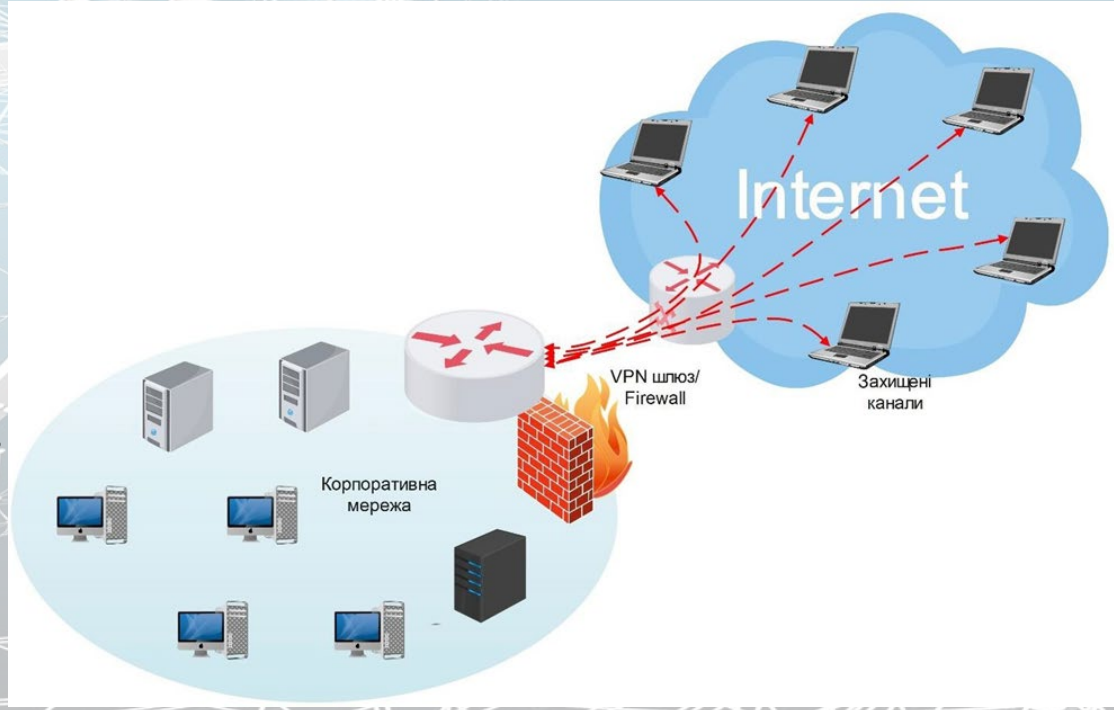
Залежно від використовуваних технологій безпеки даних мережі віртуальні приватні мережі діляться на два класи:

- мережі VPN на основі розмежування трафіку (розглядали в попередніх розділах);
- мережі VPN на основі шифрування (працюють на основі техніки захищених каналів).

Технології VPN на основі шифрування включають шифрування, автентифікацію і тунелювання.

- Шифрування гарантує конфіденційність корпоративних даних при передачі через відкриту мережу.
- Автентифікація відповідає за те, щоб взаємодіючі системи (користувачі) на обох кінцях VPN були впевнені в ідентичності один одного.
- Тунелювання надає можливість передавати зашифровані пакети по відкритій публічній мережі.

На рис. показаний приклад організації віртуальної приватної мережі на основі шифрування, що використовується працівниками підприємства, які працюють віддалено




БЕЗПЕКА
КОРПОРАТИВНИХ
МЕРЕЖ

Тенденції розвитку безпекових мережевих технологій

Мета заходів в сфері інформаційної безпеки – захистити інтереси суб’єктів інформаційних стосунків. Інтереси ці різноманітні, але усі вони концентруються навколо трьох основних аспектів:

– доступність;
– цілісність;
– конфіденційність.

Перший крок при побудові системи ІБ організації – ранжирування і деталізація цих аспектів.

Важливість проблематики ІБ пояснюється двома головними причинами:

– цінністю накопичених інформаційних ресурсів;
– критичною залежністю від інформаційних технологій.

Успіх в області інформаційної безпеки може принести тільки комплексний підхід, що поєднує заходи чотирьох рівнів:

– законодавчого;
– адміністративного;
– процедурного;
– програмно-технічного.

Законодавчий, адміністративний і процедурний рівні

Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Необхідно всіляко підкреслювати важливість проблеми ІБ; сконцентрувати ресурси на найважливіших напрямах досліджень; зорієнтувати освітню діяльність; створити і підтримувати негативне відношення до порушників ІБ – усе це функції законодавчого рівня

Головне завдання заходів адміністративного рівня – сформувати програму робіт в області інформаційної безпеки і забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ.

Заходи процедурного рівня орієнтовані на людей (а не на технічні засоби) і підрозділяються на наступні види:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновних робіт.

На цьому рівні застосовні важливі принципи безпеки:

- – безперервність захисту у просторі та часі;
- – розділення обов’язків;
- – мінімізація привілеїв.

Програмно-технічні заходи

Програмно-технічні заходи, тобто заходи, спрямовані на контроль комп'ютерних сутностей: устаткування, програм і/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки.

Тенденції побудови архітектури безпеки інформації

- превентивні, перешкоджаючі порушенням ІБ;
- заходи виявлення порушень;
- локалізуючі, звужуючі зону дії порушень;
- заходи по виявленню порушника;
- заходи відновлення режиму безпеки.

Виділимо найважливіші моменти для кожного з перерахованих сервісів безпеки:

- Переважними є криптографічні методи автентифікації, що реалізовуються програмним або апаратно-програмним способом.
- В умовах, коли поняття довіреного програмного забезпечення відходить в минуле, стає анахронізмом і найпоширеніша – довільна (дискреційна) – модель управління доступом. У її термінах неможливо навіть пояснити, що таке «троянська» програма.

Засади організації захисту інформації в корпоративних мережах. Політика безпеки

З точки зору безпеки істотними видаються наступні аспекти ІС:

- корпоративна мережа має декілька територіально рознесених частин, зв’язки між якими знаходяться у веденні зовнішнього постачальника мережевих послуг, виходячи за межі зони, контрольованої організацією;
- корпоративна мережа має одне або декілька підключень до інтернету;
- на кожній з рознесених частин ІВС можуть знаходитися критично важливі сервери, в доступі до яких мають потребу співробітники, працюючі на віддалених робочих місцях, мобільні користувачі і, можливо, співробітники інших організацій;
- для доступу користувачів можуть застосовуватися не лише комп’ютери, але і споживчі пристрої, що використовують, безпровідний зв’язок;
- впродовж одного сеансу роботи користувачеві доводиться звертатися до декількох інформаційних сервісів, що спираються на різні апаратно-програмні платформи;
- до доступності інформаційних сервісів висуваються жорсткі вимоги, які виражаються в необхідності цілодобового функціонування з максимальним часом простою близько декількох хвилин;
- інформаційна система є мережею з активними агентами, тобто в процесі роботи програмні компоненти, такі як аплети або сервлети, передаються з однієї машини на іншу і виконуються в цільовому середовищі, підтримуючи зв’язок з віддаленими компонентами;
- не усі призначені для користувача системи контролюються мережевими і/або системними адміністраторами організації;
- програмне забезпечення, особливо отримане по мережі, не може вважатися надійним, в нім можуть бути помилки, що створюють проблеми в захисті.

Засади організації захисту інформації в корпоративних мережах. Архітектурна безпека

З практичної точки зору найбільш важливими є наступні принципи архітектурної безпеки:

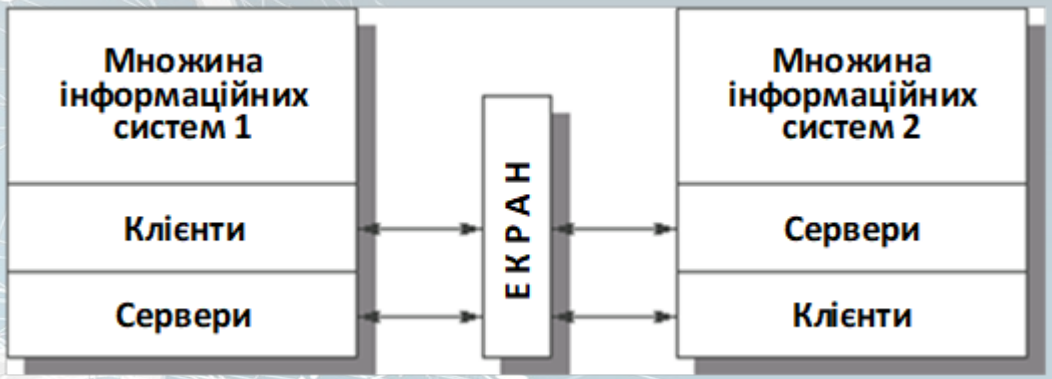
- безперервність захисту у просторі та часі, неможливість минути захисні засоби;
- наслідування визнаних стандартів, використання апробованих рішень;
- ієрархічна організація з невеликим числом сутностей на кожному рівні;
- посилення найслабкішої ланки;
- неможливість переходу в небезпечний стан;
- мінімізація привілеїв;
- розділення обов’язків;
- ешелонованість оборони;
- різноманітність захисних засобів;
- простота і керованість інформаційної системи.

Для забезпечення високої доступності необхідно дотримуватися наступних принципів архітектурної безпеки:

- внесення в конфігурацію тієї або іншої форми надмірності (резервне устаткування, запасні канали зв’язку і тому подібне);
- наявність засобів виявлення нештатних ситуацій;
- наявність засобів реконфігурування для відновлення, ізоляції і заміни компонентів, що відмовили або піддалися атаці на доступність;
- розосередженість мережевого управління;
- відсутність єдиної точки відмови;
- виділення підмереж і ізоляція груп користувачів один від одного.

Засади організації захисту інформації в корпоративних мережах. Екранування

Формальна постановка завдання екранування полягає в наступному. Нехай є дві множини ІС. Екран – цей засіб розмежування доступу клієнтів з однієї множини до серверів з іншої множини. Екран здійснює свої функції, контролюючи усі інформаційні потоки між двома або безліччю систем (рис. зверху)



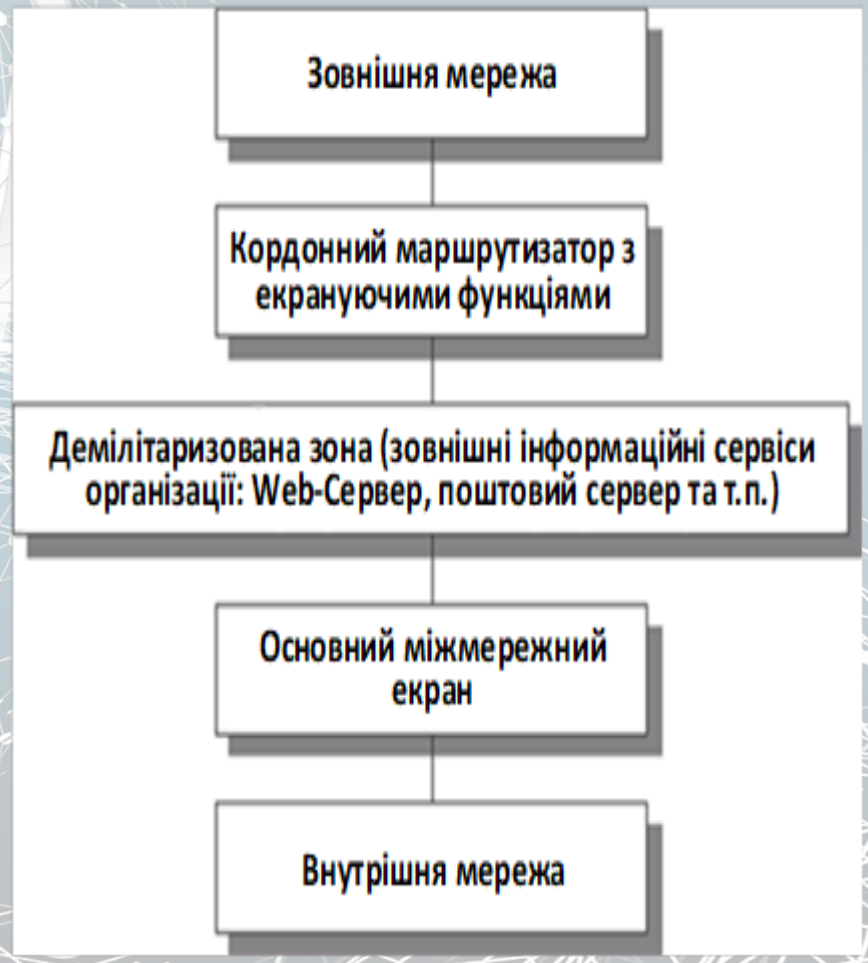
На наступному рівні деталізації екран зручно представляти як послідовність фільтрів. Кожен з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може і відразу «перекинути» за екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата і повернення результату (рис.знизу)



Засади організації захисту інформації в корпоративних мережах. Багаторівневий захист корпоративних мереж

Міжмережевий екран розташовується між мережею, що захищається (внутрішньою), і зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішній МЕ, в другому – про внутрішній. Залежно від точки зору, зовнішній міжмережевий екран можна вважати першою або останньою (але не єдиною) лінією оборони. Першою – якщо дивитися на світ очима зовнішнього зловмисника. Останньою – якщо прагнути до захищеності усіх компонентів корпоративної мережі і припинення неправомірних дій внутрішніх користувачів.

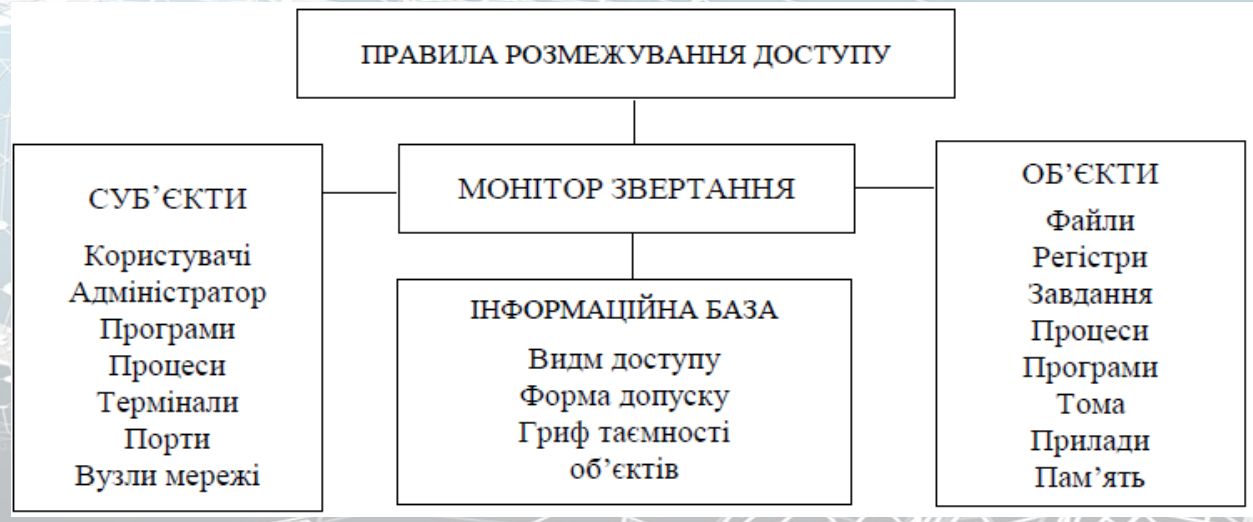
В силу принципів ешелонованості оборони для захисту зовнішніх підключень зазвичай використовується двокомпонентне екранування (рис.). Первинна фільтрація (наприклад, блокування пакетів протоколу SNMP, що керує, або пакетів з певними IP-адресами, внесеними в «чорний список») здійснюється граничним маршрутизатором, за яким розташовується так звана демілітаризована зона (мережа з помірною довірою безпеки – веб, електронна пошта і тому подібне) і основний МЕ, що захищає внутрішню частину корпоративної мережі.



Принципи надання доступу до IP в корпоративних мережах

- Принцип обґрунтованості доступу.
- Принцип достатньої глибини контролю доступу.
- Принцип розмежування потоків інформації.
- Принцип чистоти повторно використовуваних ресурсів.
- Принцип персональної відповідальності.
- Принцип цілісності засобів захисту.

Реалізація перерахованих принципів здійснюється за допомогою так званого «монітора звернень», контролюючого будь-які запити до даних або програм з боку користувачів (чи їх програм) по встановлених для них видах доступу до цих даних і програм. Такий монітор представляється у вигляді схеми (рис.)



Методи ідентифікації і автентифікації користувачів та контролю доступу

Перевірка достовірності (автентифікація) може проводитися різними методами і засобами. Нині в автоматизованих системах використовуються три основні способи автентифікації за:

- паролем або особистим ідентифікуючим номером (користувач «знає»);
- деяким предметом, який є у користувача (користувач «має»);
- якими-небудь фізіологічними ознаками, властивими конкретним особам (користувач «є»).

Схеми розмежування доступу зручно розділити на дві групи:

- «списковi» схеми, в яких захисні механізми вбудовуються в кожен об’єкт і здійснюють контроль відповідно до списків доступу цього об’єкту;
- «мандатні» схеми, в яких захисний механізм об’єкту реагує на деякий мандат, і суб’єкт повинен мати набір мандатів для доступу до усіх необхідних йому об’єктів.

Застосування систем виявлення вторгнень до корпоративних мереж

Існують два основні типи IDS: вузлові (HIDS) і мережеві (NIDS). Система HIDS розташовується на окремому вузлі і відстежує ознаки атак на цей вузол. Система NIDS знаходиться на окремій системі, що відстежує мережевий трафік на наявність ознак атак, що проводяться в підконтрольному сегменті мережі. На рис. показані два типи IDS, які можуть бути присутніми в мережевому середовищі



Вірогідне виникнення розбіжностей, пов’язаних з управлінням і налаштуванням, між адміністраторами безпеки (керівниками роботою IDS) і системними адміністраторами. Оскільки процес повинен постійно знаходитися в активному стані, потрібна хороша координація в їх роботі.

Існує п’ять основних типів датчиків HIDS:

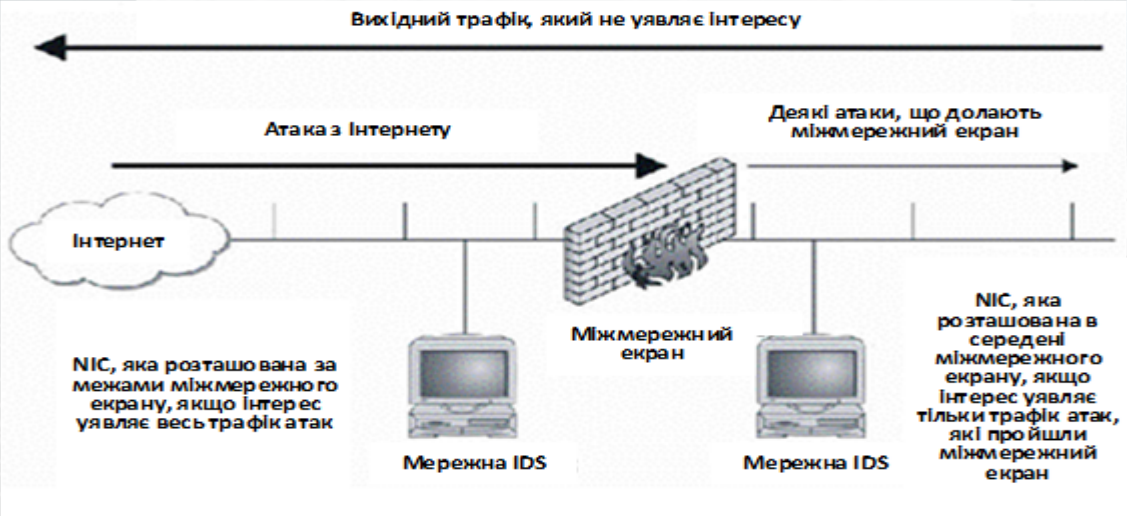
- аналізатори журналів;
- датчики ознак;
- аналізатори системних викликів;
- аналізатори поведінки додатків;
- контролери цілісності файлів.



Класифікація політик виявлення вторгнень (1)

При створенні політики IDS необхідно виконати наступні кроки:

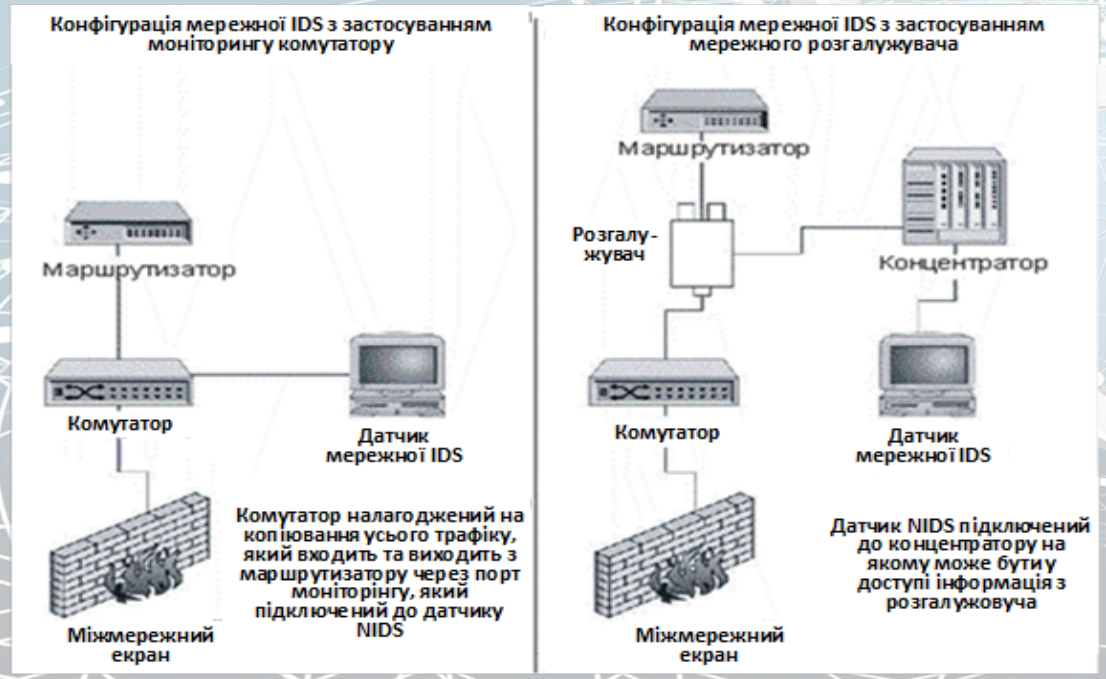
1. Визначити цілі створення IDS.
   - виявлення атак;
   - запобігання атакам;
   - виявлення порушень політики;
   - примус до використання політик;
   - примус до наслідування політиків з'єднань;
   - збір доказів.
2. Вибрати об'єкти моніторингу.



Політика	NIDS	HIDS
Виявлення атак	Увесь трафік, що поступає на системи (мережеві екрани, веб-сервери, сервери додатків і так далі), що потенційно атауються	Невдалі спроби входу. Спроби з'єднання. Вдалий вхід з видалених систем.
Запобігання атакам	Те ж, що і для виявлення атак	Те ж, що і для виявлення атак.
Виявлення порушень політики	Увесь трафік HTTP, що формується на системах клієнтах. Увесь трафік FTP, що формується на системах клієнтах	Успішні HTTP-з'єднання. Успішні FTP-з'єднання. Завантажувані файли.
Примус до використання політик	Те саме, що і для виявлення порушень політики	Те ж, що і для виявлення порушення політики.
Примус до відповідності політикам з'єднань	Увесь трафік, що порушує примусово використовувану політику з'єднання	Успішні з'єднання із заборонених адрес або по заборонених портах.
Збір доказів	Вміст усього трафіку, що формується на системі-меті або атакуючій системі	Усі успішні підключення, витікаючі з атакуючої системи. Усі невдалі з'єднання з атакуючих систем. Усі натиснення клавіш з інтерактивних сеансів на атакуючих системах.

Класифікація політик виявлення вторгнень (1)

3. Вибрати дії у відповідь.
   - Активна обробка подій
   - Автоматична і автоматизована відповідь
4. Встановити пороги.
5. Застосувати політику.



Політика	Пасивні дії у відповідь	Активні дії у відповідь
Виявлення атак	Ведення журналів Ведення додаткових журналів Повідомлення	Немає активної дії у відповідь.
Запобігання атакам	Ведення журналів Повідомлення	Закриття з'єднання. Завершення процесу. Переналаштування міжмережевого екрану.
Виявлення порушень політики	Ведення журналів Повідомлення	Немає активної дії у відповідь.
Примусове використання політик	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштування проксі.
Примусове використання політик з'єднання	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштування маршрутизатора або міжмережевого екрану.
Збір доказів	Ведення журналів Ведення додаткових журналів Повідомлення	Обманні дії. Можливе закриття з'єднання.

Практика застосування політики IDS

Політика може бути перевірена на практиці без ушкодження легітимного трафіку або переривання легального доступу користувачів до комп'ютерів, для цього розглядається:

- Конфігурація системи виявлення вторгнень
  - Події дослідження.
  - Атаки.
  - Порушення політики.
  - Підозрілі або нез'ясовні події.
- Дослідження підозрілих подій та запобігання вторгненням
  - Ідентифікувати системи.
  - Записувати в журнал відомості про додатковий трафік між джерелом і пунктом призначення.
  - Записувати в журнал увесь трафік, що виходить з джерела.
  - Записувати в журнал вміст пакетів з джерела.

Ім'я події	Дія	IP-адреса джерела	IP-адреса пункту призначення	Протокол	Порт джерела	Кінцевий порт
SUS_ACT	Повідомлення, занесення в журнал	Джерело підозрілої активності	Пункт призначення підозрілої активності	TCP, UDP і/або ICMP, залежно від типу виявленої активності	Будь-хто	Будь-хто

Ім'я події	Дія	IP-адреса джерела	IP-адреса пункту призначення	Протокол	Порт джерела	Кінцевий порт
SUS_ACT	Повідомлення, запис в журнал утримуваного пакету	Джерело п дозрілої активності	Пункт призначення підозрілої активності	TCP або UDP	Будь-хто	Порт, на який спрямован ий підозрілий трафік
SUS_ACT	Повідомлення, запис в журнал утримуваного пакету	Пункт призначення під зрілої активності	Джерело підозр лої активності	TCP або UDP	Порт, на який спрямований підозрілий трафік	Будь-хто

Практика застосування політики IDS. Запобігання вторгненням

Процес запобігання атаці за допомогою NIDS є складним. У стандартній конфігурації NIDS датчик розташовується в тому місці, з якого він може відстежувати трафік (рис.). При вступі через канал зв'язку даних атаки датчик перехоплює пакет і починає його аналізувати. У деякий момент датчик визначає, що пакет є атакою, і робить дію. Ця дія, як правило, полягає в закритті з'єднання (тільки якщо атака проводиться через з'єднання TCP) або в переналаштуванні міжмережевого екрану для блокування подальшого трафіку з джерела. На жаль, у випадку з NIDS час працює не на користь досягнення мети. Під час аналізу пакету датчиком пакет продовжує свій рух по мережі. У більшості випадків пакет досягає мети ще перед закриттям з'єднання або виконанням дій з переналаштування міжмережевого екрану. Найчастіше атака випереджає дії датчика з її запобігання.

Розглянута архітектура не є єдино можливою. Також можливо розташувати датчик NIDS на міжмережевому екрані або реалізувати його тісний взаємозв'язок з міжмережевим екраном, щоб останній не пропускав трафік без дозволу датчика NIDS.



Методи і засоби аналізу безпеки програмного забезпечення

Широко відомі різні засоби програмного забезпечення виявлення елементів – від простих антивірусних програм-сканерів до складних відладчиків і дизасемблерів – аналізаторів і саме на базі цих засобів і виробився набір методів, якими здійснюється аналіз безпеки ПЗ.

Комплексна система дослідження безпеки ПЗ повинна включати:

- Контрольно-випробні методи – це методи, в яких критерієм безпеки програми служить факт реєстрації в ході тестування програми порушення вимог по безпеці, що пред'являються в системі передбачуваного застосування досліджуваної програми. Тестування може проводитися за допомогою тестових запусків, виконання у віртуальному програмному середовищі, за допомогою символічного виконання програми, її інтерпретації і іншими методами.
- При проведенні аналізу безпеки за допомогою логіко-аналітичних методів будується модель програми і формально доводиться еквівалентність моделі досліджуваної програми і моделі РПЗ. У простому випадку моделлю програми може виступати її бітовий образ, в якості моделей вірусів безліч їх сигнатур, а доказ еквівалентності полягає в пошуку сигнатур вірусів в програмі. Складніші методи використовують формальні моделі, засновані на сукупності ознак, властивих тій або іншій групі РПЗ.

Запитання для самоконтролю

1. Методи і засоби аналізу безпеки програмного забезпечення.
2. Контрольно-випробні методи аналізу безпеки програмного забезпечення.
3. Логіко-аналітичні методи контролю безпеки програм.
4. Інформаційні технології та принципи організації інформаційної безпеки.
5. Види та властивості інформації як предмета захисту.
6. Інформаційні технології та проблеми їхньої безпеки.
7. Принципи організації інформаційної безпеки.
8. Моделі управління мережевими ресурсами.
9. Програмні та апаратні засоби захисту в інформаційних системах.
10. Технології захисту інформації при міжмережевій взаємодії.
11. Захист повідомлень при передачі каналами та лініями зв’язку.
12. Принципи побудови мережевих екранів.
13. Технології захисту у мережах на основі протоколів TCP/IP.
14. Реалізація загроз інформації у мережах на основі протоколів TCP/IP.
15. Принципи побудови мереж VPN.
16. Виявлення мережевих атак шляхом аналізу трафіка.
17. Основи захвату та аналізу мережевого трафіка.
18. Виявлення мережевих атак шляхом аналізу трафіка.
19. Надійність та стійкість програмного забезпечення.
20. Методи забезпечення стійкості програмного забезпечення.

