МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

КАФЕДРА КОМП'ЮТЕРНО-
ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

КОМПЛЕКСНА БЕЗПЕКА ІНФОРМАЦІЙНИХ МЕРЕЖЕВИХ СИСТЕМ

НАВЧАЛЬНИЙ ПОСІБНИК

для студентів спеціальності
174 «Автоматизація, комп'ютерно-інтегровані технології
та робототехніка»

Тернопіль
2023

УДК 681.3

К63

ISBN 978-617-7875-63-4

Укладачі:
Микитишин А.Г., канд. техн. наук, доцент,
Митник М.М., канд. техн. наук, доцент,
Голотенко О.С., канд. техн. наук, доцент,
Карташов В.В., канд.техн. наук, доцент.

Рецензенти:
Карпінський М.П, доктор технічних наук, професор;
Гордєєва О.О. доктор технічних наук, професор.

Відповідальний за випуск *Голотенко О.С.*, канд. техн. наук, доцент

Посібник рекомендовано до друку вченою радою
Тернопільського національного технічного університету імені Івана Пулюя
протокол №6 від 20 червня 2023 р.

Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.

ЗМІСТ

ВСТУП

В даний час, в Україні, в зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Розвиток нових інформаційних технологій і загальна комп'ютеризація призвели до того, що інформаційна безпека не тільки стає обов'язковою, вона є однією з характеристик інформаційної системи (ІС).

Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє першочергову роль (наприклад, банківські інформаційні системи). Під безпекою ІС розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів. Інакше кажучи, це здатність протидіяти різним впливи на ІС. Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів. Якщо виходити з класичного розгляду кібернетичної моделі будь-якої керованої системи, впливи на неї можуть носити випадковий або навмисний характер. Однак в цьому посібнику основна увага приділяється загрозам навмисним, які на відміну від випадкових мають на меті нанесення шкоди керованій системі або користувачам. Це робиться нерідко заради отримання особистої вигоди.

Численні публікації останніх років показують, що зловживання інформацією, що циркулює в ІС або передається по каналах зв'язку, удосконалювалися не менше інтенсивно, ніж заходи захисту від них. В даний час для забезпечення захисту інформації необхідна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії і т. д.). Комплексний характер захисту виникає з комплексних дій зловмисників, які прагнуть будь-якими засобами добути важливу для них інформацію.

Сьогодні можна стверджувати, що народжується нова сучасна технологія – технологія захисту інформації в комп'ютерних інформаційних системах і в мережах передачі даних. Реалізація цієї технології вимагає значних витрат і зусиль. Однак все це дозволяє уникнути значно переважаючих втрат і збитків, які можуть виникнути при реальному здійсненні атак на ІС.

1. Основні поняття, концепції і принципи інформаційної безпеки

1.1. Ідентифікація, автентифікація і авторизація

Для пояснення таких базових понять інформаційної безпеки, як ідентифікація, автентифікація і авторизація, уявімо інформаційну систему (ІС) у вигляді спрощеної моделі контрольованого доступу, коли кілька користувачів спільно працюють з ресурсами інформаційної системи. Народжена півстоліття тому і спрямована на підвищення ефективності застосування комп'ютера концепція поділу ресурсів висунула проблеми безпеки обчислювальних систем на перший план – необхідно було **контролювати доступ** користувачів до комп'ютера, захищаючи системні і користувацькі дані від помилкових або зловмисних дій. Контрольований доступ є важливим напрямком забезпечення безпеки поряд з іншими засобами безпеки: криптографічним захистом, аудитом, сегментацією мережі і т. п.

У моделі контрольованого доступу визначені об'єкти, суб'єкти, операції і система контролю доступу (рис. 1.1).