Забезпечення безпеки корпоративної мережі за OSI моделлю на фізичному рівні (1)

Прикладом протоколу фізичного рівня може служити специфікація 10BaseT технології Ethernet, яка визначає як кабель, що використовується неекрановану пару категорії з хвильовим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів, манчестерський код для представлення даних в кабелі, а також деякі інші характеристики середи і електричних сигналів.

Найбільш поширених специфікацій фізичного рівня належать:

- EIA-RS-232-C, CCITT V.24/V.28 – механічні/електричні характеристики незбалансованого послідовного інтерфейсу;
- EIA-RS-422/449, CCITT V.10 – механічні, електричні і оптичні характеристики збалансованого послідовного інтерфейсу;
- IEEE 802.3 – Ethernet;
- IEEE 802.5 – Token ring.

Стандарти для фізичного рівня пишуть ті ж організації, що й для канального – ITU, IEEE, ISO, ANSI, EIA/TIA, FCC. Вони реалізуються в мережних адаптерах пристроїв. Технології певні цими організаціями включають 4 області стандартів фізичного рівня:

- фізичні й електричні властивості середовища;
- механічні властивості конекторів;
- вистава бітів у вигляді сигналів;
- визначення службових сигналів. Три основні функції фізичного рівня:
- фізичні компоненти;
- кодування (encding) даних – приведення бітів кадра до визначеного виду;
- сигналізація (signaling) у середовище за допомогою сигналів;
- час біта (bit time) – час приміщення біта в середовище передачі.

Забезпечення безпеки корпоративної мережі за OSI моделлю на фізичному рівні (2)

Для побудови мереж застосовують різні види середовищ передачі даних.

- Мідний кабель чутливий до електромагнітної інтерференції. Для захисту від неї використовують екрановані типи мідного кабелю.
- Неекранована вита пари (unshielded twisted-pair) представляє із себе 4х або 2х парний кабель. Пари перекручуються між собою для зменшення перешкод (crosstalk), що наводяться провідниками один на одного. Усі пари маркуються по кольорах, щоб точно визначити обрану пару на різних кінцях кабелю. У якості конектора застосовується RJ-45. Стандарти розподілу пінів по кольорах у конекторі 586A (застарілий) і 586B.
- Прямий кабель (straight-through) – обоє кінці кабелю обжимаються одним стандартом. Застосовується для з’єднання різних пристроїв (ПК – комутатор, роутер – комутатор).
- Скретний кабель (crossover) – кінці кабелю обжимаються за різними стандартами. Застосовується для з’єднання однакових пристроїв (комутатор – комутатор, роутер – роутер, ПК – ПК).
- Перевернений кабель (rollover) – RJ45 на COM/USB, використовується для підключення до консольних портів мережного встаткування Cisco.
- Коаксіальний кабель – складається із двох провідників, центральна жила й обплетення. Раніше застосовувався для побудови локальних мереж, сьогодні застосовується в мережах кабельного телебачення.
- Екранована вита пара (shielded twisted-pair cable) – пари екрануються окремо й усі разом. Раніше застосовувався для мереж Token Ring, зараз застосовується для мереж 10G Ethernet.

Можна виділити два основні середовища передачі даних:

- проводове (за участю кабелів);
- безпроводове (без участі кабелів).

Забезпечення безпеки корпоративної мережі за OSI моделлю на фізичному рівні (3)

Забезпечення безпеки на фізичному рівні полягає у забезпеченні структурної цілісності мережі. Структурна цілісність мережі – здатність зберігати неподільність системи. Основними загрозами структурної цілісності мережі є:

- проникнення в систему (отримання несанкціонованого доступу до ресурсів мережі);
- фізичне пошкодження мережі;
- створення завад у безпроводових каналах передачі даних.

Для реалізація цих загроз необхідно володіти апріорними знаннями про будову мережі. Проникнення у систему здійснюється з метою вводу хибної інформації, модифікації інформації, що передається в мережі, несанкціонованого користування ресурсами мережі (частотним, часовим, апаратним). Для проникнення в мережі необхідно, щоб порушник:

- мав устаткування сумісне з устаткуванням мережі;
- був здатний розпізнавати структуру і параметри сигналу;
- знав параметри мережі (ідентифікатор мережі, що закриває інфраструктуру мережі; був занесеним в таблицю дозволених адрес в точці доступу, і т. ін.);
- мав ключ шифру (у разі шифрування інформації в мережі) тощо.

Адміністративними (організаційними) методами з джерелами завад бореться служба радіоконтролю частотних ресурсів, яка повинна розробляти заходи по припиненню випромінювань джерел завад, що заважають зареєстрованим радіозасобам. Згідно рекомендаціям МСЕ такими заходами можуть бути:

- зміна частоти;
- використання направлених антен;
- коректування розкладів або експлуатаційні угоди (розділення за часом);
- зміна класу випромінювання;
- переміщення окремих каналів в багатоканальній системі передачі;
- перенесення навантаження на інші наявні частоти;
- припинення роботи однієї із станцій, що є джерелом завад для інших.

Забезпечення безпеки корпоративної мережі за OSI моделлю на канальному рівні (1)

Канальний рівень розділяється на два підрівня:
- LLC – фреймуючий пакет і визначальний протокол мережного рівня. (реалізується в драйверах);
- MAC – додає адреси канального рівня й маркірує початок і кінець кадру. (реалізується в мережному адаптері).

Протоколи й стандарти канального рівня пишуться такими організаціями як ISO, IEEE, ITU, ANSI.
Контроль доступу до середовища регулює переміщення кадрів у середовище передачі даних.
Контрольований (controlled) – кожному вузлу виділяється час на передачу даних – Token Ring, FDDI. При цьому:
- тільки одна станція одноразово може передавати дані;
- кожна станція чекає своєї черги;
- немає колізій;
- дані передає тільки станція, що одержала маркер.

Асоціативний (contention-based) – будь-який вузол може передати дані в будь-який момент (Ethernet, Wireless)
- станції можуть передавати в будь-який момент;
- присутні колізії;
- механізми боротьби з колізіями CSMA/CD Ethernet, CSMA/CA Wi-Fi.

Типи передачі даних:
- half duplex – поки одна станція передає, інші чекають своєї черги;
- full duplex – станція може одночасно передавати і ухвалювати дані.

Типи топології:
- логічна – описує як дані передаються по мережі;
- фізична – описує як вузли з’єднані між собою.

Логічна й фізична топології мережі можуть не збігатися.
Точка-точка (Point-to-Point) – тільки два вузли з’єднано один з одним фізично або логічно.
Множинний доступ (multi access) – більш 3 пристроїв з’єднаних загальним середовищем передачі даних.
Кільце (ring) – пристрої з’єднані в кільце або зірку, дані передаються від одного до іншого у вигляді кільця.

Забезпечення безпеки корпоративної мережі за OSI моделлю на канальному рівні (2)

Одним із завдань канального рівня є перевірка доступності середовища передачі. Інше завдання канального рівня – реалізація механізмів виявлення та корекції помилок. Для цього на канальному рівні біти групуються в набори, звані кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру.

Основні поля заголовка кадру для будь-якого протоколу:

- початок кадру;
- адреси;
- довжина кадру або тип протоколу 3 рівня.

Типи атак на канальному рівні локальних обчислювальних мереж

- Пасивні:
  - підслуховування (sniffing) і аналіз мережного трафіку, використовують недоліки в протоколах і мережному устаткуванні. За допомогою сніфера можна отримати корисну, а інколи і конфіденційну інформацію (наприклад, імена користувачів і паролі);
  - підміна довіреного суб'єкта. Велика частина мереж і операційних систем (ОС) використовують IP-адресу комп'ютера, для того, щоб визначати, чи той це адресат, який потрібний. В деяких випадках можливе некоректне привласнення IP (або MAC) – адреси або підміна цих адрес відправника іншою адресою. Такий спосіб атаки називають фальсифікацією адреси.
- Активні:
  - відмова в обслуговуванні (Denial of Service, DOS). Цей тип атак не націлений на діставання доступу до мережі або на здобуття з цієї мережі якої-небудь інформації. Атака DOS робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування якого-небудь ресурсу мережі, ОС або застосування. Вона паралізує роботу мережі і позбавляє звичайних користувачів доступу до загальних ресурсів організації. При цьому використовуються протоколи TCP і ICMP. Найбільш відомі: TCP SYN Flood; Ping of Death;
  - порушення роботи мережі або її ділянок – деякі недоліки протоколів канального рівню не можуть використовуватися передбаченим чином. Тобто, не можна навмисно вплинути на їх поведінку, але є можливість порушити їх нормальну роботу і таким чином розхитати відмовостійкість ділянки мережі або всієї мережі. Приклад: Переповнення таблиці комутації.

Забезпечення безпеки корпоративної мережі за OSI моделлю на мережному рівні (1)

Мережевий рівень – найбільш вразливий рівень з погляду захисту. На ньому формується вся маршрутизована інформація, відправник і одержувач фігурують явно, здійснюється управління потоком. Протоколи канального рівня локальних мереж забезпечують доставку даних між вузлами тільки в мережі з відповідною топологією. Це обмеження не дозволяє створювати мережі з розвинутою структурою.

Для виконання функцій по передачі даних між вузлами по мережі, мережний рівень використовує:

- адресацію;
- інкапсуляцію/декапсуляцию;
- маршрутизацію.

Протоколи мережного рівня: Ipv4, Ipv6, IPX, Appletalk, CLNS/Decnet. Характеристики Ipv4:

- без установлення сеансу (connectionless);
- ненадійний (unreliable) – не гарантує доставку (best effort), пакети можуть губитися, функції по забезпеченню надійності покладають на протоколи транспортного рівня;
- не залежить від середовища передачі (media independent), крім MTU, канальний рівень повідомляє розмір максимального блоку передачі (MTU) мережному рівню. При перевищенні розміру MTU пакет може бути фрагментований перед передачею.

Забезпечення безпеки корпоративної мережі за OSI моделлю на мережному рівні (2)

Замість того, щоб тримати всі пристрої в одній мережі, більш практично ділити їх на групи.
Групувати пристрої можна по:

- місцю знаходження – групувати вузли, що перебувають поруч (на одному поверсі, в одному будинку);
- цілям – групувати вузли по виконуваних завданнях і типах трафіку;
- приналежності – групувати вузли по приналежності до тієї або іншої компанії, відділу.

Проблеми великих мереж:

- зниження продуктивності – велика кількість вузлів в одному сегменті створює багато широкомовного трафіка, що навантажує мережу;
- погрози безпеки – у точку переходу з однієї мережі в іншу можна налаштувати обмеження за типом трафіку й адрес;
- управління адресацією – вузлам немає необхідності зберігати багато маршрутів, досить знати адреса свого шлюзу.

IP-Адреса є 32-бітною, ієрархічною та складається з 2 частин:

- мережна частина – указує на мережу, у якій перебуває вузол;
- вузлова частина – указує на вузол у мережі.

Розмір мережної частини визначається маскою мережі або довжиною префікса.

Забезпечення безпеки корпоративної мережі за OSI моделлю на мережному рівні (3)

Проблема вибору найкращого шляху називається маршрутизацією, і її вирішення є однією з головних задач мережного рівня.

На мережному рівні визначаються два види протоколів. Перший вид – мережні протоколи (routedprotocols) – реалізують переміщення пакетів в мережі. До мережного рівня відносять і інший вид протоколів, що називаються протоколами обміну маршрутною інформацією або протоколами маршрутизації (routing protocols). Протоколи мережного рівня реалізуються програмними модулями операційної системи, а також програмними і апаратними засобами маршрутизаторів.

Для передачі інформації між вузлами, що перебувають у різних мережах, необхідні маршрутизатори. Вони є прикордонними пристроями, що з'єднують мережі один з одним. Для маршрутизатора мережі в яких перебувають його порти є підключеними (directly connected). А ті мережі до яких підключені його сусіди – вилученими (remote). Якщо ПК потрібно відправити інформацію вузлу не з його мережі, то він направляє її своєму шлюзу. Шлюз (він же маршрутизатор) вибирає шлях передачі інформації ґрунтуючись на своїй таблиці маршрутів.

Порядок обробки таблиці маршрутизатором.

- рівняються адреси мереж і адреса призначення побітно. Вибирається адреса з найбільшим збігом біт;
- якщо немає жодного підходящого, тоді маршрут за замовчуванням;
- якщо немає ні першого, ні другого – пакет викидається, а на адресу джерела висилається повідомлення про помилку.

Забезпечення безпеки корпоративної мережі за OSI моделлю на транспортному рівні (1)

Протоколи сеансового рівня OSI/ISO забезпечують механізми управління сеансами управління сеансом, включаючи реєстрацію, управління діалогом і обмін параметрами сеансу. Ці протоколи описані в стандартах ISO 8326/CCITT X.215 (визначення і основні характеристики сеансової служби) і стандартах ISO 8327/CCITT X.225, визначальних специфікації протоколів:

- BCS – базової комбінованої підмножини;
- BSS – базової підмножини синхронізації;
- BAS – базової підмножини функціонування.

Протоколи рівня представлення OSI/ISO забезпечують прозорий для прикладних процесів зв’язок ES, реалізованих на різних комп’ютерних платформах і різному операційному середовищі. Ці протоколи описані в стандартах ISO 8822/CCITT X.216 (визначення служби) і ISO 8823/CCITT X.226, визначальній специфікації протоколу:

- базові процедури встановлення/закінчення з’єднання;
- контекстне управління (вибірка/видалення контексту);
- контекстне представлення при повторній синхронізації або відновленні активності.

На протоколи сеансового рівня і рівня представлення даних лягає основне навантаження по забезпеченню безпеки мережі. На сеансовому рівні безпека забезпечується за допомогою ідентифікаторів і паролів користувачів.

Забезпечення безпеки корпоративної мережі за OSI моделлю на транспортному рівні (2)

Сеансовий рівень є максимально високим рівнем моделі OSI, на якому можливе формування захищених віртуальних каналів. Протоколи формування захищених віртуальних каналів на сеансовому рівні прозорі для прикладних протоколів захисту, а також високорівневих протоколів надання різних сервісів (протоколів HTTP, FTP, POP3, SMTP, NNTP та ін.).

У загальному випадку програми-посередники, які традиційно використовуються в міжмережевих екранах, можуть виконувати такі функції:

- ідентифікація та автентифікація користувачів;
- криптозазист переданих даних;
- розмежування доступу до ресурсів внутрішньої мережі та розмежування доступу до ресурсів зовнішньої мережі;
- фільтрація і перетворення потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;
- трансляція внутрішніх мережевих адрес для вихідних пакетів повідомлень;
- реєстрація подій та реагування на поставлені події;
- кешування даних, запитуваних із зовнішньої мережі.

Забезпечення безпеки корпоративної мережі за OSI моделлю на транспортному рівні (3)

Протокол Secure Sockets Layer (SSL), споконвічно орієнтований на захист інформаційного обміну між клієнтом і сервером комп'ютерної мережі, є промисловим протоколом сеансового рівня моделі OSI використовують для забезпечення безпеки інформаційного обміну криптографічні методи захисту інформації. Конфіденційність переданих даних забезпечується за рахунок їх криптографічного закриття, а аутентифікація взаємодіючих сторін, а також достовірність і цілісність циркулюючої інформації – за рахунок формування та перевірки цифрового підпису.

Ядром протоколу SSL є технологія комплексного використання асиметричних і симетричних криптосистем.

Відповідно до протоколу SSL криптозахищені тунелі створюються між кінцевими точками віртуальної мережі. Протокол SSL передбачає два етапи взаємодії клієнта і сервера при формуванні та підтримці захищається з'єднання:

- встановлення SSL-сесії;
- захищене взаємодія.

У процесі становлення SSL-сесії вирішуються наступні завдання:

- аутентифікація сторін;
- узгодження криптографічних алгоритмів і алгоритмів стиснення, які будуть використовуватися при захищеному інформаційному обміні;
- формування спільного секретного майстер-ключа;
- генерація на основі сформованого майстер-ключа загальних секретних сеансових ключів для криптозахисту інформаційного обміну.

Забезпечення безпеки корпоративної мережі за OSI моделлю на транспортному рівні (4)

У режимі односторонньої аутентифікації сервера без аутентифікації клієнта процедура встановлення SSL-сесії між клієнтом і сервером включає наступні кроки.

Клієнт посилає серверу запит на встановлення захищеного з'єднання, в якому передає деякі формальні параметри цього з'єднання:

- поточний час і дату;
- випадкову послідовність (RAND_CL);
- набір підтримуваних клієнтом алгоритмів симетричного шифрування і алгоритмів обчислення геш-функції;
- набір підтримуваних алгоритмів стиснення та ін.

Сервер обробляє запит від клієнта і передає йому узгоджений набір параметрів:

- ідентифікатор SSL-сесії;
- конкретні криптографічні алгоритми з числа запропонованих клієнтом (якщо з якої-небудь причини запропоновані алгоритми або їх параметри не задовольняють вимогам сервера, сесія закривається);
- сертифікат сервера, завірений цифровим підписом центру сертифікації;
- випадкову послідовність (RAND_SERV).

Клієнт перевіряє отриманий сертифікат сервера за допомогою відкритого ключа центру сертифікації, який йому відомий. При негативному результаті перевірки сесія закривається, а при позитивному – клієнт виконує наступні дії:

- генерує випадкову 48-байтну послідовність Pre_MasterSecret, призначену для генерації загального секретного майстер-ключа; шифрує Pre_MasterSecret з відкритого ключа сервера, отриманому в сертифікаті сервера, і посилає серверу;
- за допомогою узгоджених геш-алгоритмів формує загальний секретний майстер-ключ (MasterSecret), використовуючи в якості параметрів послідовність Pre_MasterSecret, послану сервера випадкову послідовність RAND_CL і одержану від нього випадкову послідовність RAND_SERV;
- використовуючи MasterSecret, обчислює криптографічні параметри SSL-сесії: формує спільні з сервером сеансові секретні ключі для симетричного шифрування й обчислення геш-функцій;
- переходить в режим захищеної взаємодії.

Сервер розшифровує отриману послідовність Pre_MasterSecret за своїм закритим клюему і виконує на її основі ті ж операції, що і клієнт:

- за допомогою узгоджених геш-алгоритмів формує загальний секретний майстер-ключ (MasterSecret), використовуючи в якості параметрів Pre_MasterSecret, а також послану клієнту випадкову послідовність RAND_SERV і одержану від нього випадкову послідовність RAND_CL;
- використовуючи MasterSecret, обчислює криптографічні параметри SSL-сесії: формує загальні з клієнтом сеансові секретні ключі для симетричного шифрування й обчислення геш-функцій;
- переходить в режим захищеної взаємодії.

Забезпечення безпеки корпоративної мережі за OSI моделлю на транспортному рівні (5)

Для перевірки ідентичності параметрів SSLсесії клієнт і сервер посилають один одному тестові повідомлення, зміст яких відомо кожної зі сторін:

- клієнт формує повідомлення з власних посилок на адресу сервера на кроці 1 та посилок, отриманих від сервера на кроці 2, вносячи елемент випадковості у вигляді послідовності MasterSecret, унікальною для даної сесії; формує код для перевірки цілісності повідомлення (MAC), шифрує повідомлення за загальним сеансовому секретному ключу й відправляє серверу;
- сервер, у свою чергу, формує повідомлення з власних посилок на адресу клієнта на кроці 2, посилок, отриманих від клієнта на кроці 1, і послідовності MasterSecret; формує код для перевірки цілісності повідомлення (MAC), шифрує повідомлення на загальному сеансовому секретному ключі і відправляє клієнту;
- у разі успішного розшифрування і перевірки цілісності кожної зі сторін отриманих тестових повідомлень, SSL-сесія вважається встановленої і сторони переходять в штатний режим захищеної взаємодії.

У процесі захищеної взаємодії із встановленими криптографічними параметрами SSL-сесії виконуються наступні дії:

- кожна сторона при передачі повідомлення формує MAC-код для подальшої перевірки цілісності повідомлення і потім зашифровує вихідне повідомлення разом з MAC-кодом по сеансовому секретному ключу;
- кожна сторона при прийомі повідомлення розшифровує його і перевіряє на цілісність (обчислюється поточний MAC-код і звіряється з MAC-кодом перевірки цілісності, отриманим разом з повідомленням);
- у разі виявлення порушення цілісності повідомлення, SSL-сесія закривається.

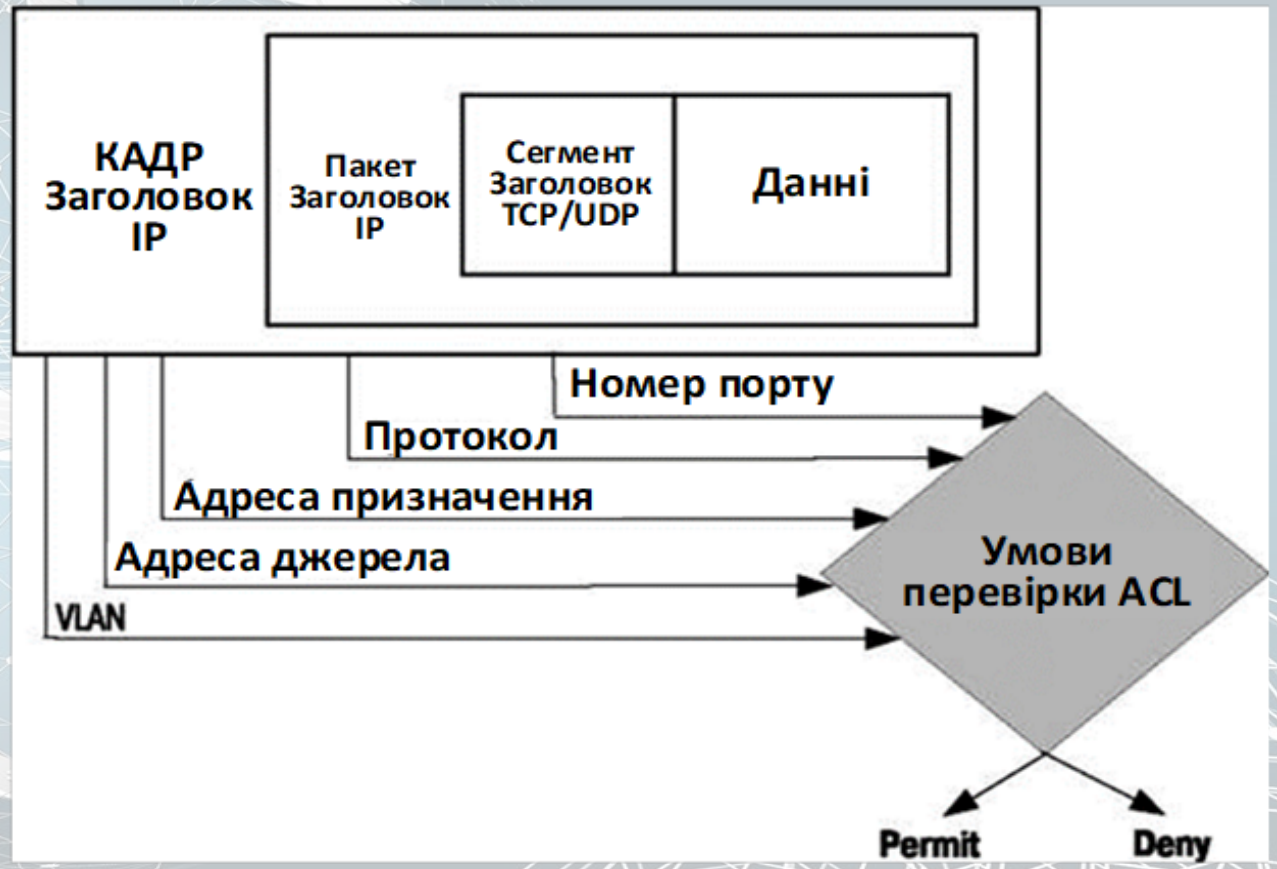
Створення списків управління доступом (ACL) (1)

Списки управління доступом (Access Control List, ACL) є потужним засобом фільтрації потоків даних без втрати продуктивності, оскільки перевірка вмісту пакетів виконується на апаратному рівні

ACL є послідовністю умов перевірки параметрів пакетів даних. Коли повідомлення поступають на вхідний порт, комутатор перевіряє параметри пакетів даних на збіг з крите-риями фільтрації, визначеними в ACL, і виконує над пакетами одну з дій: permit («дозволити») або deny («заборонити»).

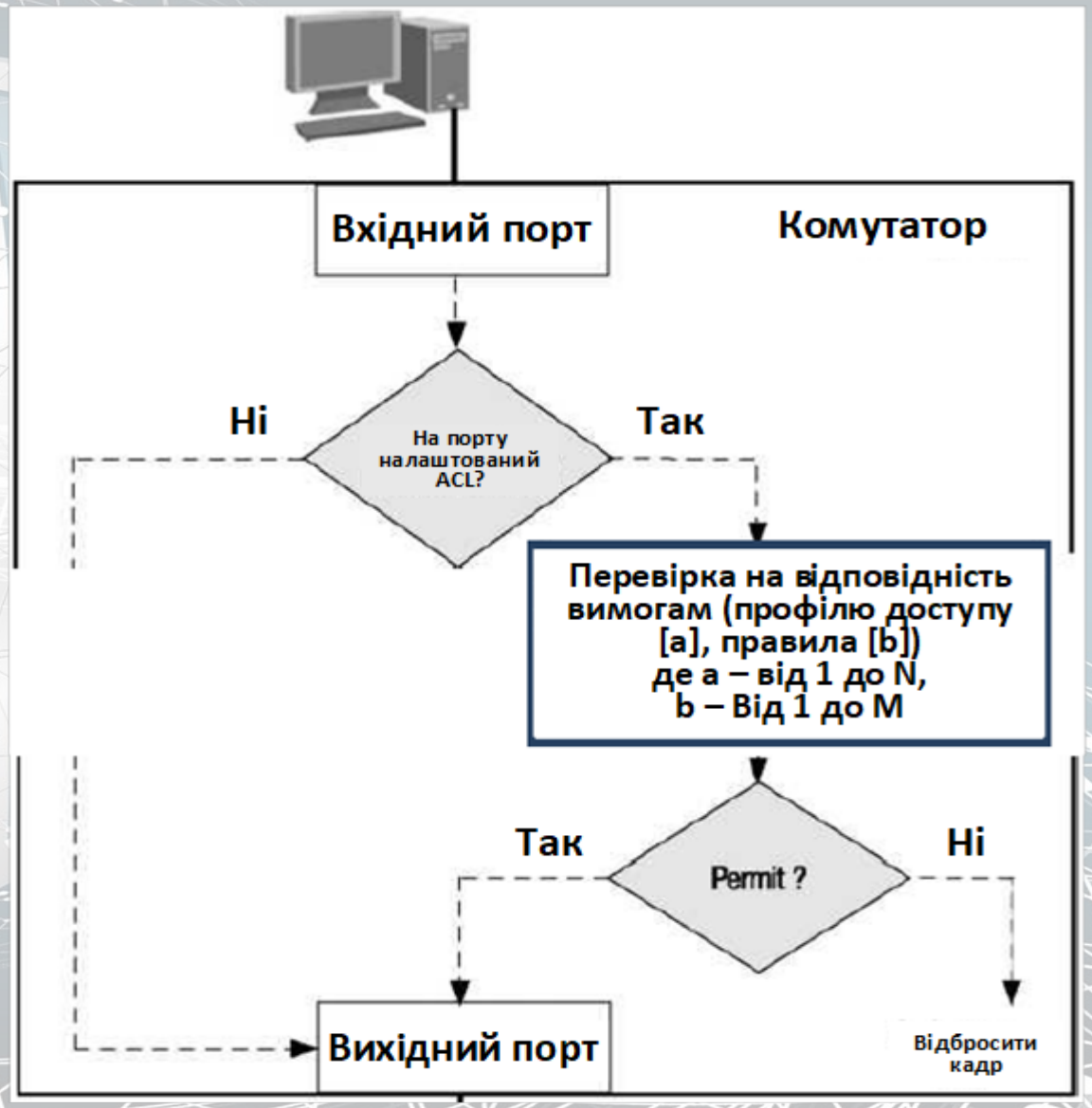
Критерії фільтрації можуть бути визначені на основі наступної информації, що міститься в пакеті:

– порт комутатора;
– MAC/IP-адрес;
– тип Ethernet/ тип протоколу;
– VLAN;
– 802.1p/DSCP;
– порт TCP/UDP (тип додатка);
– перші 80 байт пакету, включаючи поле даних.



Створення списків управління доступом (ACL) (2)

Списки управління доступом складаються з профілів доступу (Access Profile) і правил (Rule). Профілі доступу визначають типи критеріїв фільтрації, які повинні перевірятися в пакеті даних (MAC-адреса, IP-адреса, номер порту, VLAN і так далі), а в правилах безпосередньо вказуються їх значення. Коли комутатор отримує кадр, він перевіряє його поля на збіг з типами критеріїв фільтрації і їх параметрами, заданими в профілях і правилах. Послідовність, в якій комутатор перевіряє кадр на збіг з параметрами фільтрації (рис. 3.2), визначається порядковим номером профілю (Profile ID) і порядковим номером правила (Rule ID). Профілі доступу і правила усередині них працюють послідовно, в порядку зростання їх номерів. Тобто кадр перевіряється на відповідність умовам фільтрації, починаючи з першого профілю і першого правила в нім. Так, кадр спочатку перевірятиметься на відповідність умовам, визначеним в правилі 1 профілю 1.



Створення списків управління доступом (ACL) (3)

Процес створення профілю доступу можна розділити на такі основні кроки:

- аналіз завдання фільтрації і визначення типу профілю доступу – Ethernet, IP або Packet Content Filtering;
- визначення стратегії фільтрації. Наприклад: відкидати кадри деяких вузлів і приймати кадри від усіх інших вузлів – ця стратегія застосовна для мережевого середовища з декількома вузлами/протоколами портів/підмережами, для яких необхідно виконувати фільтрацію; приймати кадри від деяких вузлів і відкидати кадри усіх інших вузлів – ця стратегія застосовна для мережевого середовища з декількома вузлами/протоколами портів/підмережами, кадри від которых дозволені в мережі. Трафік інших вузлів відкидатиметься;
- визначення, маски профілю доступу (Access Profile Mask) і створення її (команда create access_profile). Маска профілю доступу використовується для вказівки, які біти значень полів IP -адрес, MAC-адреса, порт TCP/UDP і так далі повинні перевірятися в пакеті даних, а які ігноруватися;
- додавання правила профілю доступу (Access Profile Rule), пов'язане з цією маскою (команда config access_profile). Правила профілю доступу перевіряються відповідно до номера access_id. Чим менший номер, тим раніше перевіряється правило. Якщо жодне правило не спрацювало, кадр пропускається.

Маска профілю доступу визначає, які біти в значеннях полів «IP-адрес», «MAC-адреса», «порт TCP/UDP» і так далі що приходять на комутатор кадрів повинні перевірятися, а які ігноруватися (рис.)

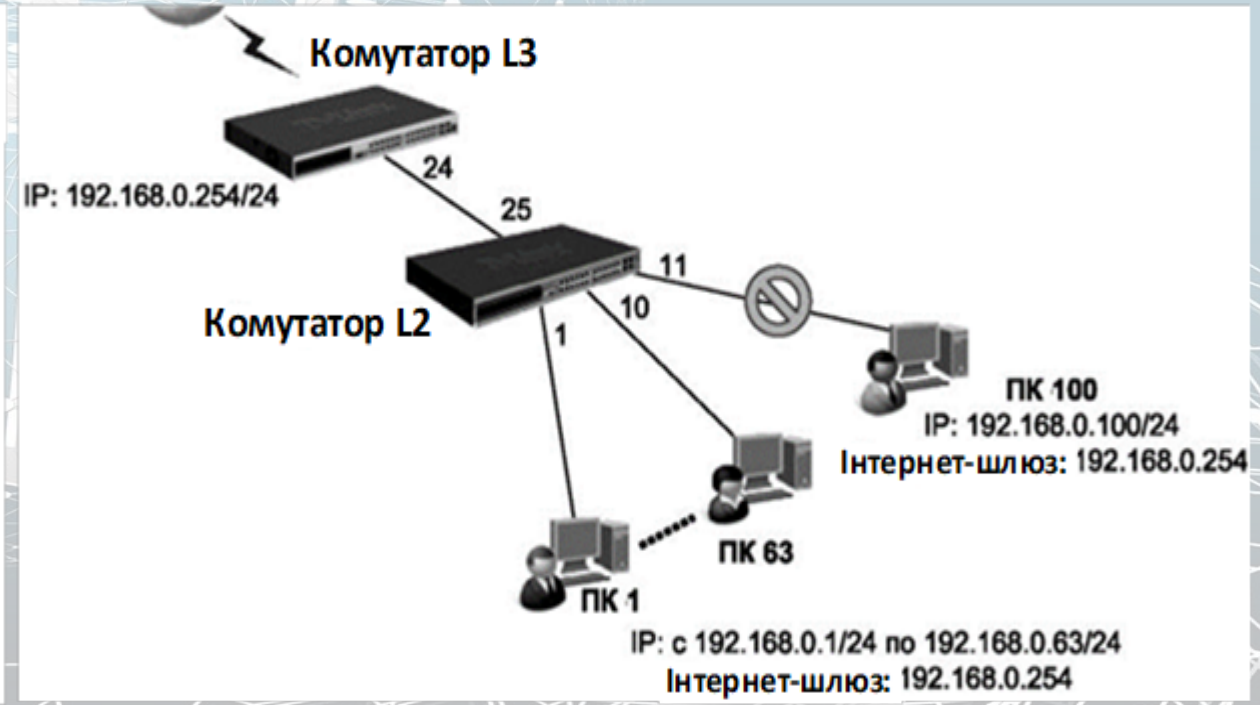


Створення списків управління доступом (ACL) (4)

У прикладі, показаному на рис., користувачі ПК 1 і ПК 2 отримають доступ в інтернет, оскільки їх MAC-адреси вказані в дозволяючому правилі 1. Як тільки користувачі інших комп'ютерів спробують вийти в інтернет, спрацює правило 2, яке забороняє проходження через комутатор кадрів з MAC-адресою призначення, рівною MAC-адресі інтернет-шлюзу.

В якості другого прикладу приведемо налаштування ACL з профілем IP (рис. праворуч).



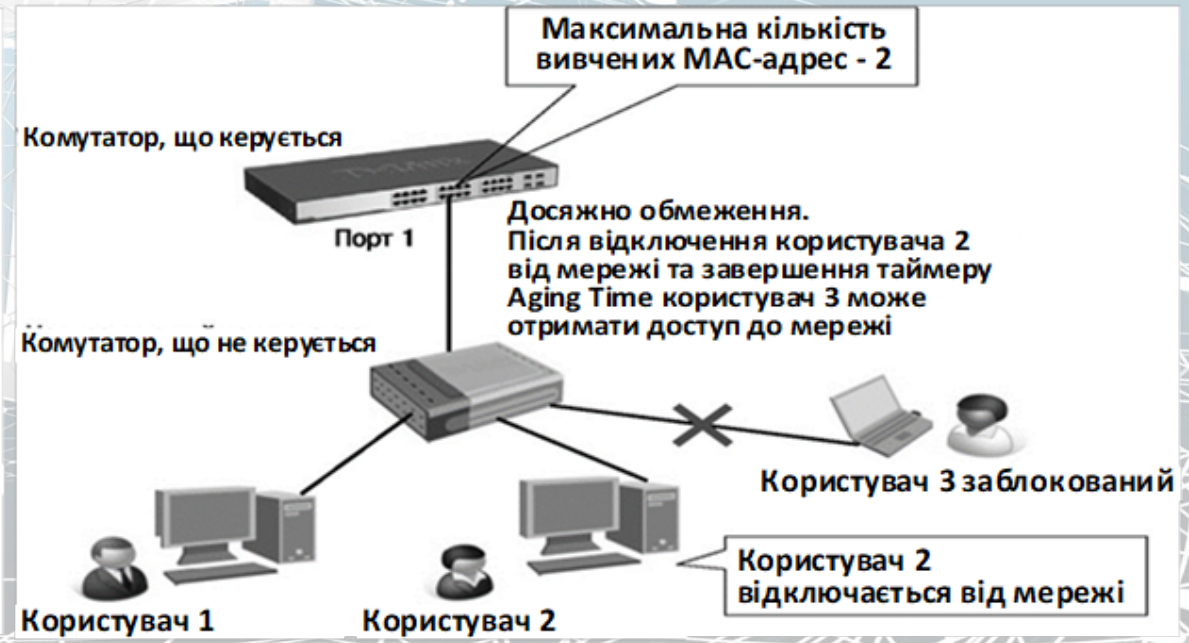


Функції контролю підключення вузлів до портів комутатора (1)

Функція Port Security (рис.ліворуч) дозволяє настроїти який-небудь порт комутатора так, щоб доступ до мережі через нього міг здійснюватися тільки певними пристроями. Пристрої, яким дозволено підключатися до порту, визначаються за MAC-адресами. MAC-адреси можуть бути вивчені динамічно або вручну налагоджені адміністратором мережі. Окрім цього, функція Port Security дозволяє обмежувати кількість MAC-адрес, що вивчаються портом, тим самим обмежуючи кількість вузлів, що підключаються до нього.

У наведеному прикладі конфігурації використовується режим Delete on Timeout. Це означає, що вивчені на порту MAC-адреси будуть видалені з таблиці комутації після закінчення часу, встановленого таймером Aging Time, якщо по них не було звернень (наприклад, робоча станція відключилася від мережі). В цьому випадку до мережі зможуть підключиться нові користувачі, MAC-адреси, яких будуть динамічно вивчені портом (рис. праворуч).





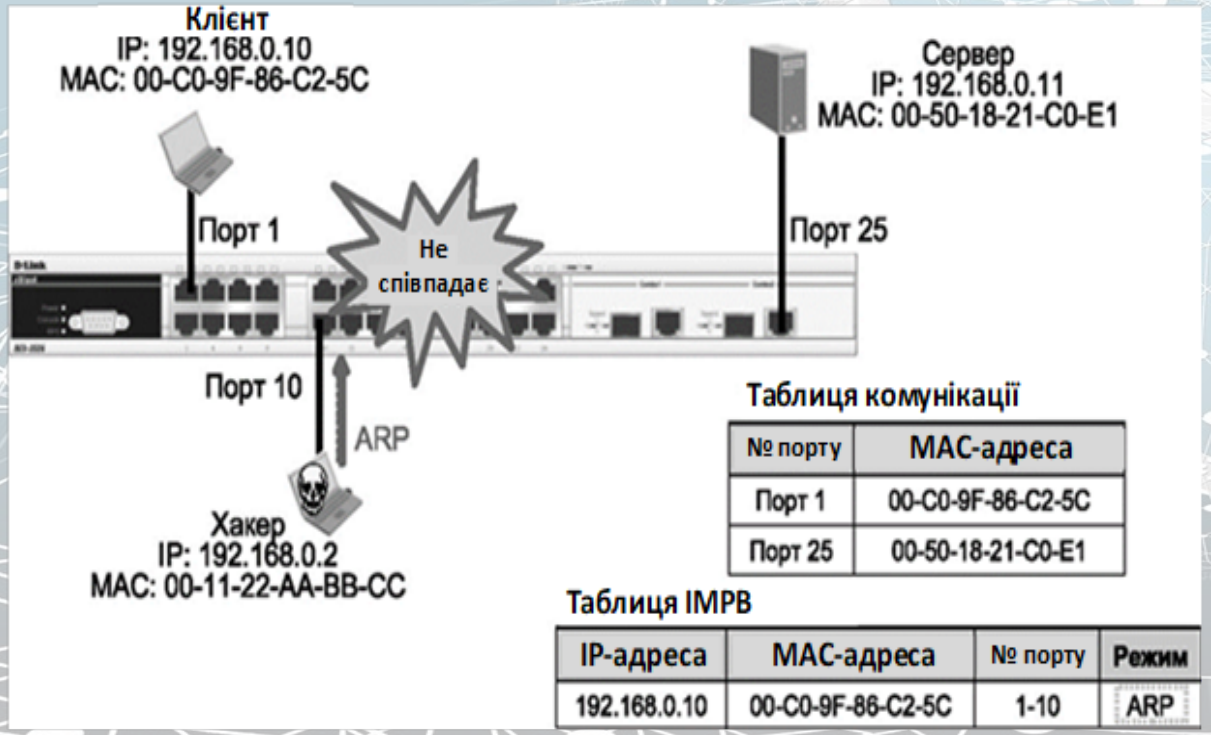
Функції контролю підключення вузлів до портів комутатора (2)

- Функція IP-MAC-Port Binding (IMPB), реалізована в комутаторах D-Link, дозволяє контролювати доступ комп'ютерів в мережу на основі їх IPта MACадрес, а також порту підключення (рис.). Адміністратор мережі може створити записи («білий лист»), зв'язуючі MACта IP-адреси комп'ютерів з портами підключення комутатора. На основі цих записів, у разі збігу усіх складових, клієнти діставатимуть доступ до мережі зі своїх комп'ютерів. У тому випадку, якщо при підключенні клієнта зв'язка MAC-IP-порт відрізнятиметься від параметрів заздалегідь зконфігурованого запису, комутатор заблокує MAC-адресу відповідного вузла із занесенням його в «чорний лист».
- Функція IP-MAC-Port Binding спеціально розроблена для управління підключенням вузлів в мережах ETTH (Ethernet-to-the-Home) і офісних мережах. Окрім цього функція IMPB дозволяє боротися з атаками типу ARPSpoofing, під час яких зловмисні користувачі перехоплюють трафік або переривають з'єднання, маніпулюючи пакетами ARP.



Функції контролю підключення вузлів до портів комутатора (3)

- На рис. ліворуч показано приклад роботи функції IP-MAC-Port Binding в режимі ARP.
- На рис. праворуч показаний приклад роботи функції IP – MAC – PortBinding в режимі DHCP Snooping. Комутатор динамічно створює запис IMPB після того, як клієнт отримає IP-адрес від DHCP-сервера.

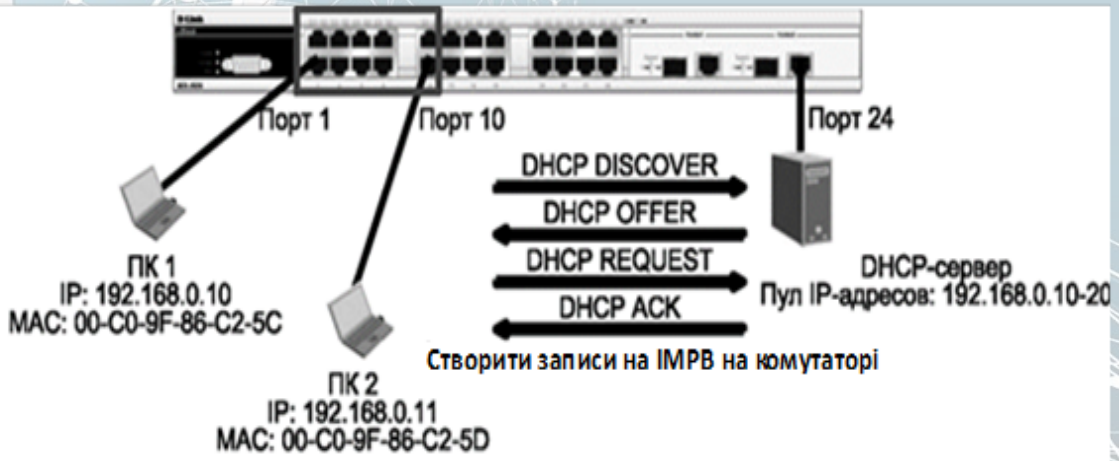


Таблиця комунікації

№ порту	MAC-адреса
Порт 1	00-C0-9F-86-C2-5C
Порт 25	00-50-18-21-C0-E1

Таблиця IMPB

IP-адреса	MAC-адреса	№ порту	Режим
192.168.0.10	00-C0-9F-86-C2-5C	1-10	ARP



Таблиця записів DHCP Snooping

IP Address	MAC Address	Lease Time	Ports	Status
192.168.0.10	00-C0-9F-86-C2-5C	86390	1	Active
192.168.0.11	00-C0-9F-86-C2-5D	86395	10	Active

Таблиця IP-MAC-Port Blinding

IP Address	MAC Address	Ports	Mode
192.168.0.10	00-C0-9F-86-C2-5C	1	AUTO
192.168.0.11	00-C0-9F-86-C2-5D	10	AUTO

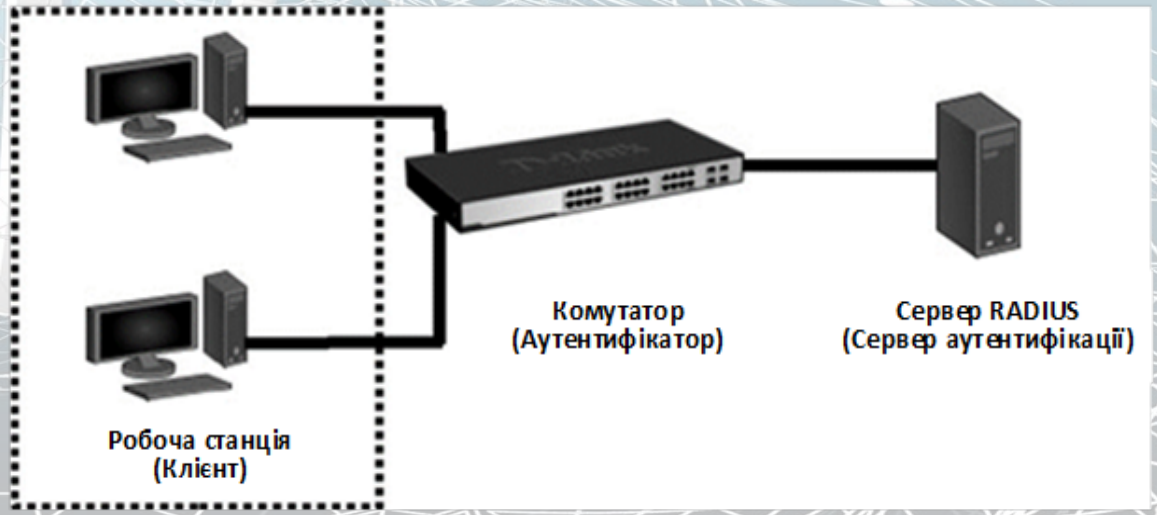
Комутатор автоматично створює записи IP-MAC-Port Blinding коли отримує пакет DHCP

Проведення аутентифікації користувачів за стандартом IEEE 802.1X (1)

У стандарті IEEE 802.1X визначені наступні три ролі, які можуть виконувати пристрої (рис. зверху) (окремо по складовим рис. знизу):

- Клієнт (client/supplicant) – це робоча станція, яка просить доступ до локальної мережі і сервісів комутатора і відповідає на запити від коммутатора
- Сервер аутентифікації (authentication server) виконує фактичну аутентифікацію клієнта
- Аутентифікатор (authenticator) управляє фізичним доступом до мережі, ґрунтуючись на статусі аутентифікації клієнта

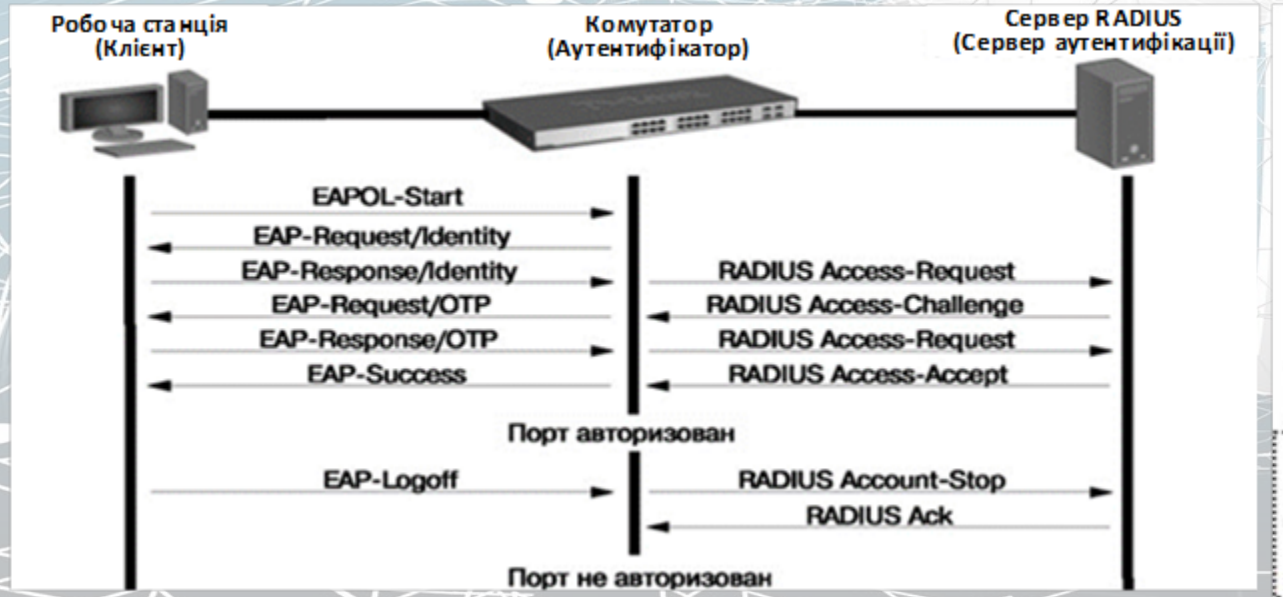


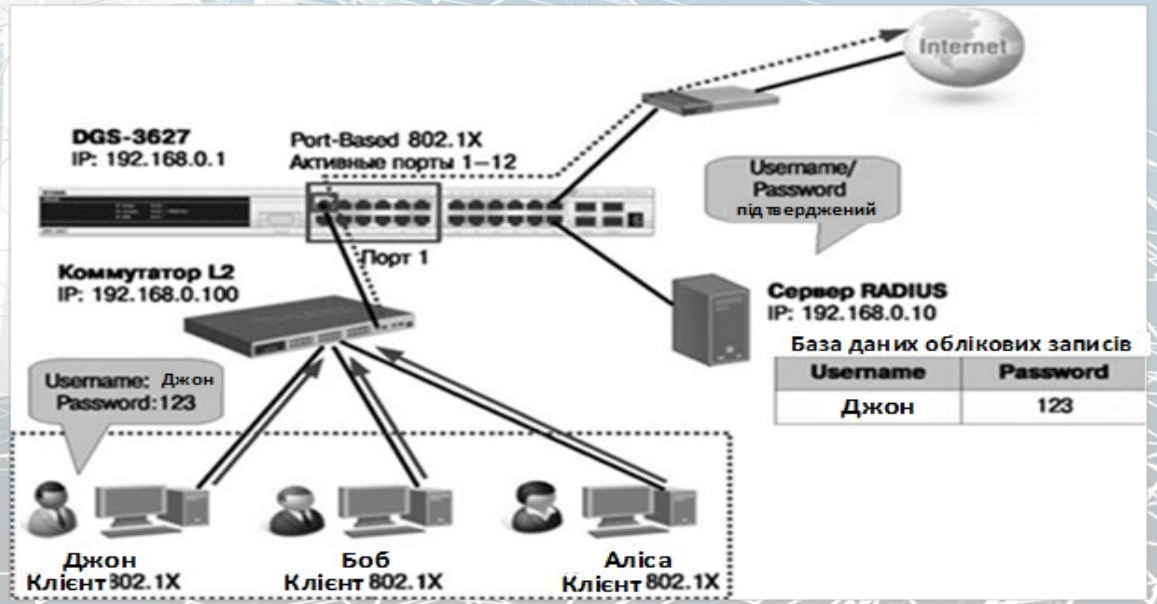


Проведення аутентифікації користувачів за стандартом IEEE 802.1X (2)

Схема обміну EAP-кадрами залежить від використовуваного аутентифікації. На рис.ліворуч показана схема обміну, що ініціюється клієнтом, де сервером RADIUS використовується метод аутентифікації One – Time – Password (OTP).

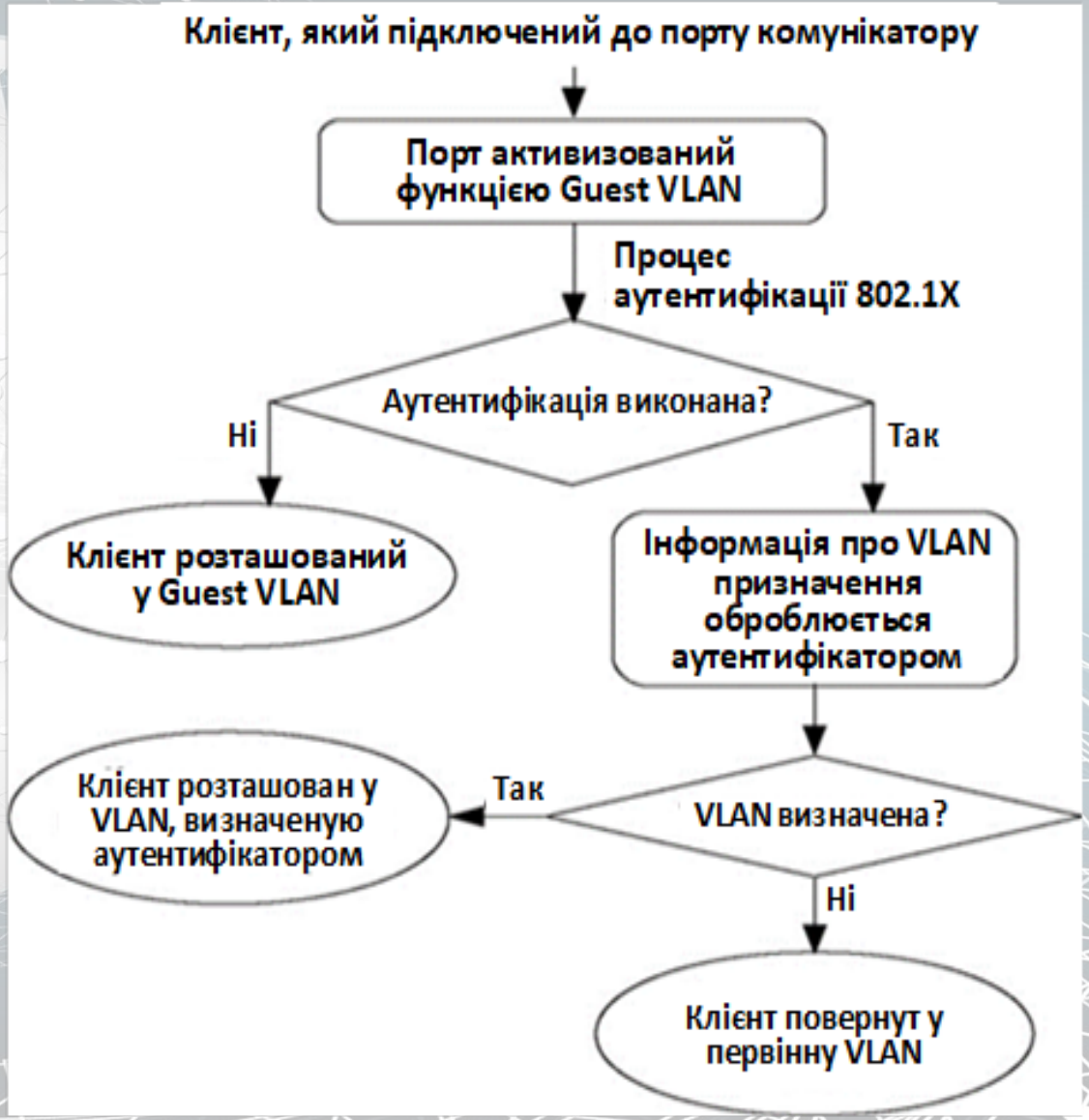
При аутентифікації 802.1X на основі портів (port-based 802.1X), після того, як порт був авторизований, будь-який користувач, підключений до нього, може отримати доступ до мережі. Розглянемо приклад налаштування функції portbased 802.1X для схеми, показаної на рис. праворуч





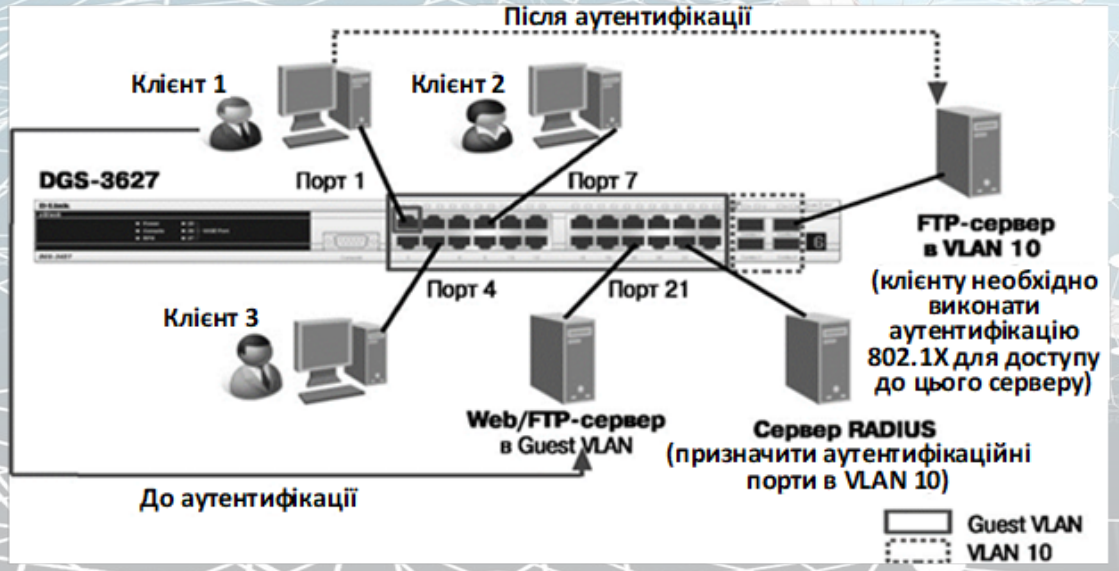
Створення гостьової VLAN з обмеженими правами (1)

- Функція Guest VLAN підтримується тільки для аутентифікації 802.1X на базі портів. Слід зазначити, що, використовуючи функцію 802.1X Guest VLAN, клієнтам можна надавати ряд обмежених сервісів до проходження процесу аутентифікації 802.1X.
- Члени Guest VLAN можуть взаємодіяти один з одним в межах цієї VLAN, навіть якщо вони не пройшли аутентифікацію 802.1X. Після успішного проходження аутентифікації член Guest VLAN може бути переміщений в VLAN призначення (Target VLAN) відповідно до атрибуту VLAN, вказаному на сервері RADIUS. Клієнт може завантажити з сервера і встановити необхідне програмне забезпечення 802.1X. Наочніше цей процес приведений на блок-схемі (рис.)