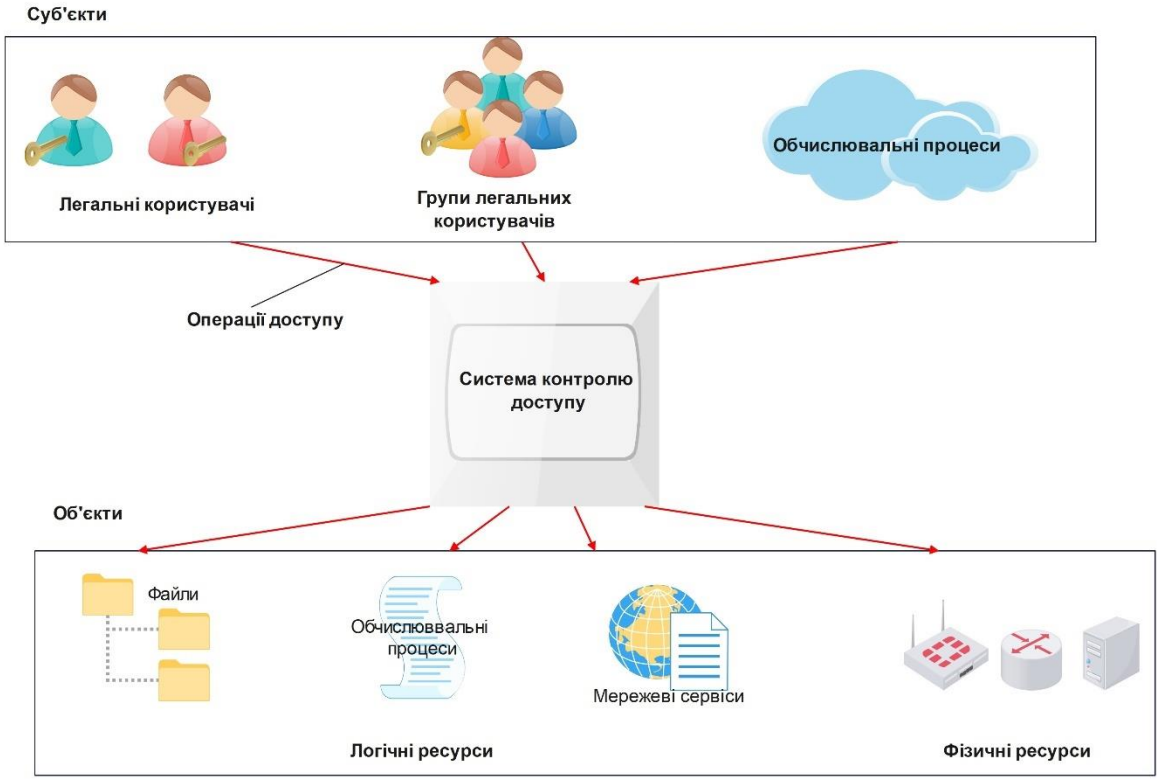


Рис. 1.1. Модель контрольованого доступу

Об’єкти представляють фізичні і логічні інформаційні ресурси (ІС). До фізичних ресурсів належать як окремі пристрої повністю (процесор, зовнішні пристрої, маршрутизатори, комутатори, фізичні канали зв’язку і т. п.), так і фізично поділювані ресурси пристрою (розділи і сектори диску, процесорний час, фізичні з’єднання каналу зв’язку). Логічними ресурсами є файли, обчислювальні процеси, мережеві сервіси, додатки, пропускна спроможність каналів зв’язку і т. п.

Суб’єкти представляють сутності, між якими поділяються інформаційні ресурси. Це можуть бути легальні користувачі ІС: персонал, який підтримує роботу ІС, зовнішні і внутрішні клієнти; групи легальних користувачів, що об’єднані по різним ознаках. Користувач здійснює доступ до об’єктів ІС не безпосередньо, а за допомогою прикладних процесів, які запускаються від його імені. Тому в якості суб’єктів виступають також прикладні обчислювальні процеси.

Операції виконуються суб’єктами над об’єктами. Для кожного типу об’єктів існує власний набір операцій, які з ними може виконувати суб’єкт. Наприклад, для файлів це операції читання, записи, видалення, виконання; для принтера – друк, перезапуск, очищення черги документів, припинення друку документа; для маршрутизатора – конфігурування і т. д.

Система контролю доступу вирішує, які операції дозволені для даного суб’єкта по відношенню до даного об’єкту. Для автоматизованого контролю доступу необхідно, щоб для кожної пари «суб’єкт-об’єкт» були однозначно визначені правила доступу, на підставі яких система могла б дозволити або заборонити виконання кожної з передбачених для даного об’єкта операції.

Найважливішими елементами керованого доступу є процедури ідентифікації, автентифікації і авторизації.

Ідентифікація – це присвоєння об’єктам і суб’єктам інформаційної системи унікальних імен – **ідентифікаторів**.

Лише при наявності унікальних ідентифікаторів система отримує можливість розпізнавати і оперувати суб’єктами і об’єктами. Одні ідентифікатори автоматично генеруються ОС і додатками (ідентифікатори процесів, ідентифікатори логічних мережевих з’єднань), інші призначаються адміністратором комп’ютерної мережі (ідентифікатори користувачів, адреси комп’ютерів, доменні імена мережевих сервісів), треті породжуються звичайними мережевими користувачами, що володіють таким правом (вибір власного імені, призначення імен файлів).

Ідентифікація користувачів є процедурою, що виконується при логічному вході в систему, коли користувач у відповідь на виведене на екрані запрошення

вводить свій ідентифікатор (ім'я), а система, звіряючись зі своїми даними, визначає, чи входить дане ім'я в число імен зареєстрованих (легальних) користувачів. Користувач може бути представлений в системі у вигляді декількох суб'єктів і відповідно мати кілька користувацьких ідентифікаторів.