Створення гостьової VLAN з обмеженими правами (2)

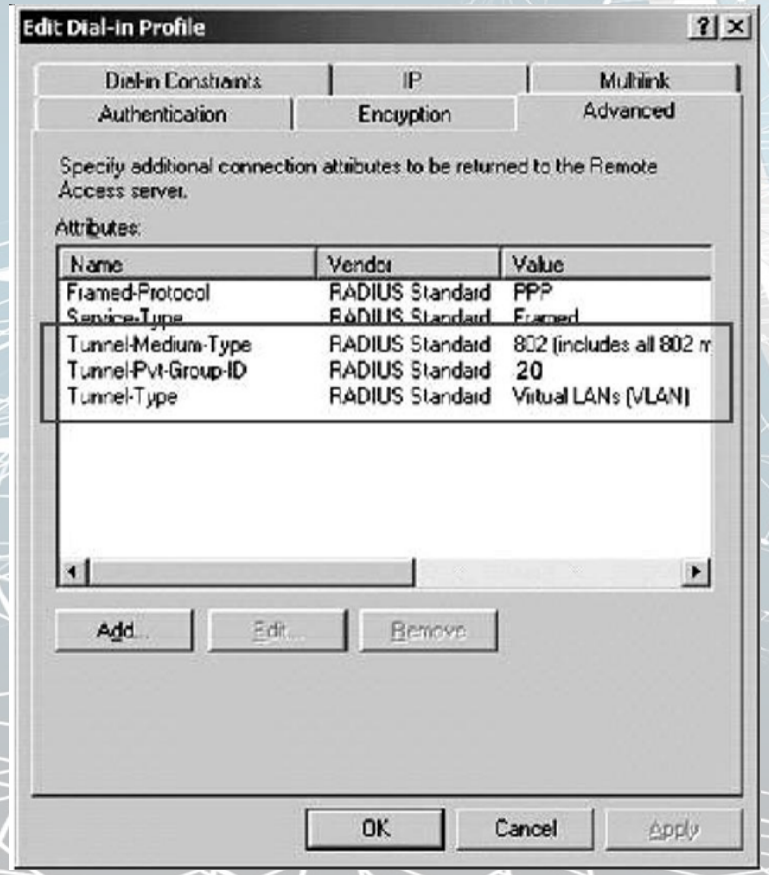
- Розглянемо приклад, показаний на рис.ліворуч. До аутентифікації клієнт 1 знаходиться в Guest VLAN і має доступ до робочих станцій, розташованих в ній, і загальнодоступному web/FTP-серверу. Після успішної аутентифікації клієнта 1 порт комутатора, до якого він підключений, буде додано в VLAN 10 і клієнт 1 зможе отримати доступ до конфіденційної інформації, що зберігається на FTPсервері VLAN 10. Якщо клієнт не пройшов аутентифікацію 802.1X, він залишиться в Guest VLAN з обмеженими правами.
- Як приклад використання і налаштування функції 802.1X Guest VLAN розглянемо схему мережі компанії (рис.праворуч), в якій користувачам неминувшим аутентифицію, що знаходиться в VLAN 10, дозволений доступ в інтернет. Після успішної аутентифікації користувачів, порти, до яких вони підключені, будуть додані в VLAN 20.





Створення гостьової VLAN з обмеженими правами (3)

- Налаштування параметрів на сервері RADIUS включає установку наступних призначених для користувача атрибутів



Перевірити конфігурацію комутатора можна за допомогою наступних команд:

```
DGS-3627#show 802.1x auth_configuration
Command: show 802.1x auth_configuration

802.1X                          : Enabled
Authentication Mode             : Port_based
Authentication Protocol         : RADIUS_EAP

Port number             : 1
Capability              : None
AdminCrlDir             : Both
OpenCrlDir              : Both
Port Control            : Auto
```

```
QuietPeriod             : 60 sec
TxPeriod                : 30 sec
Supp Timeout            : 30 sec
Server Timeout          : 30 sec
MaxReq                  : 2 times
ReAuthPeriod            : 3600 sec
ReAuthenticate          : Disabled

DGS-3627#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
---------------------------------

Guest VLAN : v10
Enable Guest VLAN Ports : 13-24

DGS-3627#show radius
Command: show radius

Idx  IP Address      Auth-Port  Acct-Port  Status  Key
---  --------------  ---------  ---------  ------  ------
 1   192.168.0.10    1812       1813       Active  123456

Total Entries: 1
```

Створення гостьової VLAN з обмеженими правами (4). Функції захисту ЦП комутатора

Комутатор може виконувати одну з наступних дій для зменшення завантаження ЦП:

- припинення отримання усіх ARP-пакетів і широкомовних IP-пакетів (при роботі функції в строгому режимі, strict mode);
- обмеження смуги пропускання для отримуваних ARP-пакетів і широкомовних IP-пакетів шляхом її динамічної зміни (при роботі функції в нестрогому режимі, fuzzy mode).

При нормалізації роботи мережі і зниженні кількості небажаних пакетів до встановленого нижнього порогового значення Falling Threshold комутатор вийде з режиму високого завантаження і механізм Safeguard Engine перестане функціонувати. Слід зазначити, що при перемиканні комутатора в режим Exhausted можуть виникати наступні побічні ефекти:

- при роботі функції Safeguard Engine в строгому режимі неможливо здійснювати адміністративний доступ до комутатора рівня 2, оскільки цей режим передбачає відкидання усіх ARP-запитів, ЦП, що поступають на інтерфейс. Для вирішення цієї проблеми в статичній ARP-таблиці робочої станції, що управляє, можна створити запис, зв’язуючий MAC-адресу комутатора з IP-адресою його інтерфейсу управління. В цьому випадку робочій станції не потрібно буде відправляти ARP-запит комутатору;
- при роботі функції Safeguard Engine в строгому режимі на комутаторі рівня 3, окрім неможливості адміністративного доступу, також може бути порушена маршрутизація між підключеними до нього підмережами, оскільки відкидатимуться ARP-запити, які поступають не лише на інтерфейс ЦП, але і на IPінтерфейси комутатора.

Створення гостьової VLAN з обмеженими правами (5). Функції захисту ЦП комутатора

Налаштування комутатора:

- активізуйте функцію Safeguard Engine:

  config safeguard_engine state enable

- задайте нижнє і верхнє порогові значення (вказуються значення у відсотках від завантаження ЦП), при яких відбуватиметься перемикання між нормальним режимом роботи і режимом Exhausted. Вкажіть режим роботи функції:

  config safeguard_engine utilization rising 40 falling 25 mode strict

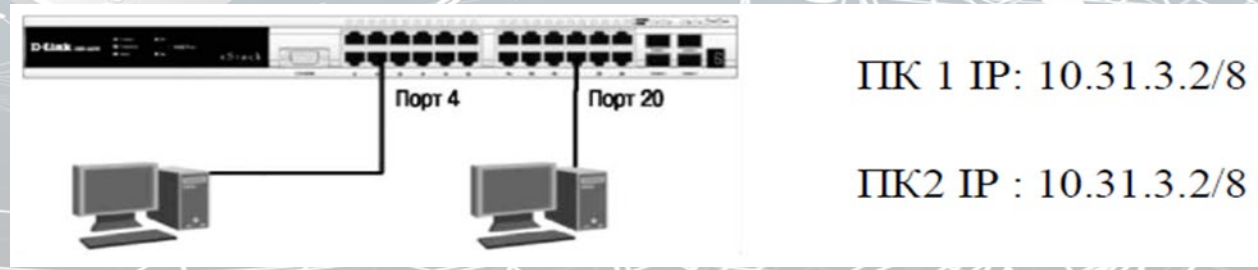
- активізуйте функцію Safeguard Engine:

  config safeguard_engine state enable

- задайте нижнє і верхнє порогові значення (вказуються значення у відсотках від завантаження ЦП), при яких відбуватиметься перемикання між нормальним режимом роботи і режимом Exhausted. Вкажіть режим роботи функції:

  config safeguard_engine utilization rising 40 falling 25 mode strict

Як приклад розглянемо завдання, в якому необхідно настроїти комутатор так, щоб пакети ICMP, що передаються комп'ютером ПК 2, не вирушали на обробку на ЦП, але при цьому ПК 2 міг передавати дані іншим пристроям, наприклад ПК 1.



Запитання для самоконтролю

1. Методи забезпечення надійності програмного забезпечення.
2. Формування інструментально-технологічних комплексів.
3. Ієрархічна декомпозиція в моделі OSI/ISO.
4. Загрози в архітектурі відкритих мереж в моделі OSI/ISO.
5. Процедури захисту в моделі OSI/ISO.
6. Сервісні служби захисту в моделі OSI/ISO.
7. Адміністрування засобів захисту в моделі OSI/ISO.
8. Реалізація захисту в моделі OSI/ISO.
9. Основні положення загальних критеріїв безпеки інформаційних технологій стандарту ISO 15408.
10. Функціональні вимоги до засобів захисту стандарту ISO 15408.
11. Вимоги гарантій засобів захисту стандарту ISO 15408.
12. Рівні гарантій безпеки стандарту ISO 15408.
13. Мета розробки, основні положення та склад загальних критеріїв стандарту ISO 15408.
14. Потенційні загрози безпеці та типові завдання захисту стандарту ISO 15408.
15. Продукт інформаційних технологій стандарту ISO 15408.
16. Профіль захисту стандарту ISO 15408.
17. Проект захисту стандарту ISO 15408.
18. Забезпечення безпеки на фізичному рівні моделі OSI.
19. Комунікаційні сигнали та кодування.
20. Забезпечення безпеки на транспортному рівні моделі OSI.

Технологія побудови захищеної корпоративної мережі

У сучасних IP –мережах існує три способи відправки пакетів від джерела до приймача:

- одноадресна передача (unicast);
- широкомовна передача (broadcast);
- багатоадресна розсилка (multicast).

При одноадресній передачі потік даних передається від вузла відправника на індивідуальну IP-адресу конкретного вузла одержувача. Широкомовна передача передбачає доставку потоку даних від вузла відправника безлічі вузлів одержувачів, підключених до мережі, з використанням широкомовної IP-адреси.

Багатоадресна розсилка забезпечує доставку потоку даних групі вузлів на IP-адресу групи багатоадресної розсилки. У цієї групи немає фізичних або географічних обмежень: вузли можуть знаходитися у будь-якій точці світу. Вузли, які зацікавлені в отриманні даних для певної групи, повинні приєднатися до цієї групи (підписатися на розсилку) за допомогою протоколу IGMP (Internet Group Management Protocol, міжмережевий протокол управління групами). Після цього пакети багатоадресної розсилки IP, що містять в полі призначення заголовка групову адресу, поступатимуть на цей вузол і оброблятися.

Адресація багатоадресної IP-розсилки (1)

Формат IP-адреси класу D показаний на рис. Перші 4 біта адреси завжди рівні 1110, інші 28 біт використовуються для ідентифікації конкретної групи одержувачів багатоадресного трафіку.

1	1	1	0	Multicast ID
Перші 4 біта				28 біт

MAC-адреса групової розсилки розпочинається з префікса, що складається з 24 бітів, – 0x01-00-5E. Наступний, 25-й біт (чи біт високого порядку) прирівнюється до 0. Останні 23 біта MAC-адреси формуються з 23 молодших бітів групового IP-адреса. Це проілюстровано на рис.

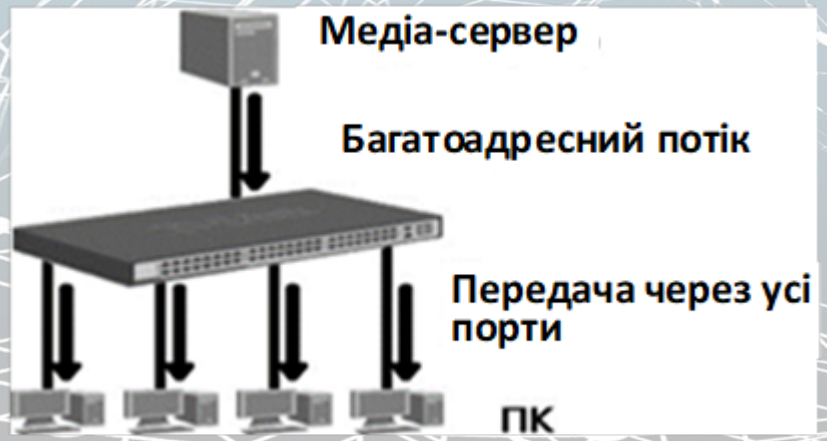


Адресація багатоадресної IP-розсилки (2)

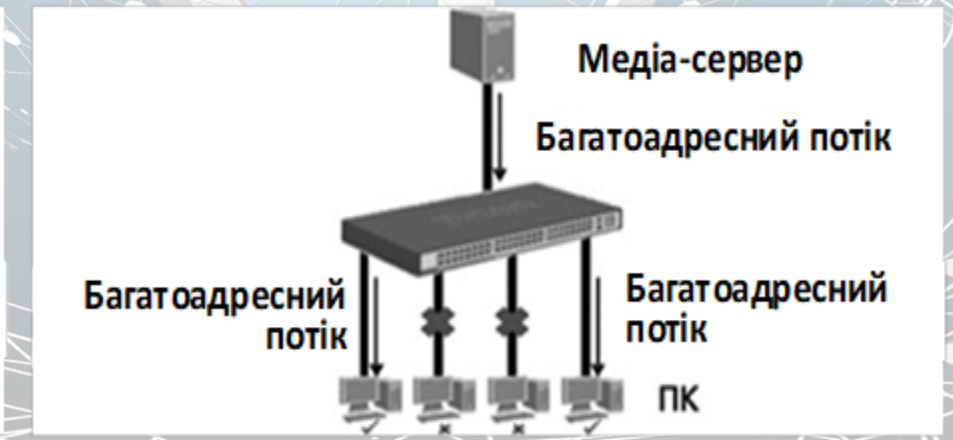
У загальному випадку протокол IGMP визначає наступні типи повідомлень:
- запит про приналежність до групи (membership query);
- відповідь про приналежність до групи (membership report);
- повідомлення про вихід з групи (leave group message).

Нині існують три версії протоколу IGMP:
- IGMP версії 1 (IGMP v1, описаний в RFC 1112);
- IGMP версії 2 (IGMP v2, описаний в RFC 2236);
- IGMP версії 3 (IGMP v3, описаний в RFC 3376).

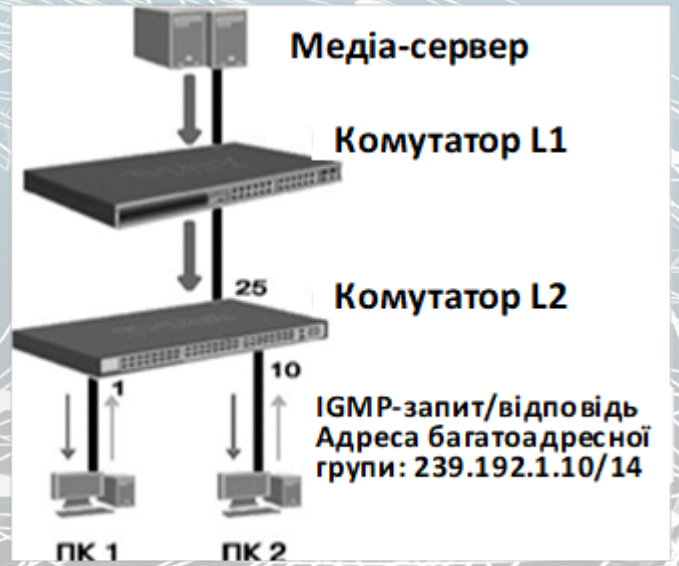
Передача багатоадресного трафіку без підтримки управління ним на комутаторі



Передача багатоадресного трафіку з підтримкою IGMP Snooping

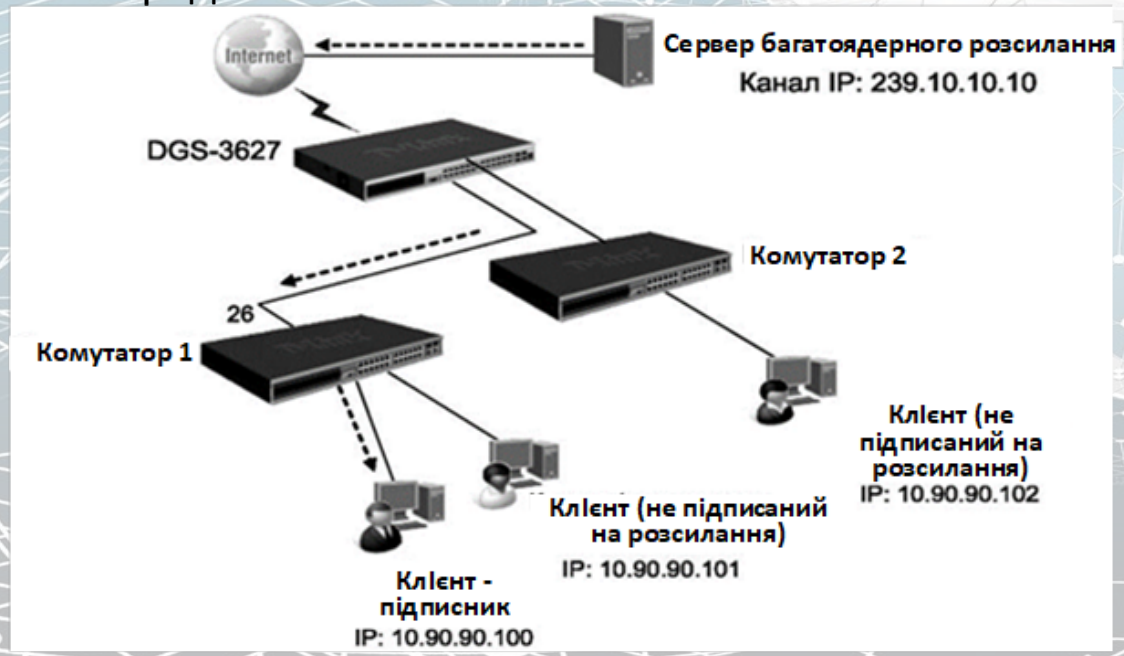


Процес створення таблиці комутації IGMP Snooping



Адресація багатоадресної IP-розсилки (3)

- Розглянемо приклад налаштування функції IGMP Snooping на комутаторах D-Link. На рис.ліворуч показана схема мережі, в якій реалізований сервіс багатоадресної розсилки. Клієнти, серед яких є передплатники багатоадресної розсилки, підключені до комутаторів другого рівня.
- На рис.праворуч приведена схема мережі, в якій на комутаторі 2 активізована функція IGMP Snooping Fast Leave. Усі порти комутатора 2 знаходяться в VLAN за замовчуванням (Default VLAN). До одного з портів комутатора підключений вузол-передплатник багатоадресної розсилки. Функція IGMP Snooping Fast Leave корисна в додатках IPTV, оскільки завдяки ній можна зменшити час відгуку, коли користувачі перемикаються між телевізійними каналами. Слід зазначити, що порт буде видалений з таблиці комутації IGMP Snooping тільки у тому випадку, якщо до нього більше не підключено жодного вузла-передплатника.



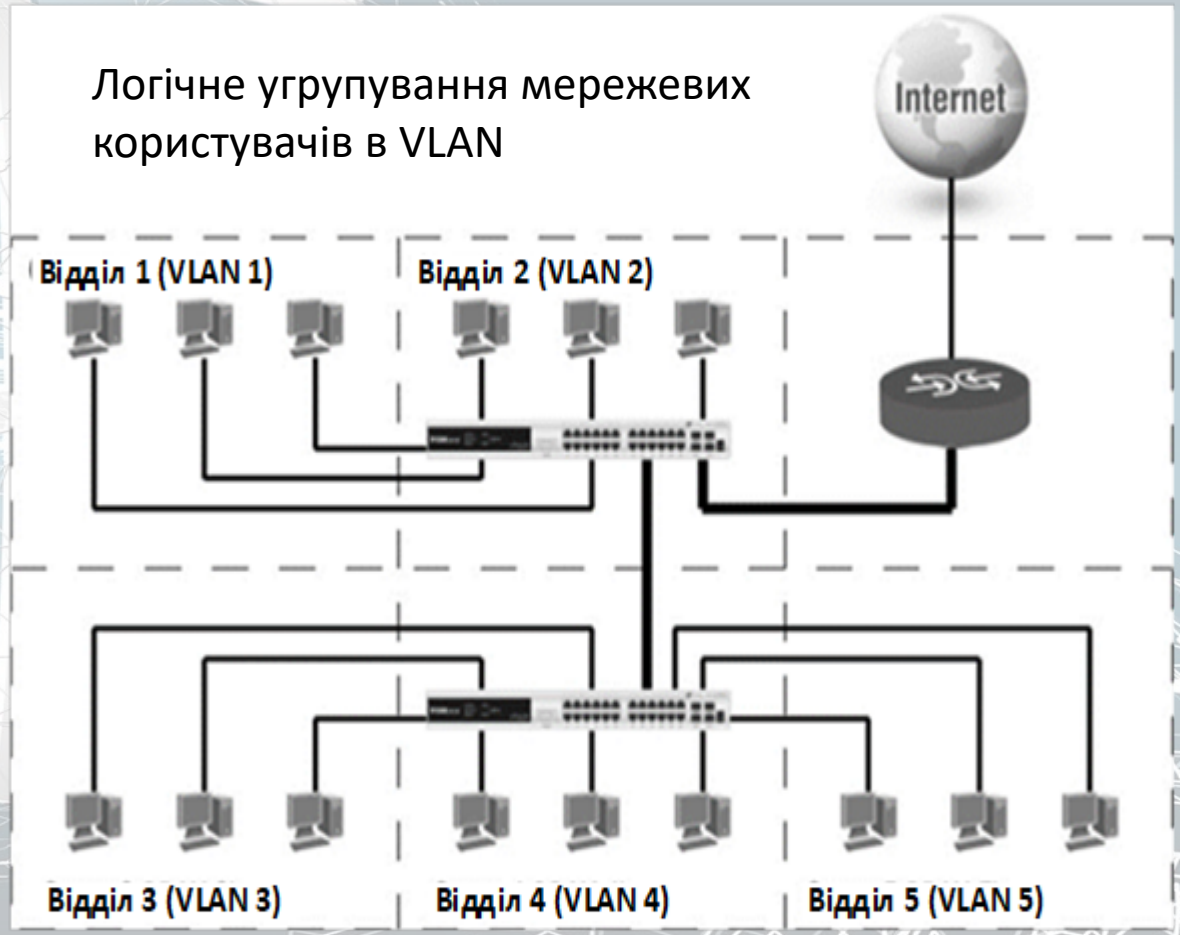


Технології побудови віртуальних локальних мереж (VLAN) (1)

Логічна сегментація мереж за допомогою технології VLAN

VLAN мають наступні переваги:

- гнучкість впровадження. VLAN є ефективним способом угрупування мережевих користувачів у віртуальні робочі групи, незважаючи на їх фізичне розміщення в мережі;
- забезпечують можливість контролю широкомовних повідомлень, що збільшує смугу пропускання, доступну для користувача;
- дозволяють підвищити безпеку мережі, визначивши за допомогою фільтрів, налагоджених на комутаторі або маршрутизаторі, політику взаємодії користувачів з різних віртуальних мереж.

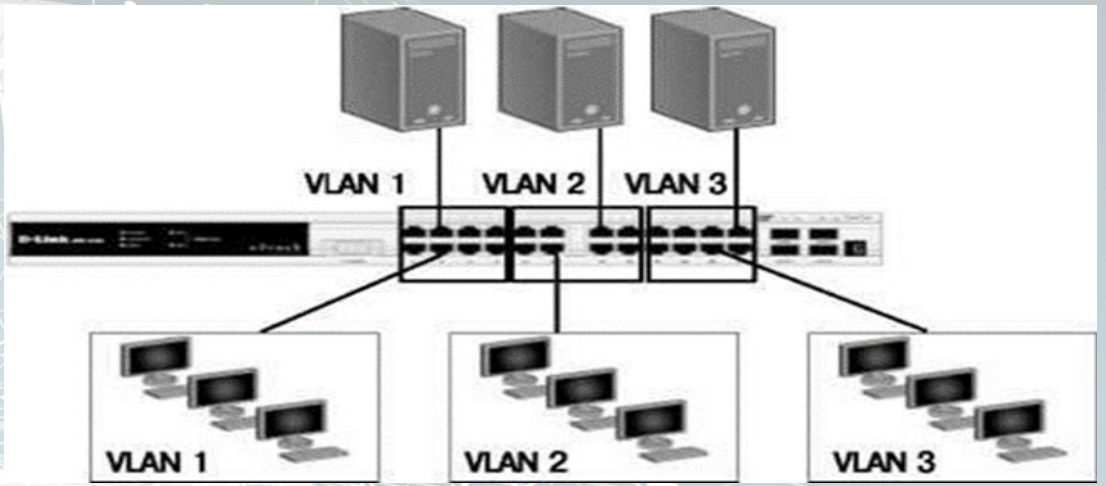


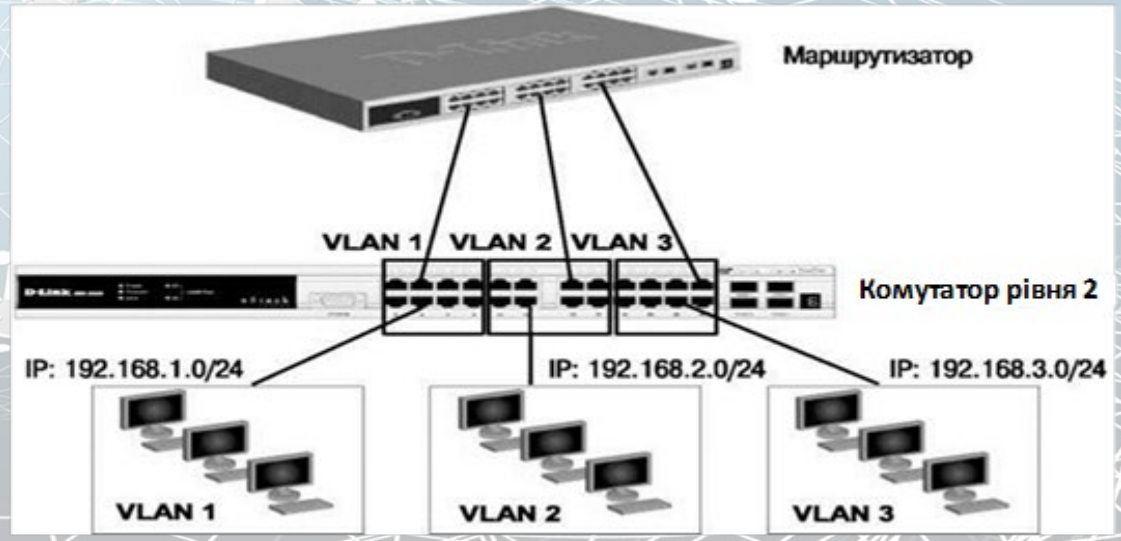
Технології побудови віртуальних локальних мереж (VLAN) (2)

У комутаторах можуть бути реалізовані наступні типи VLAN:

- на основі портів;
- на основі стандарту IEEE 802.1Q;
- на основі стандарту IEEE 802.1ad (Q-in-Q VLAN);
- на основі портів і протоколів IEEE 802.1v;
- на основі MAC-адрес;
- асиметричні.

При використанні VLAN на основі портів (port-based VLAN) кожен порт призначається в певну VLAN, незалежно від того, який користувач або комп'ютер підключений до цього порту (рисунки). Це означає, що усі користувачі, підключені до цього порту, будуть членами однієї VLAN. Конфігурація портів статична і може бути змінена тільки вручну.



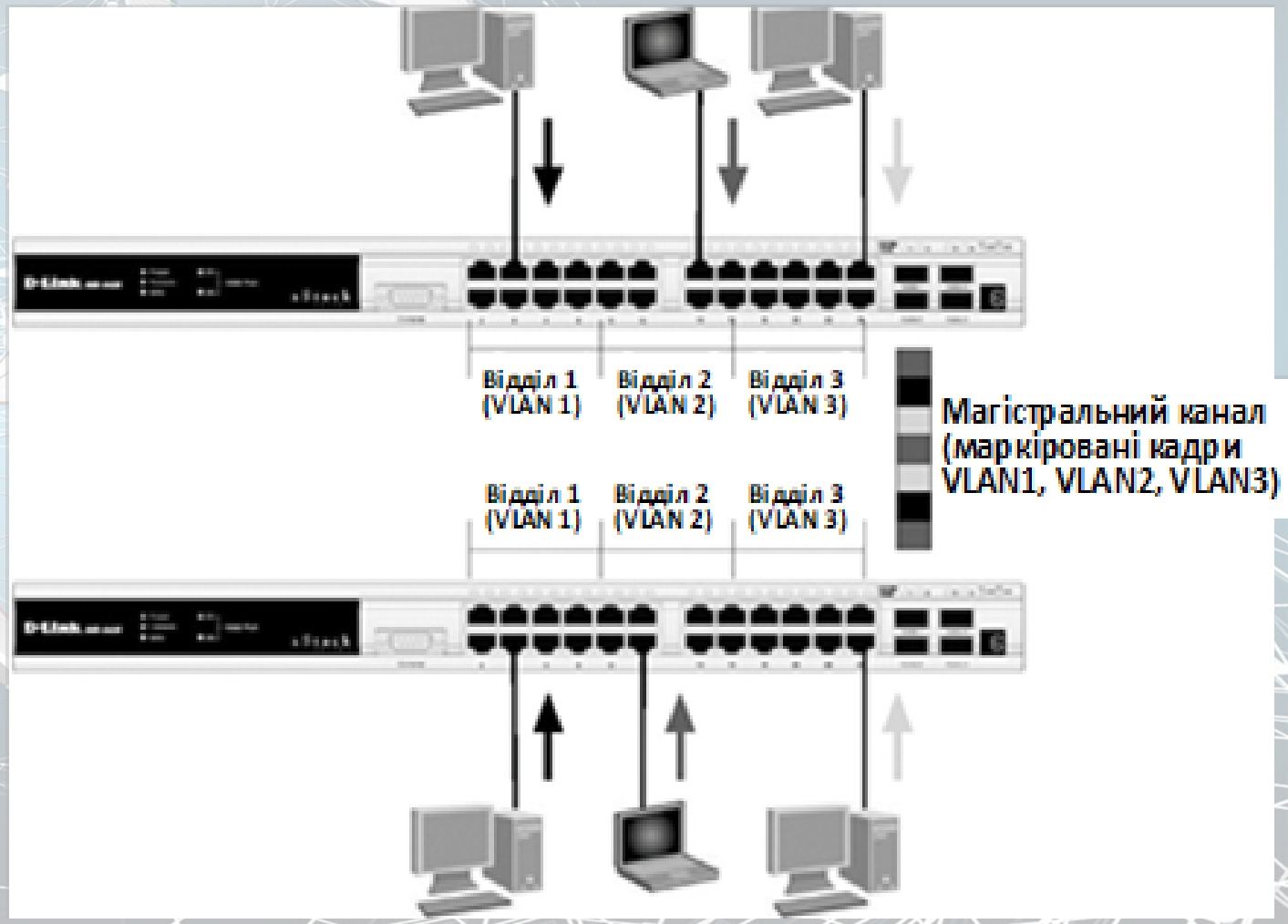


Технології побудови віртуальних локальних мереж (VLAN) (3)

Розв’язати проблему комунікатора портів можна двома способами: використати комутатори, які на основі фірмового рішення дозволяють включати порт декілька VLAN, або використати комутатори рівня 3 (рис.).

Переваги VLAN стандарту IEEE 802.1Q

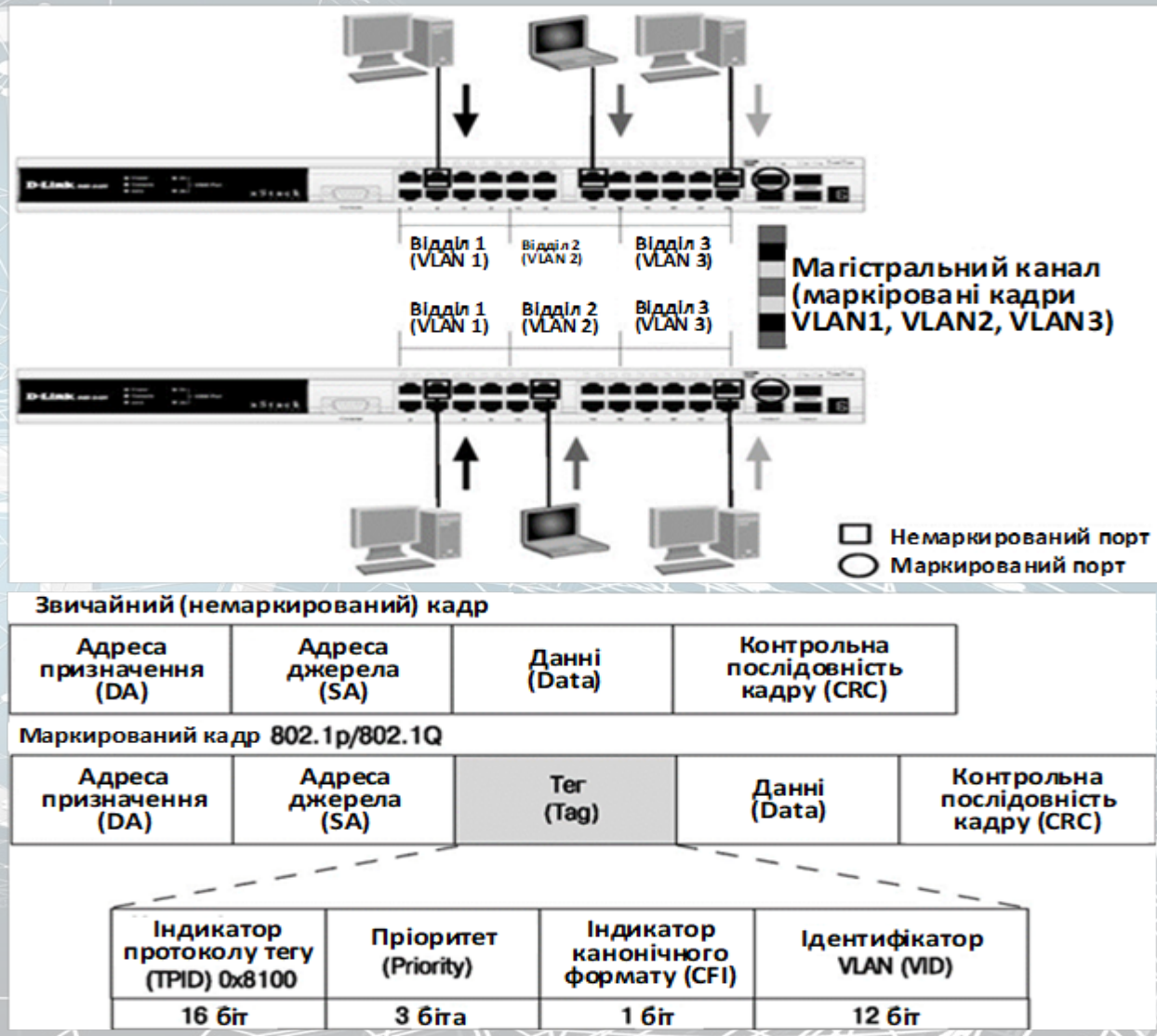
- гнучкість і зручність в налаштуванні
- дозволяє активізувати алгоритм єднального дерева (Spanning Tree)
- здатність VLAN IEEE 802.1Q додавати і витягати теги із заголовків кадрів
- облаштування різних виробників, що підтримують стандарт
- зв’язати підмережі на мережевому рівні, потрібний маршрутизатор або комутатор L3



Особливості реалізації VLAN стандарту 802.1Q (1)

Стандарт IEEE 802.1Q визначає зміни в структурі кадру Ethernet, що дозволяють передавати інформацію про VLAN по мережі. На рис. зображені маркіровані і немаркіровані порти VLAN і формат тегу 802.1Q VLAN.

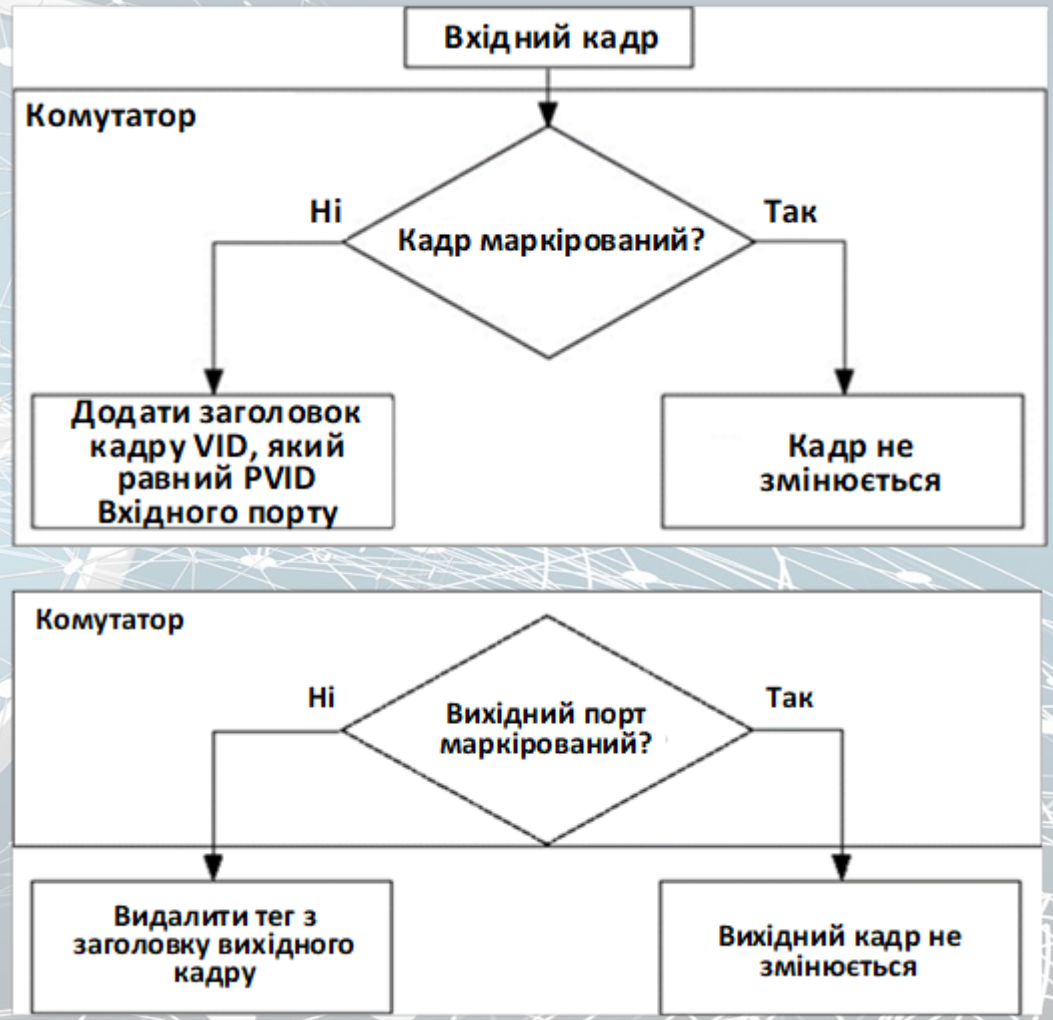
Кожен фізичний порт комутатора має параметр, що називається ідентифікатор порту VLAN (PVID). Цей параметр використовується для того, щоб визначити, в яку VLAN комутатор направить немаркований кадр, що входить, з підключеного до порту сегменту, коли кадр треба передати на інший порт (усередині комутатора в заголовки усіх немаркованих кадрів додається ідентифікатор VID, рівний PVID порту, на який вони були прийняті). Цей механізм дозволяє одночасно існувати в одній мережі пристроям з підтримкою і без підтримки стандарту IEEE 802.1Q.



Особливості реалізації VLAN стандарту 802.1Q (2)

Правила вхідного трафіку (рис. зверху) виконують класифікацію кожного отримуваного кадру відносно приналежності до певній VLAN, а також можуть служити для ухвалення рішення про прийом кадру для подальшої обробки або його відкидання на основі формату прийнятого кадру.

Правила вихідного трафіку (рис. знизу) визначають формат витікаючого кадру – маркований або немаркований. Якщо вихідний порт є немаркованим (untagged), то він витягатиме тег 802.1Q із заголовків усіх маркірованих кадрів, що виходять через нього. Якщо вихідний порт налагоджений як маркований (tagged), то він зберігатиме тег 802.1Q в заголовках усіх маркірованих кадрів, що виходять через нього.

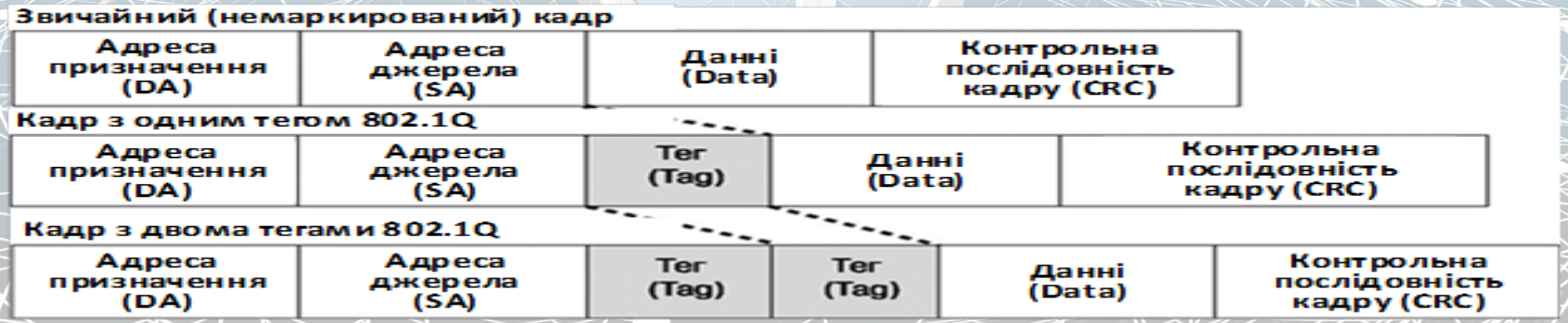


Реалізації VLAN з розширеннями стандарту IEEE 802.1Q

Функція Q-in-Q, також відома як DoubleVLAN, відповідає стандарту IEEE 802.1ad, який є розширенням стандарту IEEE 802.1Q. Вона дозволяє додавати в маркіровані кадри Ethernet другий тег IEEE 802.1Q.

На рис. зображені формати звичайного кадру Ethernet, кадру Ethernet з тегом 802.1Q, кадру Ethernet з двома тегами 802.1Q.

Інкапсуляція кадру Ethernet другим тегом відбувається таким чином: тег, що містить ідентифікатор VLAN мережі провайдера (зовнішній тег), вставляється перед внутрішнім тегом, що містить клієнтський ідентифікатор VLAN. Передача кадрів в мережі провайдера здійснюється тільки на основі зовнішнього тега SP- VLAN ID, внутрішній тег користувацької мережі CVLAN ID при цьому прихований.



Особливості реалізації статичних і динамічних VLAN

Існують два основні способи, що дозволяють встановлювати членство в VLAN: статичні VLAN і динамічні VLAN.

У статичних VLAN встановлення членства здійснюється вручну адміністратором мережі. При зміні топології мережі або переміщенні користувача на інше робоче місце адміністраторові вимагається вручну виконувати прив'язку VLANпорт для кожного нового з'єднання.

Членство в динамічних VLAN може встановлюватися динамічно на магістральних інтерфейсах комутаторів на основі протоколу GVRP (GARP VLAN Registration Protocol). Протокол GARP (Generic Attribute Registration Protocol) використовується для реєстрації і відміни рєстрації атрибутів, таких як VID.

Статичні записи про реєстрацію в VLAN (Static VLAN Registration Entries) використовуються для уявлення інформації про статичних VLAN у базі даних фільтрації. Ці записи дозволяють задавати точні налаштування для кожного порту VLAN: ідентифікатор VLAN, тип порту (маркований або немаркований), один з елементів протоколу GVRP, що управляють:

– fixed (порт завжди є членом цією VLAN);

– forbidden (порту заборонено реєструватися як членові цією VLAN);

– normal (звичайна реєстрація за допомогою протоколу GVRP).

Елементи GVRP, що управляють, використовуються для активізації роботи протоколу на портах комутатора, а також для вказівки тієї, чи може ця VLAN бути зареєстрована на порту.

Динамічні записи про реєстрацію в VLAN (Dynamic VLAN Registration Entries) використовуються для уявлення у базі даних фільтрації інформації про порти, членство в VLAN яких встановлено динамічно. Ці записи створюються, оновлюються і віддаляються в процесі роботи протоколу GVRP.

Запитання для самоконтролю

1. Керування сеансами TCP. Протокол UDP.
2. Варіанти застосування функції контролю підключення вузлів до портів комутатора.
3. Забезпечення безпеки на канальному рівні моделі OSI.
4. Механізми доступу до середовища та фреймування.
5. Забезпечення безпеки на рівні додатків моделі OSI.
6. Служби рівня додатків моделі OSI.
7. Забезпечення безпеки на мережному рівні моделі OSI.
8. Протоколи мережного рівня IPVN.
9. Маршрутизація на мережному рівні моделі OSI.
10. Особливості управління багатоадресною розсилкою на 2-му рівні моделі OSI (IGMP Snooping).
11. Планування захищеної мережі.
12. Організація захищеного підключення.
13. Особливості реалізації статичних і динамічних VLAN.
14. Методика створення списків управління доступом (ACL).
15. Призначення і зміст списків управління доступом.
16. Типи профілів доступу.
17. Процес створення профілю доступу.
18. Приклади налаштування ACL.
19. Варіанти списків реалізації управління доступом (ACL).
20. Основні команди комутаторів.

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ІНТЕРНЕТ

Найбільш поширені сервіси

Сервіс	Протокол	Послуги захисту інформації	Системи захисту
Електронна пошта	SMTP – основний протокол передачі пошти, використовується для прийому і передачі електронної пошти	Автентифікація, конфіденційність даних. Керування доступом. Цілісність даних. Причетність	PGP, S/MIME Брандмауер
Система віддаленого доступу	TELNET – використовується для підключення до віддалених систем, приєднаних до мережі, застосовує базові можливості по емуляції термінала	Автентифікація. Конфіденційність да- них. Керування доступом. Цілісність даних. Причетність	SOCS, Бранд-мауер
Міжсистем-ний файло-вий обмін	FTP – протокол передачі файлів, використовується для прийому або передачі файлів між системами в мережі	Автентифікація, конфіденційність даних. Керування доступом. Цілісність даних. Причетність	SSL/TLS, SOCS, Брандмауер
Служба мережевих імен	DNS – використовується TELNET, FTP і іншими сервісами для трансляції імен хостів на IP адреси	Автентифікація. Конфіденційність даних. Керування доступом. Цілісність даних. Причетність	Брандмауер

gopher	Засіб пошуку і перегляду інформації за допомогою системи меню, яке може забезпечити дружній інтерфейс до інших інформаційних сервісів
WAIS	Глобальний інформаційний сервіс, використовується для індексування і пошуку в базах даних файлів
WWW/http	Всесвітня павутина, об'єднання FTP, gopher, WAIS і інших інформаційних сервісів, що використовує протокол передачі гіпертексту (http), і програми Netscape, Microsoft Internet Explorer і Mosaic як клієнтські програми
NFS	Мережева файлова система, дозволяє системам спільно використовувати директорії й диски, при цьому видалена директорія або диск здаються такими, що знаходяться на локальній машині
NIS	Мережеві інформаційні сервіси, дозволяють декільком системам спільно використовувати бази даних, наприклад файл паролів, для централізованого керування ними
Система X Windows	Графічна віконна середа і набір прикладних бібліотек, використовуваних на робочих станціях
rlogin, rsh та інші r-сервіси	Реалізують концепцію хостів, які довіряють один одному, дозволяючи виконувати команди на інших комп'ютерах, не вводячи пароль

Використання засобів безпеки для захисту сервісів

Сервіс	Ідентифікація і автентифікація	Керування доступом	Брандмауер	Засоби контролю програм, що імпортуються	Шифрування	Архітектура	Комерційне усунення наслідків інцидентів	Організаційні заходи
Віддалений доступ	X	X	X		X			X
Електронна пошта	X			X	X			X
Публікація інформації		X	X			X		X
Дослідження		X	X	X		X		X
Електронна комерція	X	X	X	X	X	X	X	X
Постійна доступність						X		X
Легкість використання						X		X

- Віддалений доступ до сервісу
- Віддалене керування
- Методи забезпечення безпеки за мережним, телефонним з'єднання включають:
  - обмеження кола осіб, які знають номери телефонів, до яких підключені модеми
  - використання пар ім'я-пароль
  - методи посиленої автентифікації:
    - модеми із зворотним дзвінком
    - одноразові паролі
    - автентифікація на основі місцезнаходження віддаленого користувача

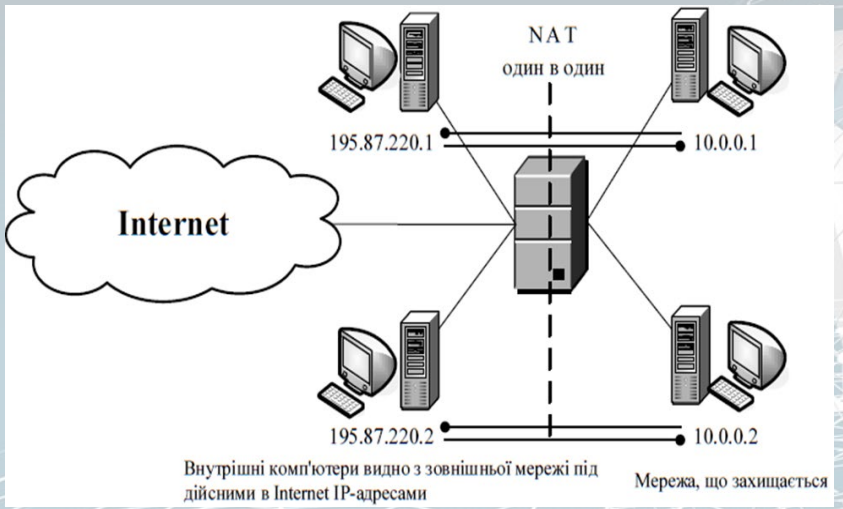
Основні засоби Інтернет

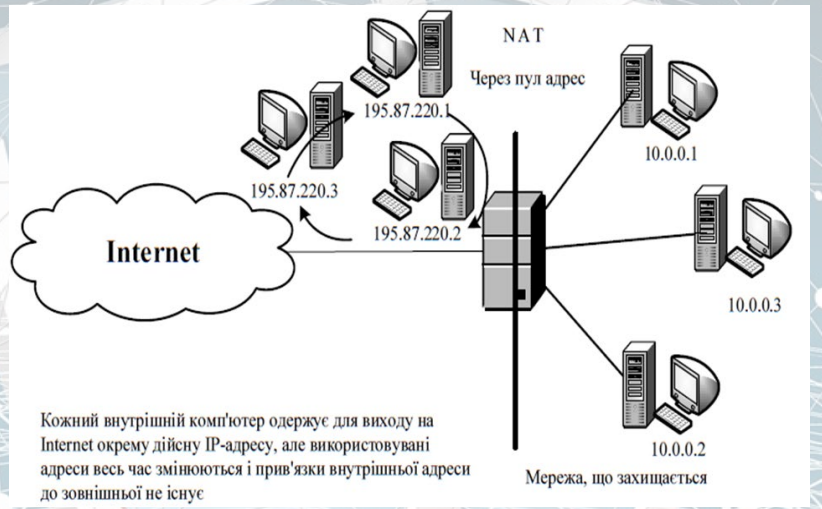
- Всесвітня павутина (WWW).
- Електронна пошта.
- Види електронної комерції
  - продаж інформації
  - концепція "електронних магазинів«
  - електронні банки
- Електронний обмін даними (EDI)
- Інформаційні транзакції
  - Статичні дані: історична інформація, карти і т. ін.
  - Корпоративна інформація: телефонні номери, адреси, структура організації і т. ін.
  - Інформація про продукцію або послуги.
  - Платна інформація: новини, періодичні видання, доступ до баз даних і т. ін.
- Електронний переклад фондів (EFT)

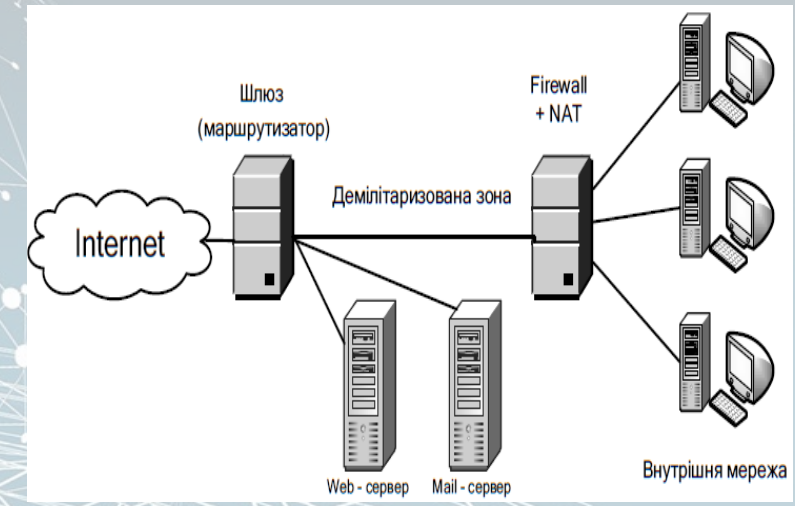
Основни способами задоволення вимог постійної доступності

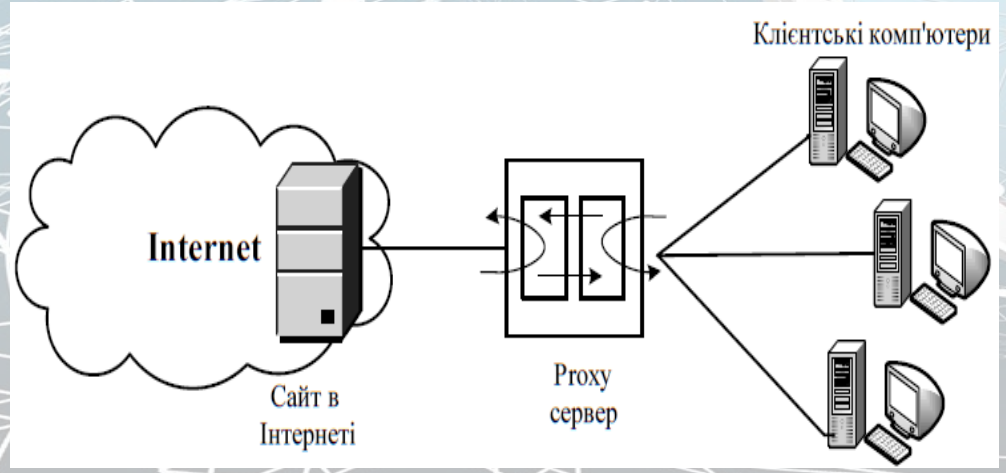
- Планування ресурсів. Помічено цікавий феномен – як тільки брандмауер встановлено, користувачі починають скаржитися, що з'єднання з Інтернетом стало повільнішим.
- Надмірність – для всіх організацій, окрім тих, що мають низький рівень ризику, необхідний резервний брандмауер у гарячому резерві.
- Відновлення – коли блок, що вийшов з ладу, відновлено, потрібно здійснити ретельний контроль його конфігурації.
- Легкість використання. Склад користувачів багатьох систем, підключених до Інтернету, може бути вельми різноманітним – від секретарів до вчених, від новачків до досвідчених користувачів.
- Одноразова реєстрація. Для виконання повсякденних завдань користувачу може знадобитися реєстрація на великому числі комп'ютерів і мереж.
- Розробка призначеного для користувача інтерфейсу. Розробка призначеного для користувача інтерфейсу для засобів забезпечення безпеки в Інтернеті повинна бути узгоджена з інтерфейсом інших додатків, які регулярно використовуються користувачами.

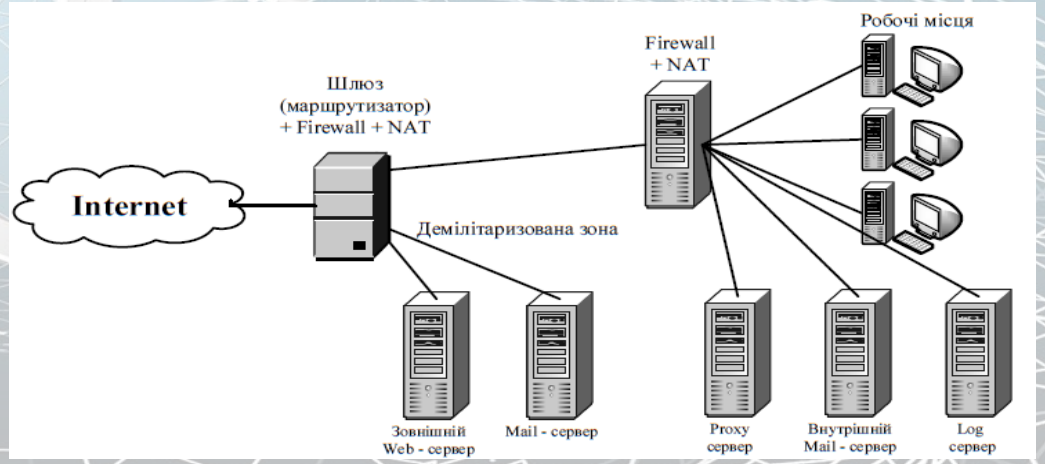
Основні принципи забезпечення безпеки в мережі Інтернет, захист за допомогою брандмауерів.