Автентифікація – це процедура підтвердження суб'єктом/об'єктом того, що він є те (тим), за що (кого) він себе видає.

Автентифікація, або, іншими словами, процедура встановлення автентичності, може застосовуватися як до користувачів, так і до інших об'єктів і суб'єктів, зокрема до даних, програмами, додатків, пристроїв, документів.

Автентифікація даних означає доказ їхньої автентичності, тобто того, що вони поступили в незміненому вигляді і саме від того суб'єкта, який оголосив про це.

У процедурі автентифікації беруть участь дві сторони:

- *автентифікований* доводить свою автентичність, пред'являючи деякий доказ – *автентифікатор*;
- *автентифікуючий* перевіряє ці докази і приймає рішення.

Автентифікація буває односторонньою і двосторонньою (взаємною).

Одностороння автентифікація використовується, зокрема, при виконанні логічного входу в захищену систему. Після того як користувач повідомляє системі свій ідентифікатор, він повинен пройти процедуру автентифікації, тобто довести, що саме йому належить введений ним ідентифікатор (ім'я користувача). Автентифікація запобігає доступ до мережі небажаних осіб і дозволяє вхід для легальних користувачів.

В якості автентифікатора автентифікований може продемонструвати знання якогось загального для обох сторін секрету, наприклад слова (пароля), або володіння певним унікальним предметом (фізичним ключем) або пред'явити власні біологічні характеристики (відбитки пальців).

У деяких випадках односторонньої автентифікації виявляється недостатньо і тоді використовують **двосторонню автентифікацію**. Наприклад, користувач, який звертається із запитом до корпоративного веб-сервера, повинен довести йому свою легальність, але він також повинен переконатися сам, що веде діалог дійсно з веб-сервером свого підприємства. Іншими словами, сервер і клієнт повинні пройти процедуру автентифікації. В цьому випадку використовується двостороння автентифікація на рівні додатків. При встановленні сеансу зв'язку між двома пристроями також часто передбачаються процедури взаємної автентифікації пристроїв на більш низькому, канальному, рівні.

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.

На відміну від автентифікації, яка дозволяє розпізнати легальних і нелегальних користувачів, авторизація стосується лише легальних користувачів, які успішно пройшли процедуру автентифікації.

Доступ до об'єктів, який отриманий в обхід дозволу системи контролю доступу, називається **несанкціонованим**, або **неавторизованим**.

1.2. Моделі інформаційної безпеки

1.2.1. Тріада «конфіденційність, доступність, цілісність»

Поняття інформаційної безпеки може бути пояснено за допомогою так званих **моделей безпеки**. Суть цих моделей полягає в наступному: безліч всіх видів порушень безпеки ділиться на кілька базових груп таким чином, щоб будь-яке можливе порушення обов'язково можна було віднести принаймні до однієї з цих груп. Потім система оголошується безпечною, якщо вона здатна протистояти кожної з цих груп порушень.

Однією з перших і найбільш популярних донині моделей безпеки є тріада «конфіденційність, цілісність і доступність» (КЦД) або («Confidentiality, Integrity, Availability», CIA).

Вперше цей принцип був викладений в статті «Захист інформації в комп'ютерних системах», написаній Зальцером і Шредером в 1974-му році і опублікованій в «Communications of the ACM». Автори вважали, що всі можливі порушення інформаційної безпеки завжди можуть бути віднесені щонайменше до однієї з трьох груп: порушення конфіденційності, порушення цілісності або порушення доступності (рис. 1.2).

Рис. 1.2. Тріада «конфіденційність, цілісність і доступність»

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.

Вимоги до безпеки можуть змінюватися в залежності від призначення інформаційної системи, характеру використовуваних даних і типу можливих загроз. Важко уявити систему, для якої порушення цілісності та доступності не являли б безпеки, разом з тим забезпечення конфіденційності не завжди є обов'язковим. Наприклад, при публікації інформації в Інтернеті з метою зробити її доступною для широкого кола людей, то конфіденційність не потрібна. Однак вимоги цілісності і доступності залишаються актуальними.

Деякі види порушень безпеки можуть бути приведені до моделі КДЦ тільки шляхом розширеного тлумачення основоположних понять конфіденційності, доступності та цілісності. Так, властивість конфіденційності по відношенню, наприклад, до пристрою друку можна інтерпретувати так, що доступ до пристрою мають лише ті користувачі, яким цей доступ адміністративно дозволений, причому вони можуть виконувати тільки ті операції з пристроєм, які для них визначені. Властивість доступність пристрою означає його готовність до роботи щоразу, коли в цьому виникає необхідність. А властивість цілісності може бути інтерпретована як властивість незмінності параметрів даного пристрою.