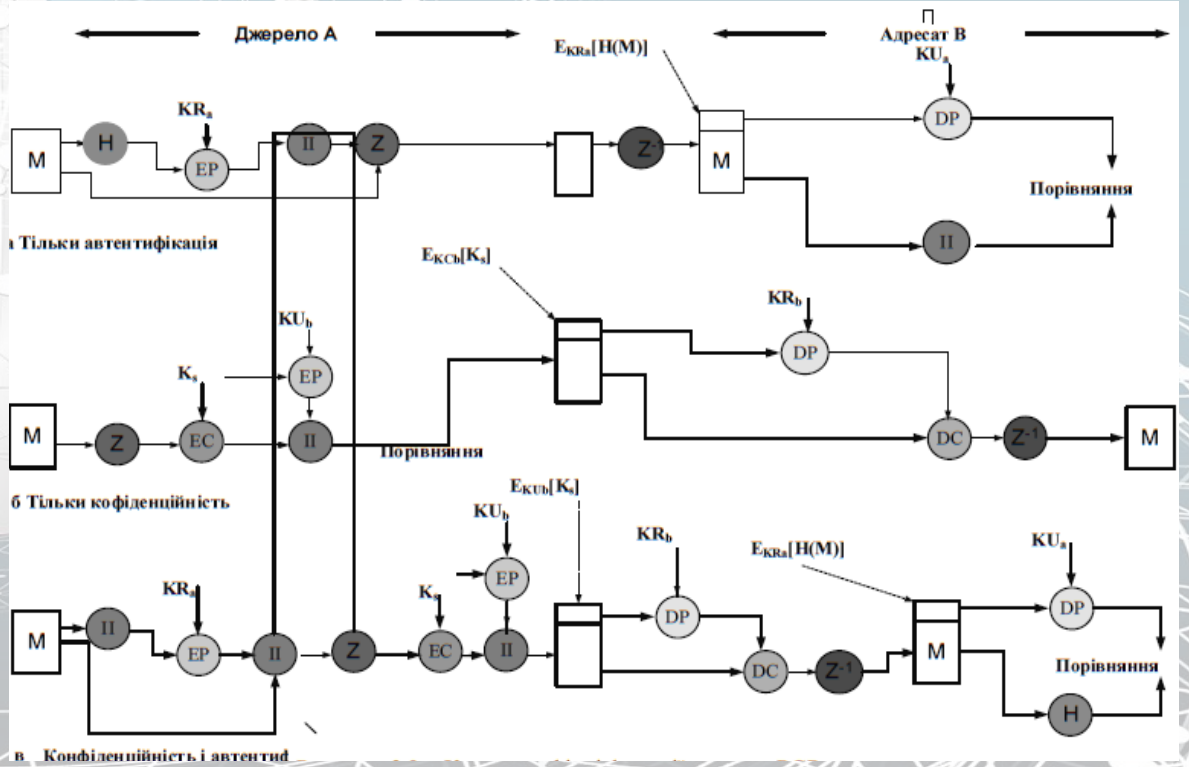




Захист електронної пошти. Система PGP

Система PGP (Pretty Good Privacy – цілком надійна секретність), що є плодом зусиль однієї людини – Філа Циммермана (Phil Zimmermann), забезпечує конфіденційність і сервіс автентифікації, які можна використовувати для електронної пошти і додатків зберігання файлів.

Функція	Використовувані алгоритми	Опис
Цифровий підпис	DSS/SHA або RSA/SHA	За допомогою SHA-1 створюєтьсяхеш-код повідомлення. Одержаний таким чином профіль повідомлення шифрується за допомогою DSS або RSA з використанням особистого ключа відправника і включається до повідомлення
Шифрування повідомлення	CAST, IDEA, AES або потрійний DES з трьома ключами і алгоритмом Діфі-Хелмана, RSA	Повідомлення шифрується за допомогою CAST-128 або IDEA, або 3DES з одноразовим сеансовим ключем, відправником, що генерується. Сеансовий ключ шифрується за допомогою алгоритму Діфі-Хелмана або RSA з використанням відкритого ключа одержувача і включається до повідомлення
Стиснення	ZIP	Повідомлення можна стиснути для зберігання або передачі, використовуючи ZIP
Сумісність на рівні електронної пошти	Перетворення у формат radix-64	Щоб забезпечити прозорість для всіх додатків електронної пошти, шифроване повідомлення можна перетворити на рядок ASCII, використовуючи перетворення у формат radix-64
Сегментація	—	Щоб задовольнити обмеження максимального розміру повідомлень, PGP виконує сегментацію і зворотну збірку повідомлення



Криптографічні перетворення типу ЕЦП мають задовольняти ряд вимог, основними з них є такі:

- алгоритми розробки і перевірки ЕЦП мають бути відкритими, тобто несекретними;
- алгоритми розробки і перевірки ЕЦП повинні мати не вище ніж поліноміальну складність;
- алгоритм побудування конфіденційного ключа і/чи підробки підпису повинний мати не нижче, ніж експонентну, тобто практично не реалізовану складність;
- ЕЦП має бути чутливою до будь-яких змін підписаних даних, тобто виявляти порушення цілісності;
- імовірність появи двох однакових підписів у різних повідомленнях не має перевищувати припустимого значення;
- обчислювальна складність вироблення і перевірки ЕЦП має бути мінімізована і мати близькі за величиною значення;
- забезпечувати захист від підміни, підробки й імітації повної ЕЦП із необхідною імовірністю;
- ЕЦП, отримані для однієї і тієї ж інформації в різний час і на різних пристроях мають відрізнятися з великою імовірністю;
- ключі вироблення ЕЦП мають бути конфіденційними, а ключі перевірки ЕЦП – відкритими;
- ЕЦП повинен мати максимальну стійкість до виявлення будь-яких змін, підробок і порушень;
- має існувати можливість прийняття ЕЦП із різними рівнями стійкості і складністю вироблення і перевірки ЕЦП;
- можливість програмної, апаратно-програмної й апаратної реалізації ЕЦП із приблизно однаковою складністю;
- можливість використання ЕЦП як з однаковими загальносистемними параметрами в мережі, так і індивідуальними для окремої частини об'єктів (суб'єктів);
- можливість багаторівневого вироблення і перевірки ЕЦП однієї і тієї ж інформації з використанням різних ключів і за необхідності різних загальносистемних параметрів;
- використаний ЕЦП має дозволяти проведення дослідних експериментів з метою забезпечення судового розгляду й арбітражу.
- має існувати можливість збереження ЕЦП як разом з інформацією, що захищається, так і окремо від неї.

Основні види атак на ЕЦП

- Атака на основі відомого відкритого ключа (key-only attack). Найслабкіша з атак, практично завжди доступна криптоаналітику (зловмиснику). Вона може виконуватися при апріорній визначеності криптоаналітика щодо реалізації ЕЦП, знанні загальносистемних параметрів, а також діючих відкритих ключах.
- Атака на основі відомих підписаних повідомлень (known-message attack). Для цієї атаки передбачається, що в розпорядженні криптоаналітика є деяке число пар (m, (r, s)) підписаних повідомлень m, при цьому він не може вибирати повідомлення m. Крім цього криптоаналітик знає систему і параметри ЕЦП.
- Проста атака з вибором підписаних повідомлень (generic chosen- message attack). У цьому випадку криптоаналітик має можливість вибрати деяку кількість підписаних повідомлень, знає загальносистемні параметри і має доступ до відкритих ключів після вибору підписаних повідомлень.
- Спрямована атака з вибором повідомлення (direct chosen-message attack). Криптоаналітик знає загальносистемні параметри, може за своїм розсудом вибирати відкритий ключ і після цього вибирати підписані повідомлення.
- Адаптивна атака з вибором підписаного повідомлення (adaptive chosen- message attack). При здійсненні атаки криптоаналітик може вибирати відкритий ключ, а також підписане повідомлення. При цьому вибір наступного підписаного повідомлення він може робити на основі знання припустимого підпису попереднього обраного повідомлення.

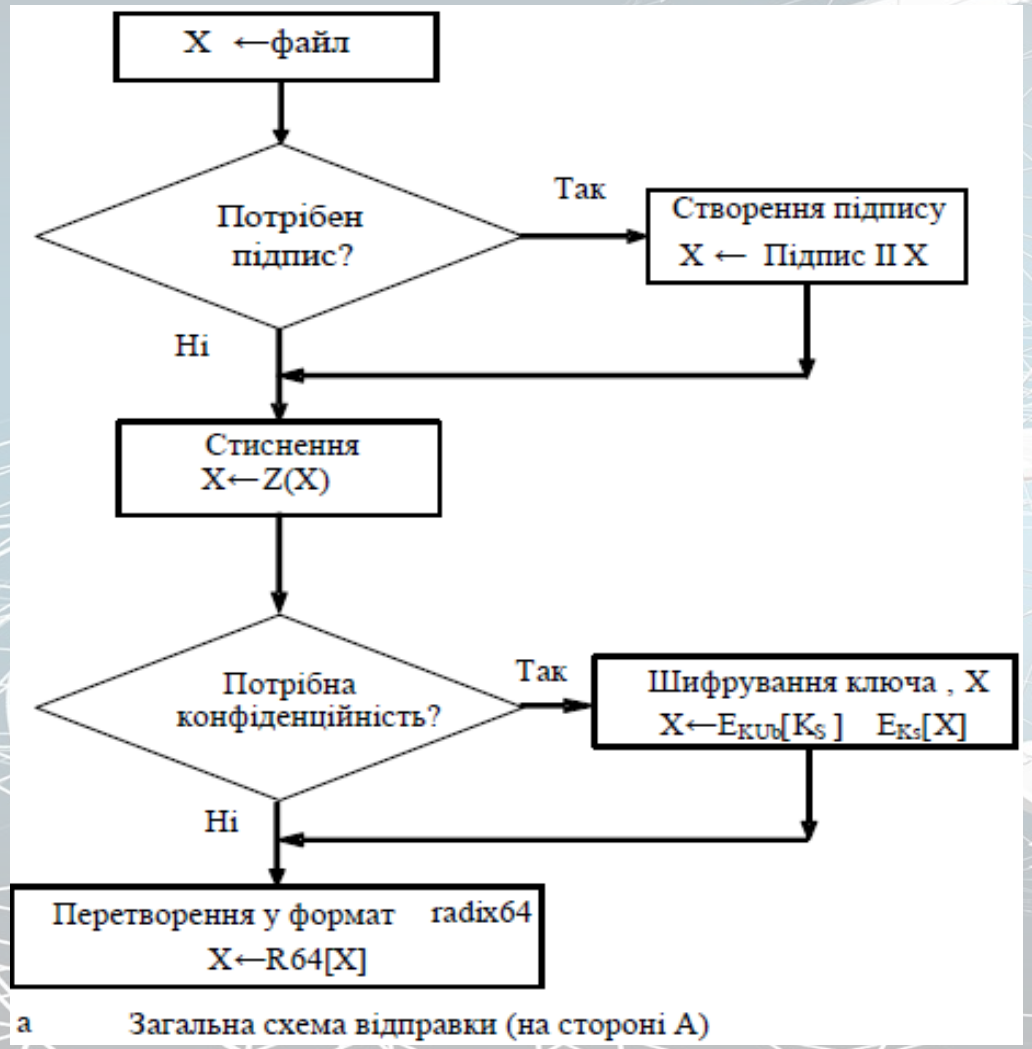
Види погроз, у порядку зростання небезпеки, для всіх схем електронних цифрових підписів

- Екзистенціальна підробка (existential forgery). Погроза полягає в створенні криптоаналітиком для будь-якого, можливо безглуздого повідомлення m′, що відрізняється від перехопленого, реального (правильного) ЕЦП.
- Селективна підробка (selective forgery). Являє загрозу створення для заздалегідь обраного повідомлення m правильного ЕЦП.
- Універсальна підробка (universal forgery). Ця погроза полягає у знаходженні криптоаналітиком алгоритму формування підпису, функціонально еквівалентному дійсному алгоритму ЕЦП, що дозволяє створити чи модифікувати дійсні підписані повідомлення.
- Повне розкриття (total break). При цій погрозі криптоаналітик може обчислити таємний ключ, можливо відмінний від d, але відповідний відкритому ключу Q. Це дозволяє криптоаналітику формувати цифрові підписи для будь- яких повідомлень і надалі нав'язувати ці повідомлення кореспондентам.

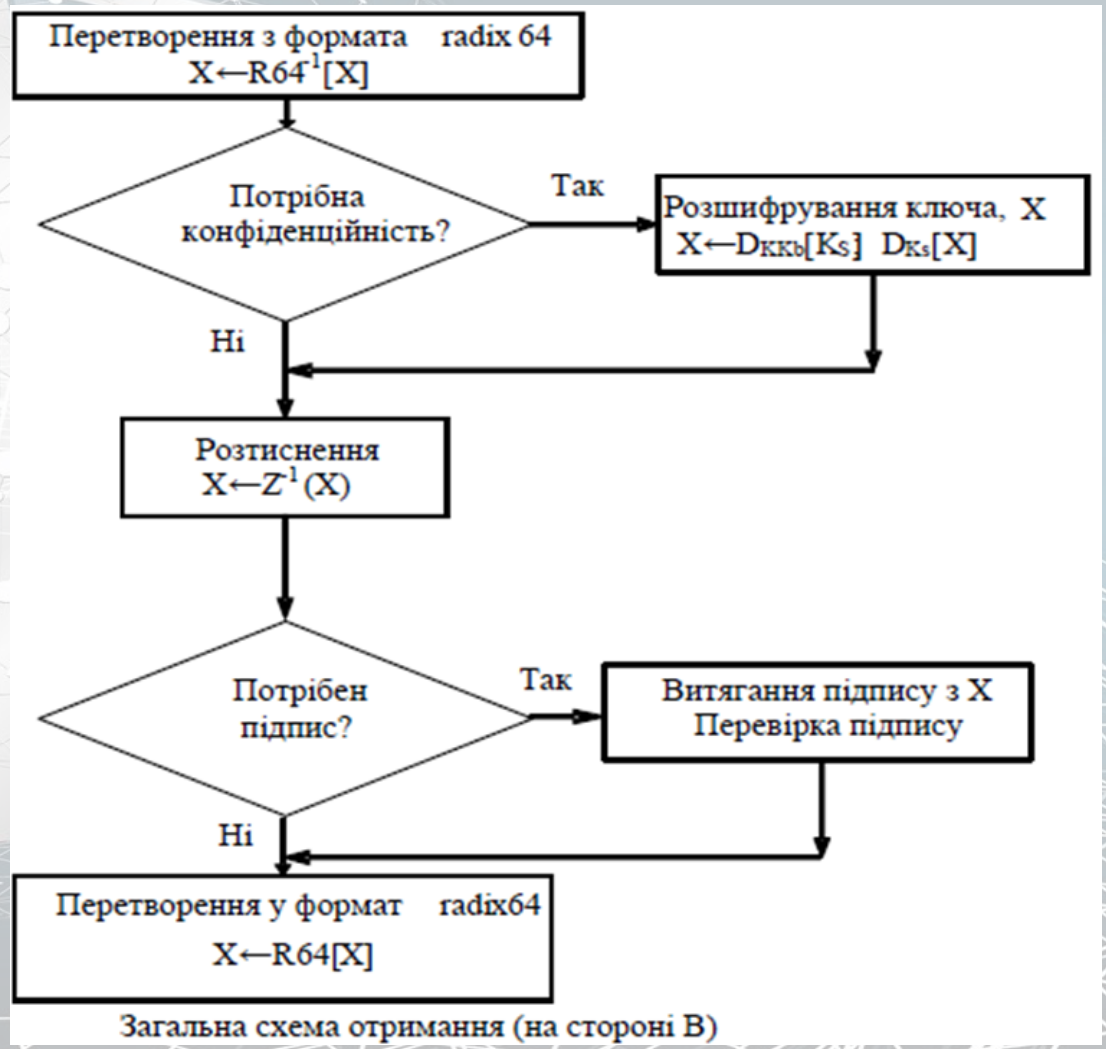
Захист ключа шифрування

- Відправник генерує повідомлення і випадкове 128-бітове число, яке виступає як сеансовий ключ тільки для цього повідомлення.
- Повідомлення шифрується за допомогою алгоритму CAST-128 (або IDEA, або 3DES) і даного сеансового ключа.
- Сеансовий ключ шифрується за допомогою алгоритму RSA і відкритого ключа одержувача і приєднується до початку повідомлення.
- Одержувач використовує RSA з особистим ключем, щоб розшифрувати і тим самим відновити сеансовий ключ.
- Сеансовий ключ застосовується для розшифрування повідомлення.

Відправлення і приймання повідомлень PGP



а Загальна схема відправки (на стороні А)



Загальна схема отримання (на стороні В)

Криптографічні ключі і зв'язки ключів

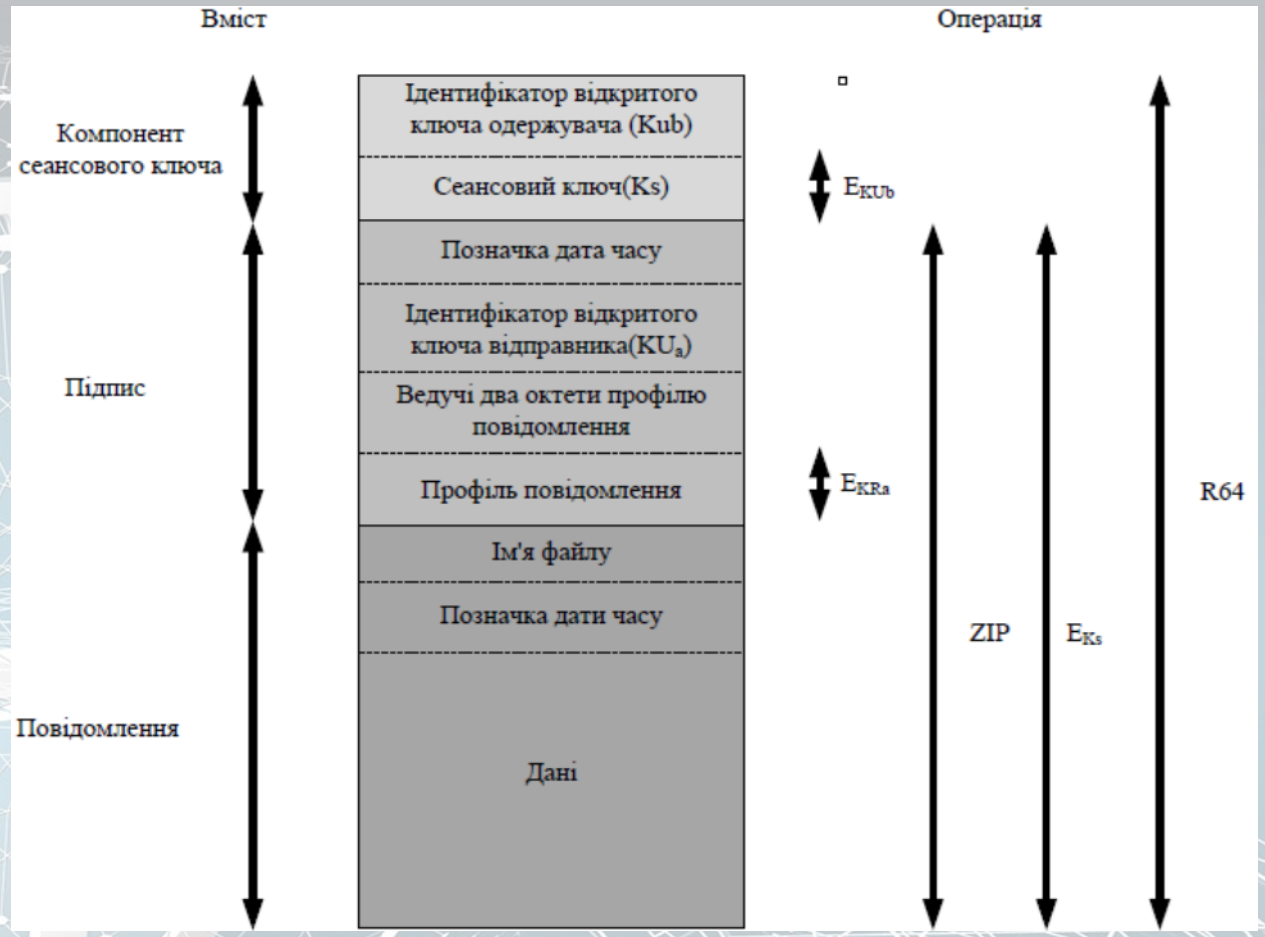
Система PGP використовує чотири типи ключів: одноразові сеансові ключі схеми традиційного шифрування, відкриті ключі, особисті ключі і парольні ключі схеми традиційного шифрування, описані нижче. Відносно цих ключів можна сформулювати такі три вимоги.

- 1. Наявність засобів генерування непередбачуваних сеансових ключів.
- 2. Наявність у користувача декількох пар відкритих/особистих ключів. Однією з причин такої вимоги є те, що користувач може час від часу міняти пару ключів. У результаті всі повідомлення на шляху проходження виявляться створеними зі старим ключем. До того ж одержувачі знатимуть тільки старий відкритий ключ, доки ними не буде одержано нову версію ключа.
- 3. На додаток до необхідності час від часу міняти ключі користувач може мати декілька пар ключів одночасно, щоб взаємодіяти з різними групами одержувачів або просто для того, щоб підсилити захист, обмежуючи обсяг матеріалу, що шифрується одним і тим же ключем. У результаті однозначної відповідності між користувачами і їх відкритими ключами немає.

Генерування сеансових ключів

Кожен сеансовий ключ зв'язується з одним повідомленням і використовується тільки для шифрування і розшифрування цього повідомлення.

Випадкові 128-бітові числа генеруються за допомогою самого алгоритму CAST-128. Введення для генератора випадкових чисел складається з 128- бітового ключа і двох 64-бітових блоків, які розглядаються як відкритий текст, що підлягає шифруванню. Використовуючи режим шифрованого зворотного зв'язку, шифрувальник CAST-128 породжує два 64-бітові блоки шифрованого тексту, які зв'язуються конкатенацією, внаслідок чого формується 128-бітовий сеансовий ключ. Алгоритм, який при цьому використовується, засновано на алгоритмі, описаному в документі ANSI X12.17.



EKUb – шифрування з використанням особистого ключа для користувача B;
EKRa – шифрування з використанням відкритого ключа для користувача A;
EKs – шифрування з використанням сеансового ключа;
ZIP – функція стиснення ZIP;
R64 – функція перетворення на формат radix 64.

Загальний формат повідомлення PGP (від A до B)

Інші вимоги до алгортму

- Ідентифікатор ключа потрібен і для цифрового підпису PGP. Через те що відправник може скористатися одним з декількох особистих ключів для шифрування профілю повідомлення, одержувач повинен знати, який відкритий ключ йому слід використовувати. Тому розділ цифрового підпису повідомлення включає 64-бітовий ідентифікатор відповідного відкритого ключа. При отриманні повідомлення одержувач перевіряє, що ідентифікатор відповідає відомому йому, відкритому ключу відправника, а потім продовжує перевірку підпису.
- Позначка дати-часу. Час створення підпису.
- Профіль повідомлення. 160-бітовий профіль повідомлення, створений за допомогою SHA-1 і шифрований з використанням особистого ключа підпису відправника. Профіль обчислюється для позначки дати-часу підпису, зв'язаної конкатенацією з порцією даних компонента повідомлення. Включення указівника дати-часу підпису в профіль забезпечує захист від атак відтворення повідомлення. Виключення імені файлу і позначки дати-часу компонента повідомлення гарантує, що відокремлений підпис буде точно збігатися з підписом, що додається в префікс повідомлення. Відокремлені підписи обчислюються для файлу, в якому немає ніяких полів заголовка (хедера) повідомлення.
- Позначка дати-часу. Дата і час створення даної пари ключів.
- Ідентифікатор ключа. Молодші 64 розряди відкритого ключа даного рядка.
- Відкритий ключ. Відкритий ключ даної пари.
- Особистий ключ. Особистий ключ даної пари; це поле шифрується
- – поле, використане для індексації таблиці
- Ідентифікатор користувача. Зазвичай тут розміщується адреса електронної пошти користувача (наприклад, ssemenov@ukr.net). Проте користувач може вказати для кожної пари ключів різні імена (наприклад, Semenov, SSemenov, SergSemenov і т.п.) або використовувати один ідентифікатор користувача кілька разів.

Загальна структура зв'язки особистих ключів

Зв'язку можна вважати таблицею, в якій кожен рядок являє одну пару відкритого/особистого ключів, що належать даному користувачу.

Загальна структура зв'язки відкритих ключів (рис.) дозволяє зберігати відкриті ключі інших користувачів, відомих даному.

Поля:

- Позначка дати-часу. Дата і час створення даного запису.
- Ідентифікатор ключа. Молодші 64 розряди відкритого ключа даного запису.
- Відкритий ключ. Відкритий ключ даного запису.
- Ідентифікатор користувача. Власник даного ключа. З одним відкритим ключем можна пов'язати декілька ідентифікаторів користувача.
- Спочатку розглянемо передачу повідомл

Кільце відкритих ключів

Позначка дати-часу	Ідентифікатор ключа*	Відкритий ключ	Довіра власнику
• • •	• • •	• • •	• • •
T_i	$KU_i \bmod 2^{64}$	KU_i	$trust_flag_i$
• • •	• • •	• • •	• • •

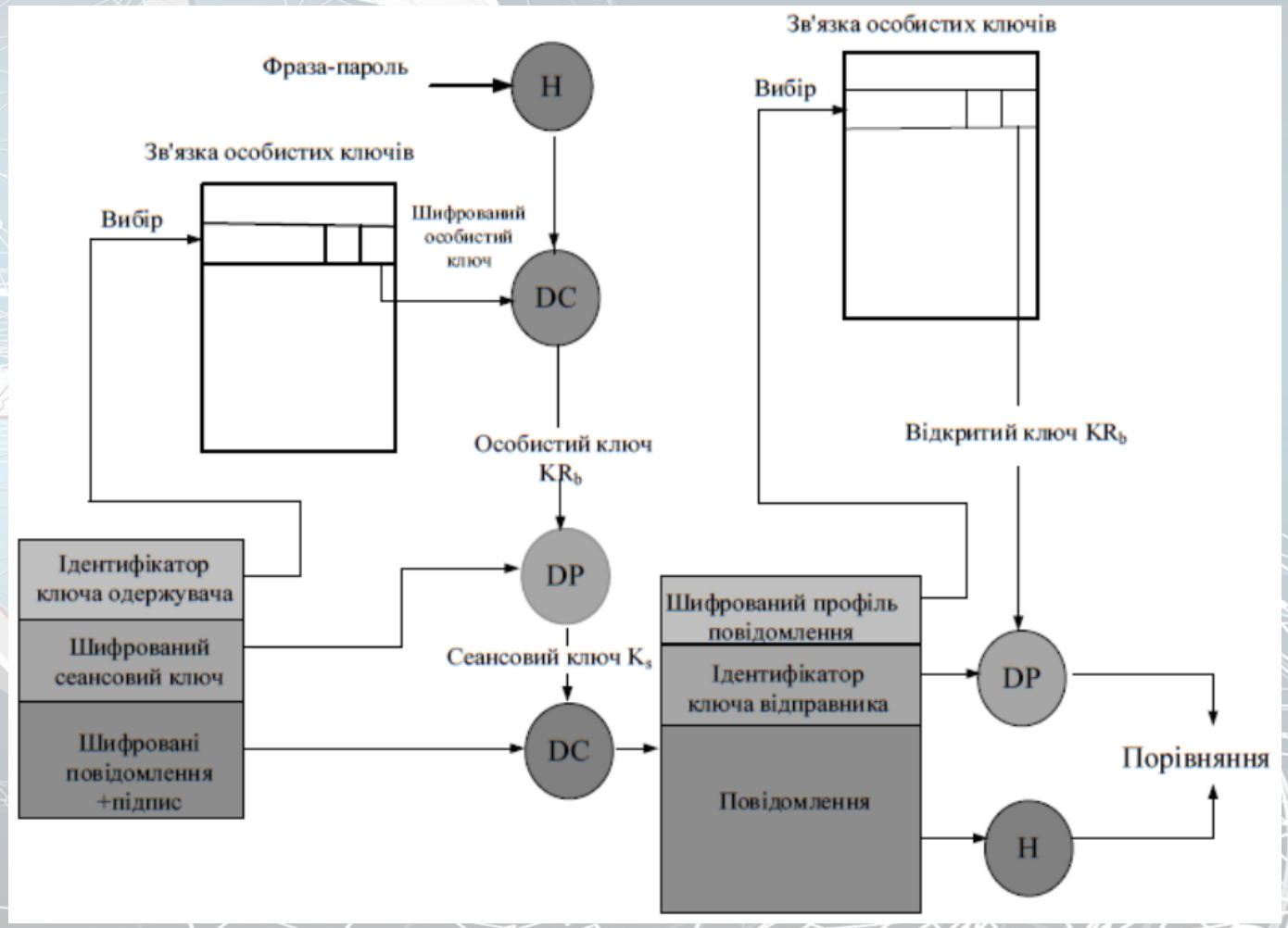
Кільце особистих ключів

Позначка дати-часу	Ідентифікатор ключа*	Відкритий ключ	Шифрований особистий ключ	Ідентифікатор користувача*
• • •	• • •	• • •	• • •	• • •
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(Pi)}[KR_i]$	Користувачі
• • •	• • •	• • •	• • •	• • •

Ідентифікатор користувача*	Законність ключа	Підпис (підписи)	Довіра підпису (підписам)
• • •	• • •	• • •	• • •
Користувач i	$trust_flag_i$		
• • •	• • •	• • •	• • •

Передача повідомлення

- Позначка дати-часу. Дата і час створення даного запису.
- Ідентифікатор ключа. Молодші 64 розряди відкритого ключа даного запису.
- Відкритий ключ. Відкритий ключ даного запису.
- Ідентифікатор користувача. Власник даного ключа. З одним відкритим ключем можна пов'язати декілька ідентифікаторів користувача.
- Спочатку розглянемо передачу повідомлення (рис.) і припустимо, що повідомлення повинне бути підписано і зашифровано. Джерело повідомлення PGP виконує такі кроки.
- • Створення підпису повідомлення
- • Шифрування повідомлення
- • Розшифрування повідомлення
- • Автентифікація повідомлення
- • Керування відкритими ключами



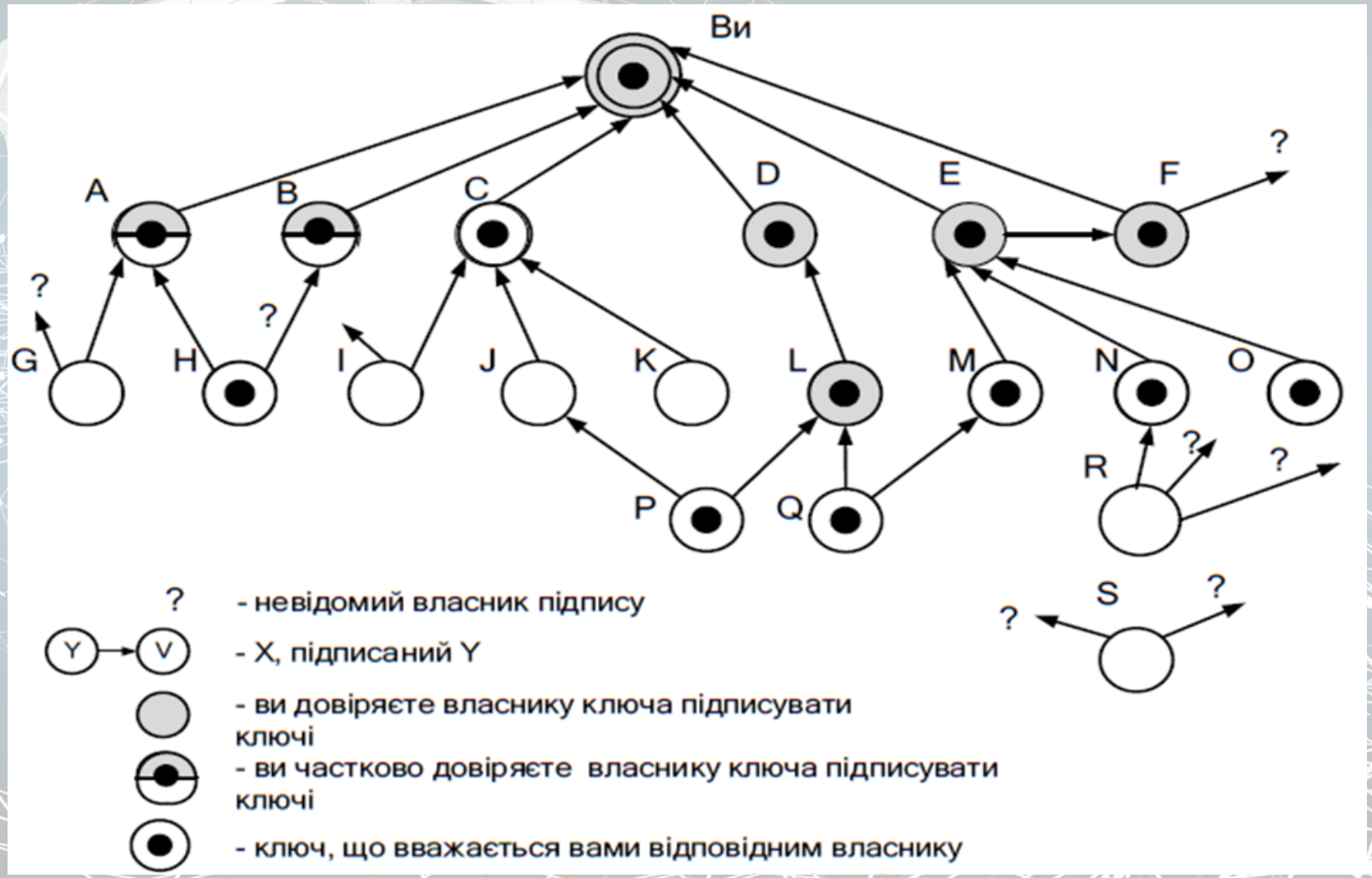
Мінімізація ризику отримання помилкових відкритих ключів

Для мінімізації ризику того, що зв'язка відкритих ключів користувача містить помилкові відкриті ключі, можливо запропонувати декілька варіантів дій. Припустимо, що А потрібно одержати надійний відкритий ключ В. Пропонується декілька варіантів процедури, які при цьому можна було б використовувати.

- Отримання ключа від В особисто (фізично).
- Перевірка ключа по телефону.
- Отримання відкритого ключа В від того, що викликає довіру обом сторонам надійного посередника D.
- Отримання відкритого ключа В від надійного уповноваженого вузла сертифікації.

Приклад моделі довіри PGP

- показано зразкову схему скріплення довіри підпису і відповідності ключа й відображено структуру зв'язки відкритих ключів. У даному випадку користувач одержав декілька відкритих ключів: частину безпосередньо від їх власників, а решту від третьої сторони, наприклад, з сервера ключів.



Захист електронної пошти. Система S/MIME

Документ RFC 822 визначає формат текстових повідомлень, які пересилаються електронною поштою.

Загальна структура повідомлення відповідного стандарту RFC 822 дуже проста. Повідомлення формується з певного числа рядків заголовка, за яким йде текст необмеженої довжини (тіло повідомлення). Заголовок повідомлення відокремлюється від тіла повідомлення порожнім рядком. Іншими словами, повідомлення є потоком тексту ASCII, де всі рядки до першого порожнього рядка вважаються рядками заголовка, що використовуються частиною агента користувача поштової системи. Рядок заголовка зазвичай складається з ключового слова, що завершується двокрапкою, за якою йдуть ключові параметри, причому довгі рядки формат дозволяє розбивати на кілька рядків. Найчастіше використовуються такі ключові слова, як From (Від), To (До), Subject (Тема) і Date (Дата). Ось приклад повідомлення.

Date: Tue, 16 Jan 2023 10:37:17(EST)

From: "SSemJohn" ss@ukr.net

Subject: Синтаксис RFC 822

To: Sarja@email.ua

c: Irina@rent.ua

Багатоцільові розширення електронної пошти. Стандарт MIME

Стандарт MIME є розширенням базового стандарту RFC 822, покликаним розв’язати деякі проблеми і подолати обмеження протоколу SMTP (Simple Mail Transfer Protocol – простий протокол передачі пошти) або деякого іншого протоколу передачі пошти і RFC 822. Відомий наступний список обмежень схеми SMTP/822.

SMTP не дозволяє передавати виконувані файли й інші об'єкти в двійковому форматі.

SMTP не дозволяє передавати текстові дані, що включають символи національних мов, оскільки такі символи подаються 8-бітовими кодами з десятковими значеннями від 128 і вище, а SMTP обмежує можливості передачі даних 7-бітовими кодами ASCII.

Сервери SMTP можуть відкинути електронне повідомлення, що перевищує певні розміри.

Шлюзи SMTP, що виконують трансляцію кодів ASCII в коди EBCDIC і назад, можуть мати різні таблиці перекладу, що виливається в проблеми трансляції.

Шлюзи SMTP, пов'язані з мережами електронної пошти, які використовують протокол X.400, не можуть обробити нетекстові дані, що включаються в повідомлення стандарту X.400.

Технічні специфікації MIME включають такі елементи.

- MIME-Version (версія MIME). Відповідний параметр повинен мати значення 1.0. Це поле указує, що повідомлення відповідає стандартам RFC 2045 і 2046.
- Content-Type (тип вмісту). Описує дані, поміщені в тіло повідомлення, достатньо детально для того, щоб агент одержувача зміг вибрати відповідний агент або механізм, що дозволяє надати одержані дані користувачу або обробити їх якимсь іншим відповідним чином.
- Content-Transfer-Encoding (кодування переданого вмісту). Указує тип перетворення, що використалося для того, щоб подати тіло повідомлення у вигляді, прийнятному для пересилання поштою.
- Content-ID) (ідентифікатор вмісту). Служить для того, щоб унікальним чином ідентифікувати об'єкти MIME серед множини контекстів.
- Content-Description (опис вмісту). Текстовий опис об'єкта у вмісті повідомлення; корисно тоді, коли об'єкт має форму, недоступну для прочитання (наприклад, звукові дані).

Типи вмісту MIME

Тип	Підтип	Опис
Text (текст)	Plain (простий) Enriched (розширений)	Неформатований текст; може бути в кодуванні ASCII або ISO 8859 Забезпечує велику гнучкість формату
Multipart (багатоком-понентний)	Mixed (змішаний)	Різні частини незалежні, але повинні передаватися разом. Вони повинні бути подані одержувачу в тому порядку, в якому вони з'являються в поштовому повідомленні Відрізняється від змішаного тільки тим, що не визначається порядок, в якому частини повідомлення повинні бути подані одержувачу
	Parallel (паралельний)	Різні частини є альтернативними варіантами однієї і тієї ж інформації. Вони розташовуються у порядку зростання точності відповідності оригіналу, і поштова система одержувача повинна вибрати для відображення користувачу "кращий" варіант
	Alternative (альтернативний) Digest (реферативний)	Подібний змішаному, але за умовчанням для поля тип/підтип кожної частини вибира- ється message/rfc822
Message (повідомлення)	rfc822 Partial (фрагментарний)	Тіло повідомлення саме є інкапсульованим повідомленням у форматі RFC 822 Служить для того, щоб вирішити фрагментацію великих поштових об'єктів деяким прозорим для одержувача способом
	External-body (зовнішний)	Містить указівник на об'єкт, що існує десь в іншому місці
Image (зображення)	Jpeg Gif	Зображення у форматі JPEG, кодування JFIF Зображення у форматі GIF
Video (відео)	Mpeg	Формат MPEG
Audio (звук)	Basic (основний)	Одноканальне 8-бітове кодування стандарту ISDN з частотою вибірки 8 КГц, виконано за законом компанування з мюхарактеристикою
Application (додаток)	PostScript Octet-stream (потік байтів)	Формат Adobe PostScript Двійкові дані загального вигляду, що складаються з 8-бітових байтів

Два методи кодування даних

Розмір	Методи кодування MIME
7bit	Усі дані подаються короткими рядками символів ASCII
8bit	Усі рядки є короткими, але можуть містити символи, що не є символами ASCII (байти з ненульовими старшими бітами)
binary	Можуть бути присутніми не тільки символи, що не є символами ASCII, але і рядки не обов'язково повинні бути достатньо короткими для транспорту SMTP
quoted-printable	Дані кодуються таким чином: якщо початкові дані є основним текстом ASCII, то в кодованій формі вони залишаються значною мірою розпізнаваними людиною
base64	Дані кодуються відображенням 6-бітових блоків вхідних даних у 8-бітові блоки вихідних, всі вони є друкованими символами ASCII
x-token	Нестандартне кодування з вказаним ім'ям

Форма	Опис
Власна форма	Тіло повідомлення, яке має бути передано, створюється у власному форматі відповідної системи. Використовуються власні набори символів і, можливо, локальні угоди про символи закінчення рядків. Тіло повідомлення може бути текстовим файлом UNIX, растровим зображенням Sun, індексованим файлом VMS, звуковими даними в залежному від системи форматі, що зберігаються тільки в пам'яті, або чимось іншим, що відповідає локальній моделі подання деякої інформації. Головне, що дані створюються в деякій "рідній" формі, яка задається типом носія
Канонічна форма	Все тіло повідомлення, включаючи додаткову інформацію, наприклад, довжину записів і, можливо, інформацію про атрибути файлу, переводиться в універсальну канонічну форму. Найуживаніша канонічна форма тіла повідомлення визначається конкретним типом тіла повідомлення, а також взаємозв'язаними з ним атрибутами. Перетворення в правильну канонічну форму може означати перетворення набору символів, трансформацію звукових даних, стиснення або якісь інші дії, застосовні до конкретного типу вмісту. Якщо використовується перетворення набору символів, слід чітко розуміти семантику подання вмісту, яка може істотно ускладнювати будь-які перетворення наборів символів (наприклад, з урахуванням синтаксично важливих символів у тексті, підтип якого відрізняється від простого)

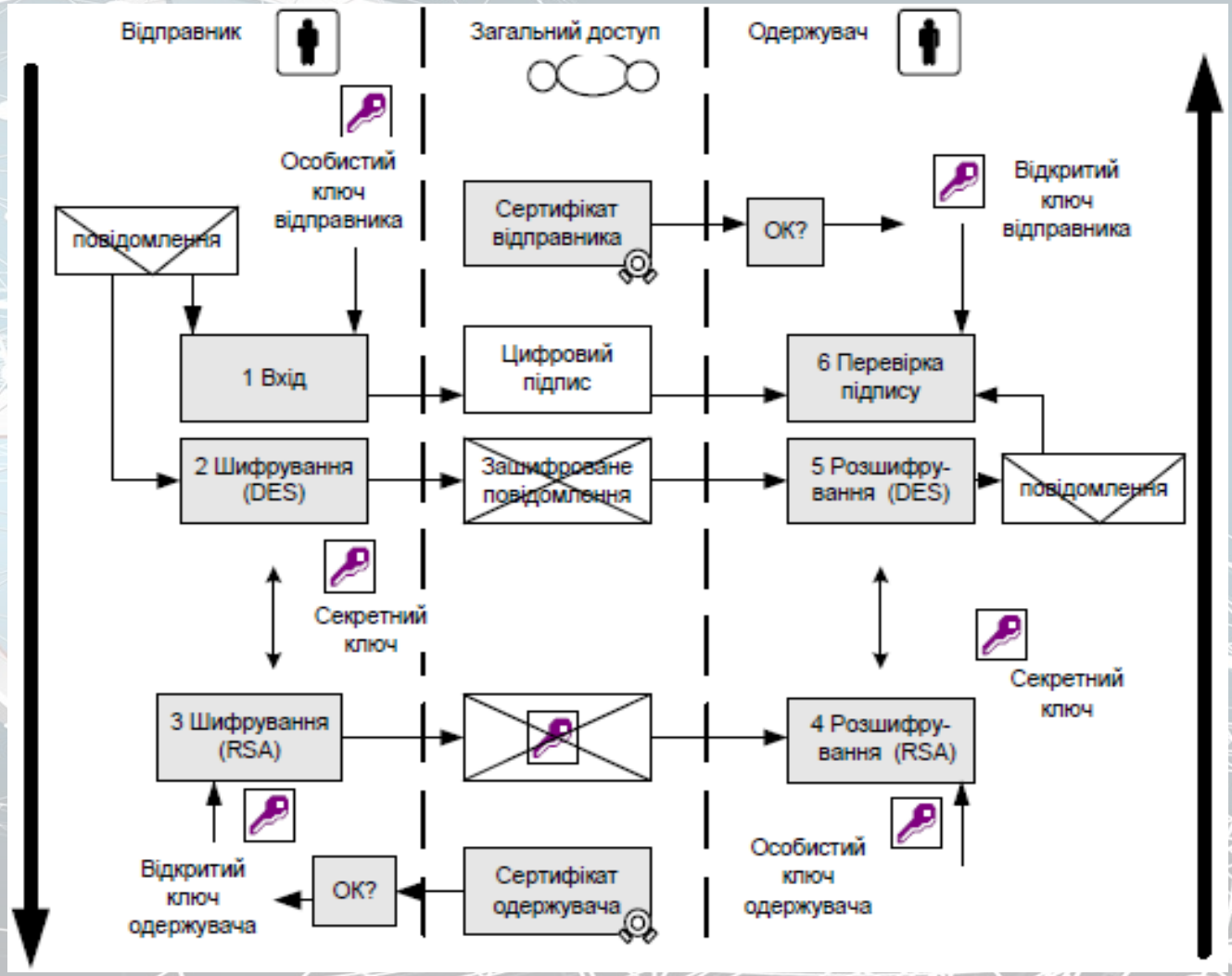
S/MIME забезпечує можливість використання таких функцій

- Упаковані дані. Складаються з шифрованого вмісту будь-якого типу і ключів шифрування вмісту для одного або більшого числа одержувачів.
- Підписані дані. Цифровий підпис формується за допомогою обчислення профілю для вмісту повідомлення, яке вимагає підпису, і потім шифрується з використанням особистого ключа сторони, яка підписує цей вміст. Після цього вміст разом з підписом переводяться у формат base64. Повідомлення з підписаними даними може бути проглянуто тільки одержувачем, що має в своєму розпорядженні можливості S/MIME.
- Відкриті підписані дані. Як і у випадку підписаних даних, формується цифровий підпис вмісту. Проте в даному разі з використанням base64 кодується тільки цифровий підпис. У результаті одержувачі без можливостей S/MIME зможуть проглянути вміст повідомлення, але не зможуть перевірити підпис.
- Підписані й упаковані дані. Можливості підпису і упаковки можуть бути вкладені одна в іншу, так що шифровані дані можуть бути підписані, а підписані або відкриті підписані дані можуть бути зашифровані.

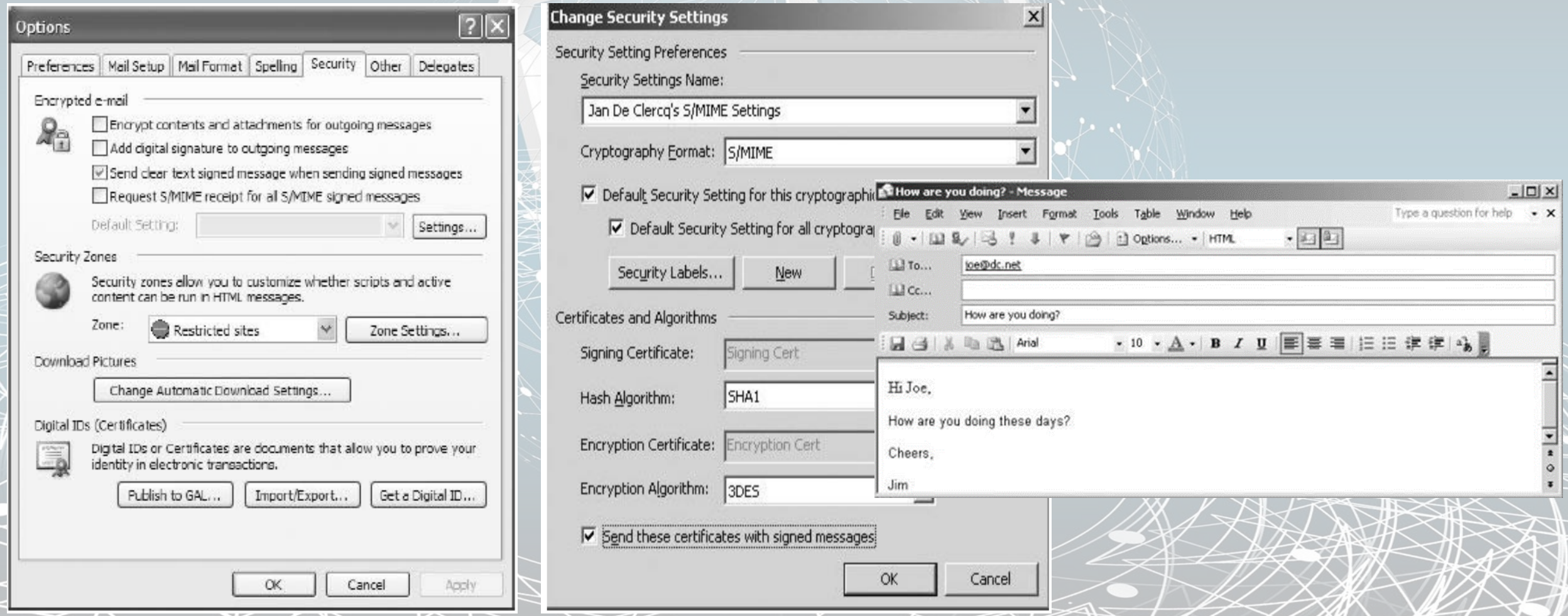
Схема використання S/MIME для автентифікації і забезпечення конфіденційності електронної пошти

Обмін S/MIME складається з таких кроків:

- Відправник створює цифрову сигнатуру для повідомлення з використанням свого приватного ключа.
- Відправник використовує єдиний ключ симетричного шифрування для шифрування повідомлення.
- Одержувач використовує свій приватний ключ, щоб розшифрувати захищену скриньку.
- Одержувач використовує відкритий ключ відправника для перевірки достовірності і цілісності повідомлення та засвідчує цифрову сигнатуру, яка є в сертифікаті відправника.



Налаштування S/MIME в Outlook



Характеристики S/MIME поштових клієнтів Microsoft

Функція	Поштовий клієнт		
	Outlook	Outlook Express	OWA
Поштовий протокол	MAPI/RPC, POP3, IMAP4, SMTP,HTTP	POP3, IMAP4, SMTP	HTTP
Постачальник сертифікатів	Exchange KMS, внутрішній ЦС, комерційний ЦС	Внутрішній ЦС, комерційний ЦС	Внутрішній ЦС, комерційний ЦС
Необхідний сервер обробки повідомлень Exchange	Ні	Ні	Так
Шифрування пошти (захист конфіденційності)	Так	Так	Так
Підпис пошти (перевірка справжності та цілісності)	Так	Так	Так
Безпечні Повідомлення	Так	Ні	Ні
Оформлення та оновлення сертифікатів користувачів	Може бути автоматизовано з використанням процедур оформлення сертифікатів Windows	Може бути автоматизовано з використанням процедур оформлення сертифікатів Windows	Може бути автоматизовано з використанням процедур оформлення сертифікатів Windows 2003 і XP
Перевірку відкликаних сертифікатів включено за умовчанням	Так	Ні	Так

Криптографічні алгоритми, які використовуються в системі S/MIME

Функція	Вимога
Створення профілю повідомлення для формування цифрового підпису	ОБОВ'ЯЗКОВА підтримка SHA-1 і MD5 РЕКОМЕНДОВАНО використання SHA-1
Шифрування профілю повідомлення для формування цифрового підпису	Для агентів відсилання і приймання ОБОВ'ЯЗКОВА підтримка DSS. Для агента відсилання РЕКОМЕНДОВАНО підтримку шифрування RSA. Для агента приймання РЕКОМЕНДОВАНО підтримку верифікації підписів RSA з довжиною ключа від 512 до 1024 біт
Шифрування сеансового ключа для передачі з повідомленням	Для агентів відсилання і прийому ОБОВ'ЯЗКОВА підтримка алгоритму Діфі-Хелмана. Для агента відсилання РЕКОМЕНДОВАНО підтримку шифрування RSA з довжиною ключа від 512 до 1024 біт. Для агента прийому РЕКОМЕНДОВАНО підтримку розшифрування RSA
Шифрування повідомлення для передачі з використанням сеансового ключа	Для агента відсилання РЕКОМЕНДОВАНО підтримку шифрування tripleDES і RC2/40. Для агента прийому ОБОВ'ЯЗКОВА підтримка розшифрування tripleDES і РЕКОМЕНДОВАНО підтримку розшифрування RC2/40

Новф типи вмісту MIME

Всі ці нові типи використовують позначення PKCS (Public-Key Cryptography Specifications – специфікації криптографії з відкритим ключем), опубліковані RSA Laboratories і доступні для S/MIME

- Упаковані дані. Підтип application/pkcs7-mime призначений для одного з чотирьох видів обробки S/MIME, кожного зі своїм унікальним параметром smime-типу.
- Підписані дані. Підтип signed Data (підписані дані) призначений для документів, підписаних однією або декількома сторонами.
- Відкрите підписане повідомлення. Відкрите підписане повідомлення виходить тоді, коли для вмісту використовується тип multipart і підтип signed.
- Запит реєстрації. Як правило, додаток або користувач звертається до центру сертифікації з приводу отримання сертифікатів відкритих ключів.

Користувач S/MIME повинен виконувати такі функції керування ключами.

- Генерування ключів. Для користувача відповідної утиліти адміністрування (наприклад, здійснюючою керування локальною мережею) ОБОВ'ЯЗКОВО повинна бути передбачена можливість генерувати окремі пари ключів Діфі-Хелмана і DSS і рекомендовано мати можливість генерувати пари ключів RSA.
- Реєстрація. Відкритий ключ користувача повинен бути зареєстрований за допомогою уповноваженого центру сертифікації для того, щоб одержати сертифікат цього ключа стандарту X.509.
- Зберігання і пошук сертифікатів. Користувачу потрібен доступ до локального списку сертифікатів, щоб мати можливість перевірити підписи, які надходять, і шифрувати повідомлення, що відправляються.

Захист інформації в електронних платіжних системах

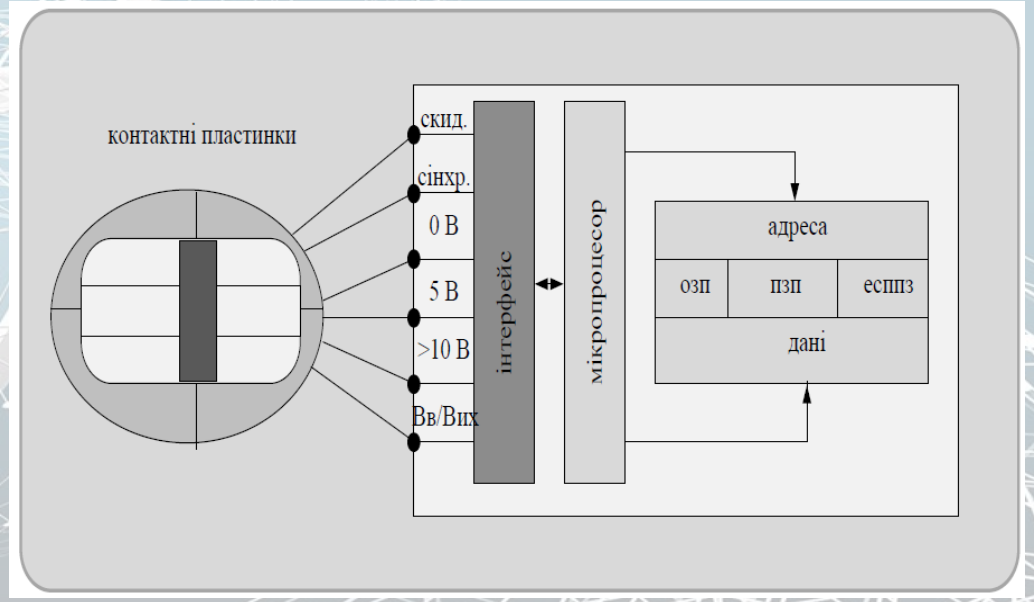
Електронні пластикові картки. Картки з мікросхемою можна класифікувати за декількома ознаками.

Перша ознака – функціональні можливості картки. Тут можна виділити такі основні типи карток:

- картки-лічильники;
- картки з пам'яттю;
- картки з мікропроцесором.

Друга ознака – тип обміну з пристроєм, якій зчитує інформацію:

- картки з контактним зчитуванням;
- картки з індукційним зчитуванням.



Електронні пластикові картки

У теперішній час у смарт-картки встановлюють:

- мікропроцесори з текстовою частотою 5 Мгц;
- оперативне ЗУ місткістю до 256 байт;
- постійне ЗУ місткістю до 10 Кбайт;
- незалежне ЗУ місткістю до 8 Кбайт.

Смарт-картка забезпечує широкий набір функцій:

- розмежування повноважень доступу до внутрішніх ресурсів (завдяки роботі із захищеною файловою системою);
- шифрування даних із застосуванням різних алгоритмів;
- формування електронного цифрового підпису;
- ведення ключової системи;
- виконання всіх операцій взаємодії власника картки, банку і торговця.

За принципом взаємодії з пристроєм, який зчитує інформацію, розрізняють картки двох типів:

- картки з контактним зчитуванням;
- картки з безконтактним зчитуванням.

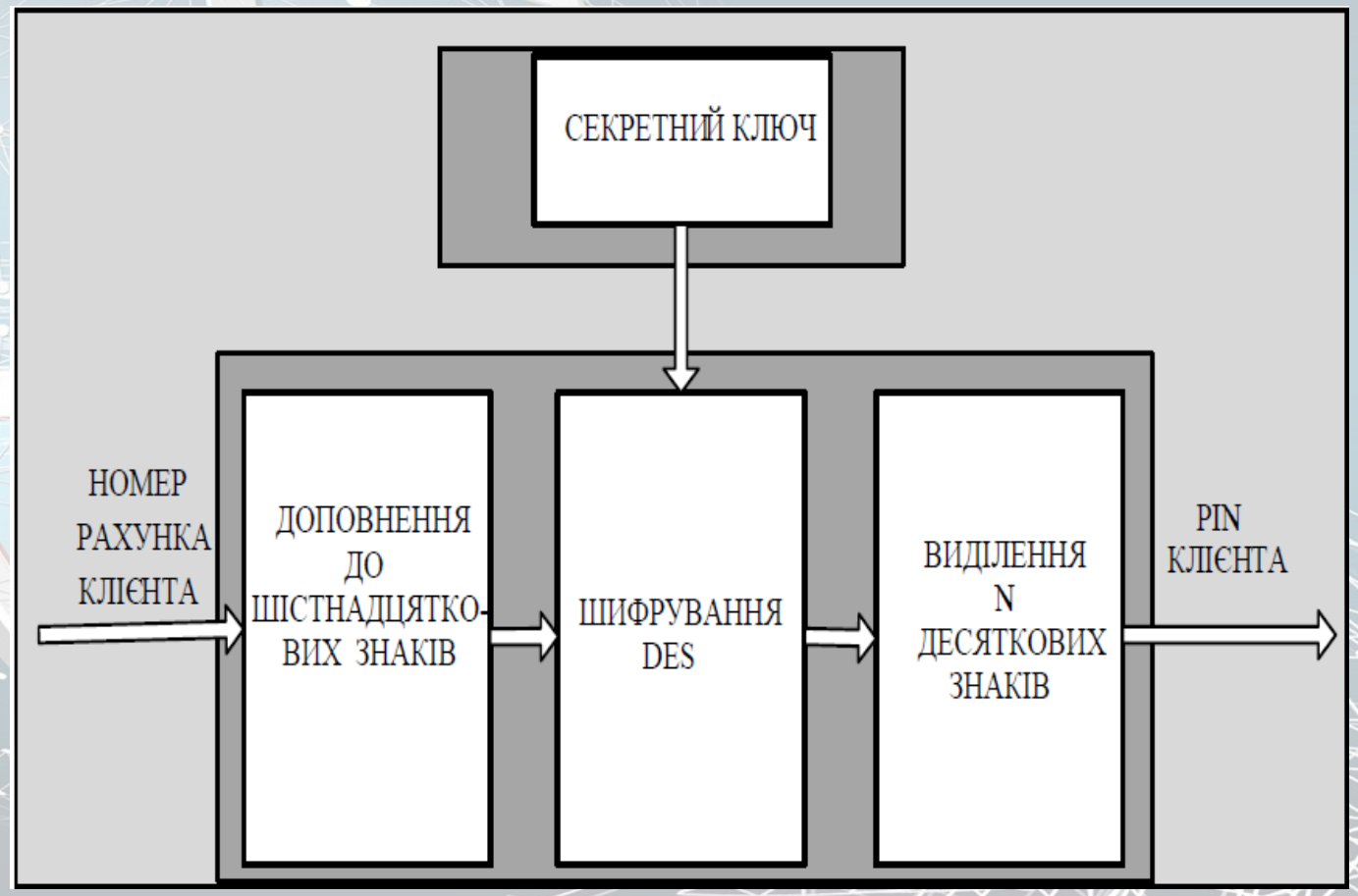
Генерації значення PIN

Метод генерації значення PIN істотно впливає на безпеку електронної платіжної системи. Взагалі, персональні ідентифікаційні номери можуть формуватися банком або власниками карт. Зокрема, клієнт розрізняє два типи PIN:

- PIN, призначений йому банком, що видав картку;
- PIN, вибраний власником картки самостійно.

Якщо PIN призначається банком, банк зазвичай використовує один з двох варіантів процедур генерації PIN.

При першому варіанті PIN генерується криптографічний з номера рахунка власника картки. Процес генерації PINa, призначеного з номера рахунку, показаний на рис. .



Забезпечення безпеки електронних платежів через мережу Інтернет

Для того щоб забезпечити повну безпеку і конфіденційність здійснення операцій, протокол SET повинен гарантувати неодмінне дотримання наступних умов.

- Абсолютна конфіденційність інформації. Власники карток повинні бути упевнені в тому, що їх платіжна інформація надійно захищена і доступна тільки вказаному адресату. Це є неодмінною умовою розвитку електронної торгівлі.
- Повне збереження даних. Учасники електронної торгівлі повинні бути упевнені в тому, що при передачі від відправника до адресата зміст повідомлення залишиться незмінним. Повідомлення, що відправляються власниками карток комерсантам, містять інформацію про замовлення, персональні дані і платіжні інструкції. Якщо в процесі передачі зміниться хоча б один з компонентів, то транзакція не буде оброблена належним чином. Тому, щоб уникнути помилок, протокол SET повинен забезпечити засоби, що гарантують збереження і незмінність повідомлень, які відправляються. Одним з таких засобів є використання цифрових підписів.
- Автентифікація (встановлення достовірності) рахунка власника картки. Використання цифрових підписів і сертифікатів власника картки гарантує автентифікацію рахунка власника картки і підтвердження того, що власник картки є законним користувачем даного номера рахунка.

Ієрархії довіри для перевірки сертифікатів SET

Сертифікати SET перевіряються в ієрархії довіри (рис.). Кожен сертифікат пов'язаний з сертифікатом підпису того об'єкта, який забезпечив його цифровим підписом. Йдучи по "дереву довіри" до відомої довіреної сторони, можна бути впевненим у тому, що сертифікат є дійсним. Наприклад, сертифікат власника картки пов'язаний з сертифікатом емітента (або асоціації за дорученням емітента), який у свою чергу пов'язаний з кореневим ключем через сертифікат асоціації.

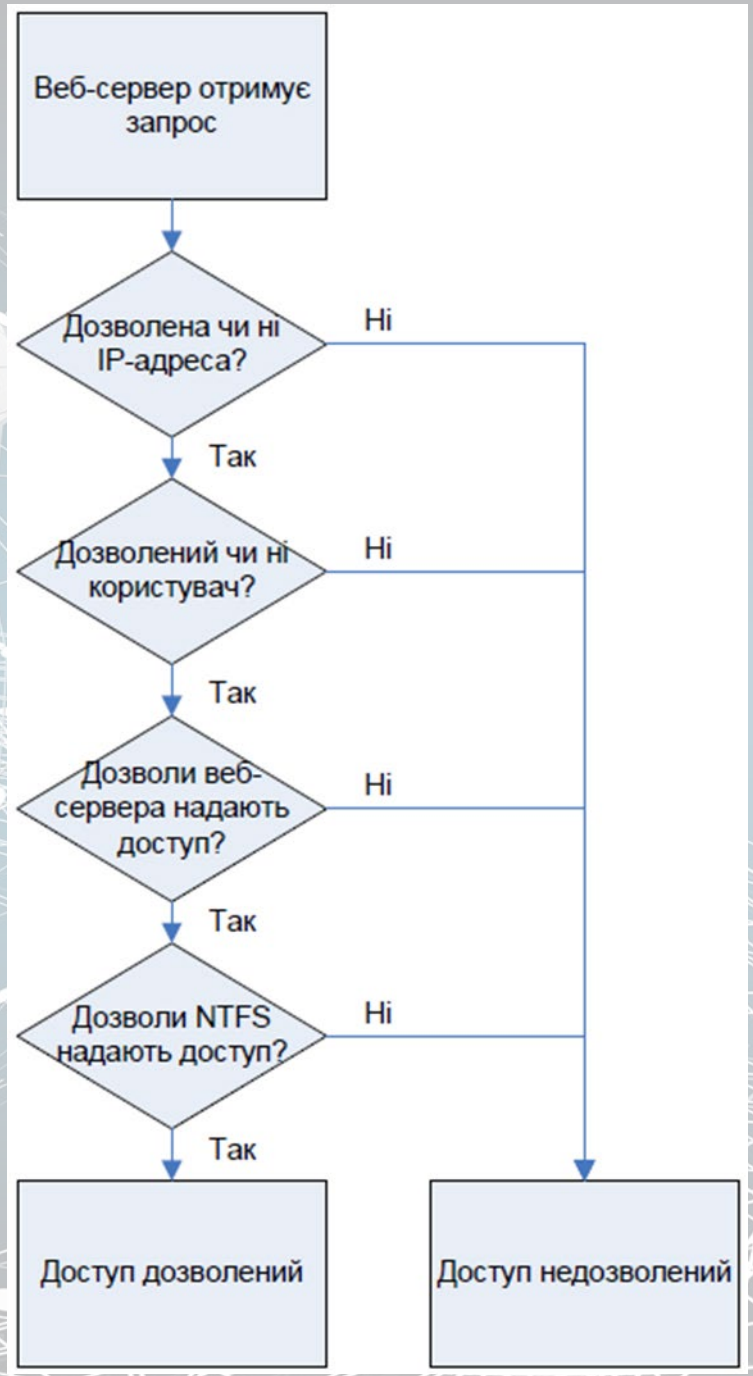


Управління доступом в мережевій технології «клієнт-сервер» для базових операційних систем

- Анонімний доступ. Анонімний доступ, який є найбільш широко використовуваним методом доступу до веб-вузлів, дозволяє будь-якому користувачеві відвідати загальні області на веб-сайті, але запобігає несанкціонованому доступу до важливих засобів адміністрування веб-сервера і приватним відомостям.
- Обмеження доступу для IP-адрес. Веб-сервер може бути налаштований таким чином, щоб забороняти доступ до вмісту веб-вузла з боку певних комп'ютерів, груп комп'ютерів і цілих мереж.
- Дозволи веб –сервера. У конфігурації веб-сервера є можливість задати дозволу для конкретних вузлів, каталогів і файлів.
- Дозволи NTFS. IIS залежить від дозволів NTFS при забезпеченні безпеки окремих файлів і каталогів від несанкціонованого доступу.

Структура процессу управління доступу

- Клієнт запитує ресурс на сервері.
- Сервер, якщо його конфігурація припускає це, запросить у клієнта відомості для перевірки автентичності. Оглядач або запропонує користувачеві ввести ім'я користувача та пароль, або передасть ці відомості автоматично.
- IP- адресу клієнта перевіряється на обмеження IP- адрес , закладені в IIS. Якщо доступ для IP- адреси заборонено , запит не виконується і користувач отримує повідомлення про помилку "403 Access Forbidden".
- IIS перевіряє допустимість облікового запису користувача. Якщо обліковий запис користувача не є припустимою , запит не виконується і користувач отримує повідомлення про помилку "403 Access Forbidden".
- IIS перевіряє наявність у користувача веб- дозволів для запитуваного ресурсу . Якщо користувач не має відповідного дозволу , запит не виконується і користувач отримує повідомлення про помилку "403 Access Forbidden".
- Будь-які модулі безпеки від незалежних розробників , додані адміністратором вузла веб , використовуються на цьому етапі.
- IIS перевіряє дозволу NTFS для ресурсу. Якщо користувач не має дозволів NTFS для ресурсу , запит не виконується і користувач отримує повідомлення про помилку "401 Access Forbidden".
- Якщо користувач має дозвіл NTFS , запит виконується.



Рівні дозволу

веб –сервера

- Читання (вибирається за замовчуванням). Користувачі можуть переглядати вміст файлу і його властивості.
- Запис. Користувачі можуть змінювати вміст файлу і його властивості.
- Доступ до тексту сценарію. Користувачі отримують доступ до вихідних файлів. Якщо вибрано дозвіл «Читання», вихідний текст може бути прочитаний. Якщо встановлено дозвіл «Запис», можна проводити запис і в вихідні тексти. «Доступ до тексту сценарію» дозволяє доступ до вихідних текстів для файлів, наприклад сценаріями в додатку ASP. Ця можливість доступна лише при встановлених дозволах «Читання » або «Запис».
- Огляд каталогів. Користувачі можуть переглядати списки і сімейства файлів.
- Запис у журнал. Запис у журнал робиться для кожного відвідування вузла веб.
- Індексація каталогу. Дозволяє службі індексації створити індекс для ресурсу.

NTFS

- Повний доступ. Користувачі можуть змінювати , додавати , переміщати і видаляти файли, властивості, пов'язані з ними, і каталоги. Крім цього, можна змінити дозволи для всіх файлів і підкаталогів.
- Зміна. Користувачі можуть переглядати і змінювати файли та їх властивості, включаючи видалення і додавання файлів в каталог або властивостей файлу до файлу.
- Читання та виконання. Користувачі можуть запускати виконувані файли, включаючи сценарії.
- Список вмісту папки. Користувачі можуть переглядати список вмісту папки.
- Читання. Користувачі можуть переглядати файли та їх властивості.
- Запис. Користувачі можуть записувати файл.Немає доступу Коли жоден з прапорців не встановлений, користувачі не мають ніякого доступу до ресурсу, навіть якщо користувач має доступ до каталогу більш високого рівня.

Контрольні запитання

1. Наведіть приклади класів електронної комерції і основні засоби їх безпеки.
2. Наведіть приклади основних сервісів, що забезпечуються зв'язком з мережею Інтернет, і засоби їх безпеки.
3. Дайте визначення брандмауера.
4. Які основні різновиди заміни мережевої адреси використовуються в брандмауерах?
5. Надайте структуру системи захисту інформації на фірмі, основним “інтернетівським” сервісом якої є електронна пошта, і ставлять високі вимоги до постійної доступності до сервісу.
6. Які основні функції системи PGP?
7. Опишіть алгоритм створення повідомлення системою PGP.
8. Опишіть алгоритм отримання повідомлення системою PGP.
9. Проілюструйте загальний формат повідомлення PGP.
10. Опишіть алгоритм визначення ступеня довіри ключам.
11. Укажіть причини, за якими алгоритми DES, “потрійний” DES з двома ключами RC2 і RC5 підходить або не підходить для PGP.
12. Опишіть загальні процедури підготовки повідомлень S/MIME. Які криптографічні алгоритми використовуються в S/MIME?
13. Дайте короткий опис типів, підтипів і вмісту S/MIME.
14. Яким чином користувачі оформляють і відновлюють сертифікати S/MIME?
15. Які механізми захисту повинні бути реалізовані для забезпечення функцій захисту інформації на окремих вузлах системи електронних платежів?
16. Опишіть набір функцій, реалізованих в смарт-картці.



Стеганографія

Основними завданнями є

- захист інформації з обмеженим доступом від несанкціонованого доступу;
- захист авторських прав на окремі види інтелектуальної власності;
- подолання систем моніторингу та управління мережевими ресурсами;
- програмне забезпечення для маскування;
- створення прихованих каналів для витоку конфіденційної інформації від законних користувачів.

Класифікація стеганографічних методів

- До методів технологічної стеганографії
  - Хімічні методи
  - Фізичні методи
- Інформаційна стеганографія
  - Методи лінгвістичної стеганографії
    - сленговий код
    - фіктивний код
    - геометрична система
  - Комп'ютерна стеганографія
    - приховування інформації
    - приховані канали
    - цифрови технології нанесення водяних знаків
    - цифрові відбитки

Класифікація способів приховування інформації

- За способом відбору контейнерів
  - методи сурогатної стеганографії,
  - селективної стеганографії
  - конструктивної стеганографії.
- За способом доступу до прихованої інформації
  - потокові контейнери
  - контейнери з довільним доступом
- З точки зору типу організації
  - систематичними
  - несистемними
- За використовуваними принципами
  - цифрові методи
  - структурні методи
- За типом інформаційного середовища
  - для текстового середовища,
  - для аудіосередовища,
  - для зображень (стоп-кадрів)
  - відеосередовищ.

Класифікація стегосистем

- Безключові стегосистеми
- Стегосистеми з закритим ключем
- Стегосистеми з відкритим ключем
- Змішані стегосистеми

Напрямки

1) вкладення інформації з метою її прихованої передачі;

2) вбудовування цифрових водяних знаків (ЦВЗ) (водяний знак);

3) вбудовування ідентифікаційних номерів (відбитки пальців);

4) Субтитри.

Текстові стеганографи

Можна виділити наступні методи, які зустрічаються в сучасних лінгвістичних стеганографах:

- методи спотворення формату текстового документа;
- синтаксичні прийоми;
- семантичні методи;
- методи формування стеганограм за допомогою прихованого повідомлення.

Методи спотворення формату текстового документа

- додавання одного або двох пробілів в кінці речення після кінцевого символу
- закодовані додатковими пробілами в кінці кожного рядка тексту
- за допомогою пробільних символів маніпулює текстами, які вирівняні по обидва боки
- проміжок між словами може бути використаний для кодування прихованих даних
- стеганографічні методи, які інтерпретують текст як двійкове зображення
- зсуву слів форматованого тексту

Синтаксичні прийоми

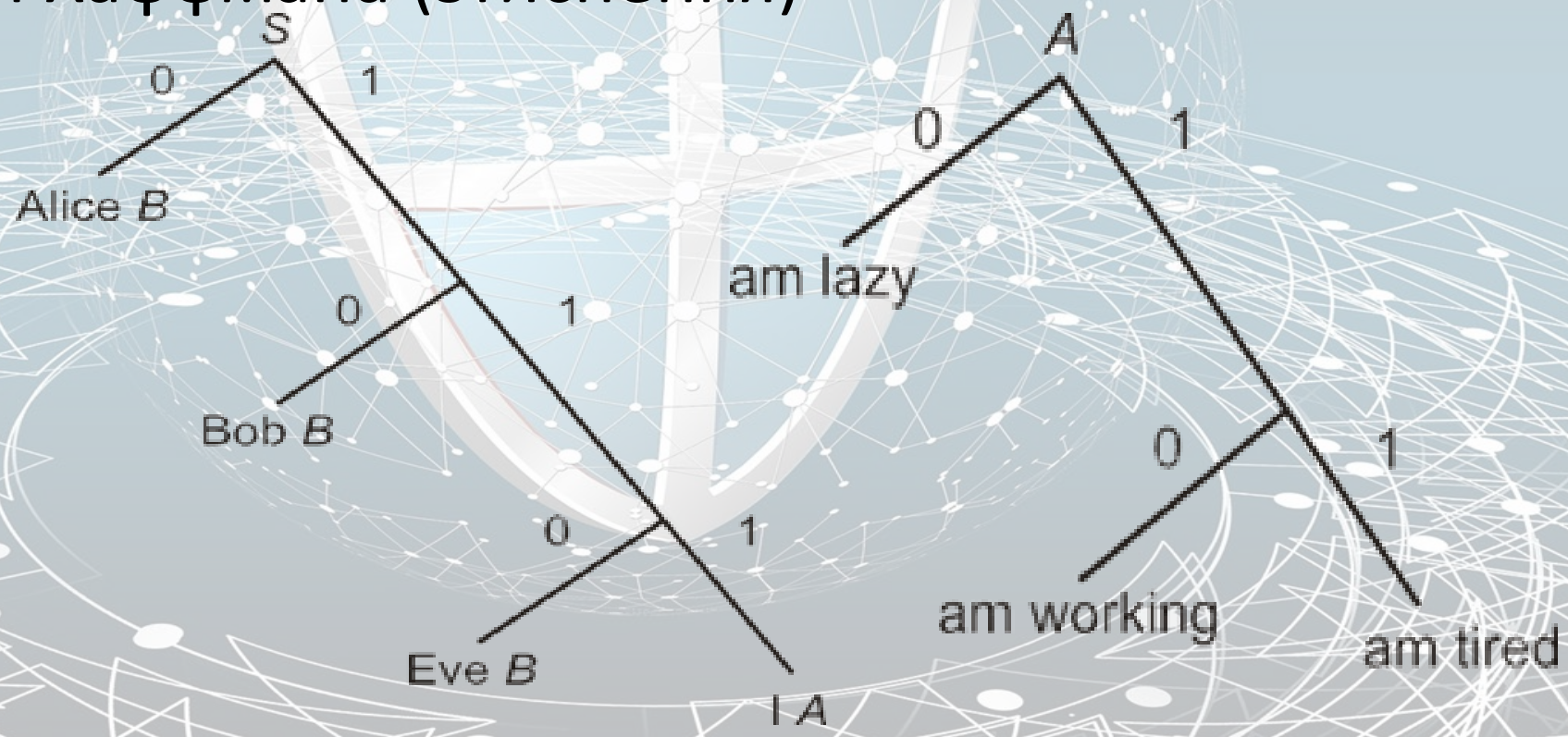
- зміни пунктуації
- способи зміни стилю
- структури тексту

Семантичні методи

- реалізується шляхом безпосередньої заміни слів
  потрібні таблиці синонімів

Методи формування стеганограм

- Функція моделювання n-го порядку
- кодування Хаффмана (зтиснення)



Структурна схема типової стегосистеми

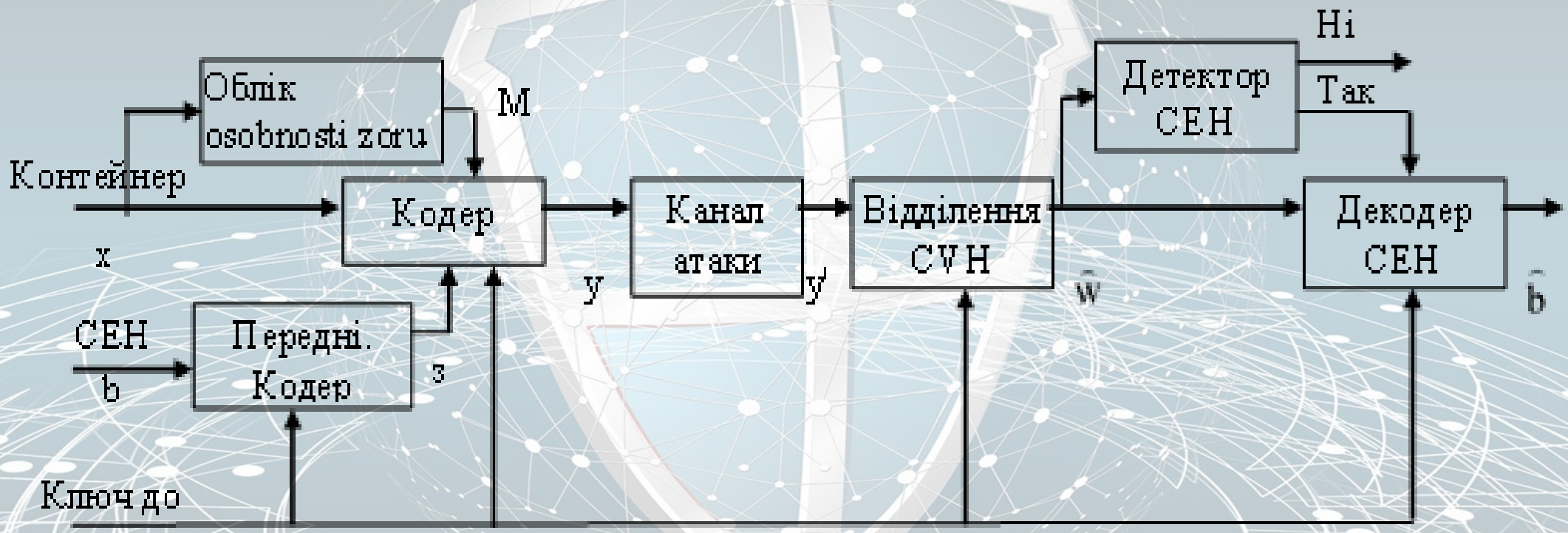
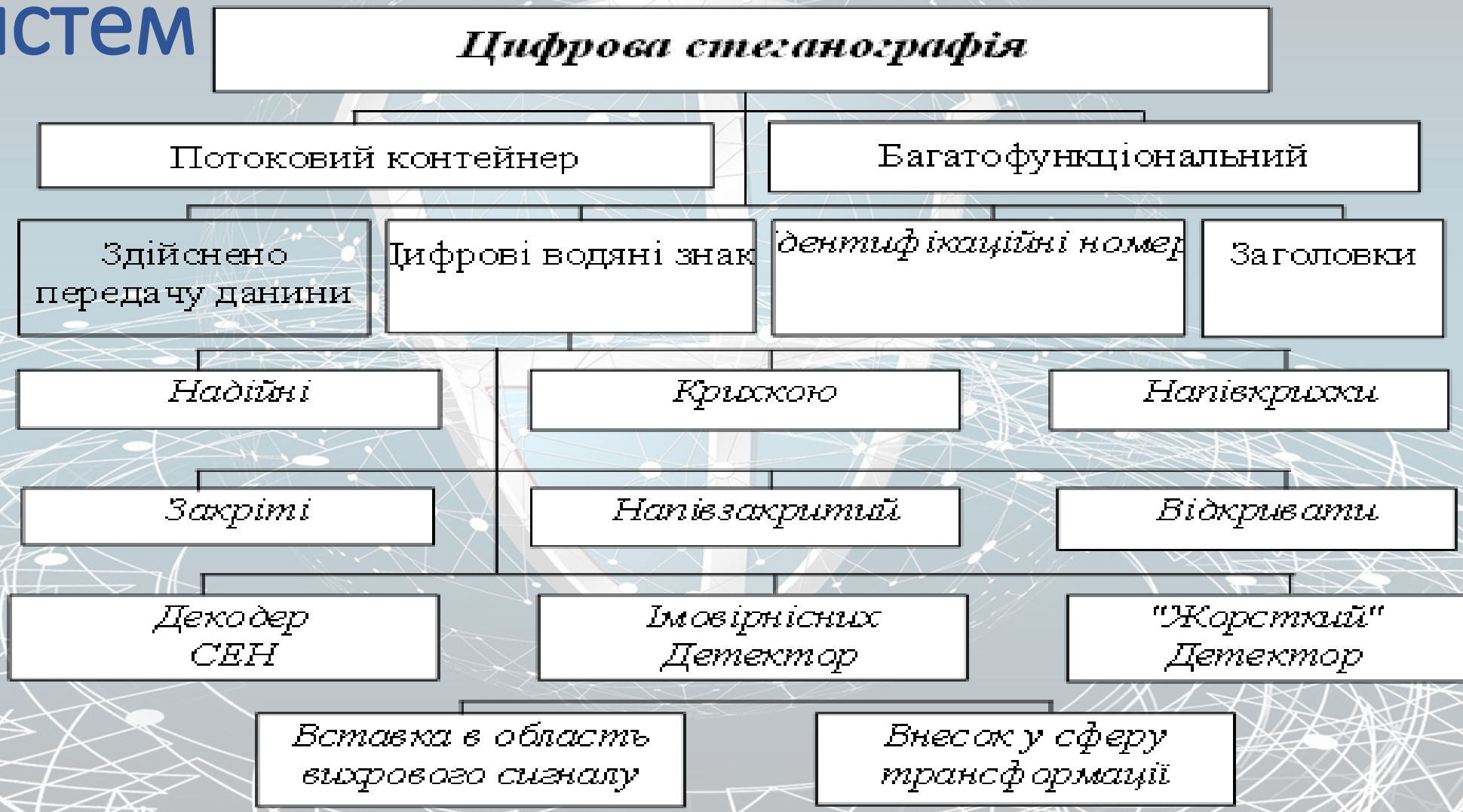


Рис.1.1. Структурна схема типової стегосистеми СЕН

Класифікація систем вбудовування

		Що потрібно датчику		Вихід датчика	
		Оригінальний знак	Базовий рівень ЦВЗ	Так/Ні	ЦВЗ
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакритий		-	+	+	-
Відкривати		-	-	-	+

Класифікація цифрових стеганографічних систем



Потенційні сфери стеганографічного виробництва

Області стеганографії

Захист від копування

Електронна комерція, копіювання контроль (DVD), Мультимедійна дистрибуція (відео за напоєм)

Приховання документів

Медичні зображення, картографія, мультимедійні бази даних

Автентифікація

Захист, електронна комерція, голосові системи
Пошта, електронна конференція

Приговане підлючвення

Військова праворуч і розвідка
Додатки, і також додаткі в тихих випадах, якщо криптографія
Немає можливості вікористоваті

Стеганографічні протоколи

- Стеганографія з відкритим ключем Криптографічна система з відкритим ключем використовується, наприклад, в цифровому підписі. У цьому випадку повідомлення підписується закритим ключем, і будь-хто, хто має відповідний відкритий ключ, може перевірити його справжність. При шифруванні даних використовується зворотний порядок: повідомлення підписується відкритим ключем, а прочитати його можуть тільки ті, у кого є відповідний закритий ключ.
- Виявлення ССЗ з нульовим розголошенням
  Категорії вимог до надійних ССЗ:
  - ЦВЗ відкривають для себе всі. У цьому випадку він служить для сповіщення власника захищеного вмісту та запобігання ненавмисному порушенню прав власника.
  - ЦВЗ виявляється хоча б однією стороною. В даному випадку його використання пов'язане з пошуком незаконно поширюваних копій, наприклад, в інтернеті.
  - ЦВЗ надзвичайно важко модифікувати або витягти з контенту. У цьому випадку СЕН використовується для аутентифікації.

Інші можливі способи введення бітів ЦВЗ в контейнер

1) Бітова інверсія
2) Бітова вставка.
3) Розрядне видалення.
4) Використання прапора біта.
5) Застосування порогових біт.
6) Використання табличних значень.
7) Динамічно змінюється таблиця.
8) Непряма динамічна таблиця.

В стегоаналізі можна виділити наступні види атак.

- Атака на основі відомого заповненого контейнера..
- Атака на основі відомого вбудованого повідомлення.
- Атака на основі вибраного прихованого повідомлення.
- Адаптивна атака на основі обраного прихованого повідомлення..
- Атака на основі обраного заповненого контейнера..

У отримувача може з'явитися можливість використовувати ще три атаки, які не мають прямих аналогів в криптоаналізі.

- Атака на основі відомого порожнього контейнера. –
- Атака на основі обраного порожнього контейнера.
- Атака на основі відомої математичної моделі контейнера або його частини.

Класифікація атак на стегосистеми системи водяних знаків

- Атаки на вбудоване повідомлення
- Атаки на стегодетектор спрямовані на те, щоб ускладнити або унеможливити належну роботу датчика
- Атаки на протокол використання
- Атаки на саму ЦВЗ

Відповідно до цієї класифікації, всі атаки на системи вбудовування ЦВЗ можна розділити на чотири групи:

1) атаки, спрямовані на видалення ЦВЗ;

2) геометричні атаки, спрямовані на спотворення контейнера;

3) криптографічні атаки;

4) атаки на використовуваний протокол вбудовування та валідації ЦВЗ.

Приховування даних на зображеннях і відео

Візуальне середовище (цифрові зображення та відео) має велику кількість надмірностей різної природи:

- надмірність коду;
- міжпіксельна надмірність;
- психовізуальна залежність.

Групи методів приховування:

- методи заміщення в часовій (просторовій) області;
- методи маскування в частотній області зображення;
- широкосмугові методи;
- статистичні методи;
- прийоми спотворення;
- структурні методи.

Методи підстановки

- метод підстановки найменшого значущого біта
- метод випадкових інтервалів
- техніка псевдовипадкової перестановки
- метод приховування блоків
- способи заміни палітри
- метод квантування зображень

Методи маскування в частотній області зображення

- дискретне косинусне перетворення,
- швидке перетворення Фур’є
- вейвлет-перетворення

Методи широкосмугового зв'язку

- за допомогою псевдовипадкової послідовності, де секретний сигнал, що відрізняється константою, модулюється псевдовипадковим сигналом;
- за допомогою стрибків частот, коли частота несучого сигналу змінюється за деяким псевдовипадковим законом.

Статистичні методи

- приховують інформацію, змінюючи деякі статичні властивості зображення

Методи спотворення

- маскування складається з ряду модифікацій контейнера, які підбираються відповідно до секретного зв'язку
- вставка прихованих даних - це спроба змінити порядок появи надлишкової інформації в контенті, а не змінити його зміст

Структурні методи

- інформація приховується на рівні змісту за допомогою структурно-інформаційних параметрів зображення (семаграма)

Приховування інформації в звуковому середовищі

- Метод найменш значущих бітів
- Методи широкосмугового кодування
- Спосіб маскування в ехосигналі
- Методи фазового приховування

Музичні стегосистеми

забезпечують приховування інформації в музичному середовищі за аналогією з імпровізацією музичних творів