За більш ніж 40 років, що минули з моменту публікації статті Зальцера і Шредера, інформаційні системи і середовище, в якому вони функціонують, зазнали революційних змін, тому не дивно, що з'явилися нові типи порушень, які набагато важче (якщо взагалі можливо) трактувати в термінах КДЦ. Наприклад, ситуація: легальний клієнт банку посилає по електронній пошті запит на зняття з рахунку великої суми, а потім заявляє, що цей запит, який хоча і був посланий від його імені, він не відправляв. Чи є це порушенням безпеки? Так. Чи були при цьому порушені конфіденційність, доступність або цілісність?

Ні. Отже, список властивостей безпечної системи слід розширити, додавши до КЦД ще одну властивість – «неспростовність».

Неспростовність або **неможливість відмови від авторства** (non-repudiation) – це такий стан системи, при якому забезпечується неможливість заперечення користувачем, який виконав будь-які дії, факту їх виконання, зокрема заперечення відправником інформації факту її відправлення і/або заперечення одержувачем інформації факту її отримання.

1.2.2. Гексада Паркера и модель STRIDE

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. 1.3).

Рис. 1.3. Гексада Паркера

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.

Ще одним варіантом визначення безпеки ІС є модель **STRIDE** (абревіатура від англомовних назв типів порушень безпеки, перерахованих нижче). 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.).

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

Рис. 1.4. Модель STRIDE

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 знімає практично всі захисні бар'єри на його шляху.

Так само як і в гексаді Паркера, в моделі STRIDE всі можливі види порушень безпеки зводяться до шести типів порушень, три з яких повторюють КЦД (з урахуванням того, що тут ці три характеристики безпеки дано в негативному по відношенню до КДЦ варіанті), проте інші три – підміна даних, відмова від відповідальності і захоплення привілеїв – відрізняють модель STRIDE від гексади Паркера.

Таким чином, визначення інформаційної безпеки на основі гексади Паркера наступне:

Інформаційна безпека (ІБ) – всі аспекти, пов'язані з визначенням, досягненням і підтримкою конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності і достовірності інформації або засобів її обробки.

1.3. Вразливість, загроза, атака

Вразливість (Vulnerability) – це слабка ланка інформаційної системи, яка, ставши відомою зловмисникові, може дозволити йому порушити її безпеку.

Вразливими є, наприклад, помилка в програмі, примітивний пароль, неправильне призначення прав доступу до файлу з важливими даними і безліч інших дефектів в розробці, експлуатації або налаштування системи.

Вразливості системи можуть бути прихованими, тобто ще не виявленими, відомими, але тільки теоретично, або ж загальновідомими, які активно використовуються зловмисниками. Для загальновідомих вразливостей в програмних продуктах виробники регулярно випускають виправлення, звані **патчами** (patch – латка). Однак, до регулярного внесення виправлень не всі і не завжди ставляться з належною увагою, через це загальновідомі, але невиправлені помилки в програмному забезпеченні є одними з найпоширеніших типів вразливостей.

Іншим типом вразливостей, якими часто користуються зловмисники, є помилки в конфігурації програмних і апаратних засобів. Наприклад, імена «адміністратор» та «гість», встановлені за замовчуванням в багатьох ОС, можуть полегшити зловмисникам доступ до системи, тому вони повинні бути відразу, при початковому конфігуруванні ОС, замінені іншими, менш очевидними іменами. З цією ж метою адміністратор повинен налаштувати підсистему інтерактивного входу на те, щоб вона не показувала останнє ім'я користувача, систему аудиту - щоб фіксувала всі успішні і неуспішні спроби входу

користувачів, а також виконати інші настільки ж прості, але необхідні налаштування.

Пошук вразливостей – важлива частина завдання забезпечення безпеки. Ця робота включає в себе регулярне тестування системи. У будь-який момент часу для будь-якої системи можна вказати безліч різних видів вразливостей, наприклад, для операційних систем і додатків нові вразливості з'являються мало не щодня; виявляти їх вручну – завдання дуже трудомістке. Тому, для автоматизації пошуку вразливостей використовують різні програмні інструменти – **засоби сканування вразливостей**, такі, наприклад, як McAfee, Nessus і ін. Сканування полягає в послідовному (адреса за адресом вузла, або номер за номером порту, або ідентифікатор за ідентифікатором мережевого з'єднання) направленні запитів цільовій системі. Потім, на підставі отриманих відповідей генерується «інформаційний відбиток» і, нарешті, порівнянням «відбитка» з записами в базі даних виконується ідентифікація вразливості.

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).

Загрози бувають технічні, що виходять з штучно створеного людиною світу техніки і технологій (зокрема, з Інтернету), а також загрози, що виникають від природних катаклізмів, військових дій, терористичних атак або економічних потрясінь.

Атака (Attack) – це реалізована загроза.

Атака може відбутися тільки тоді, коли одночасно існують вразливість і спрямована на використання цієї вразливості загроза (рис. 1.5).

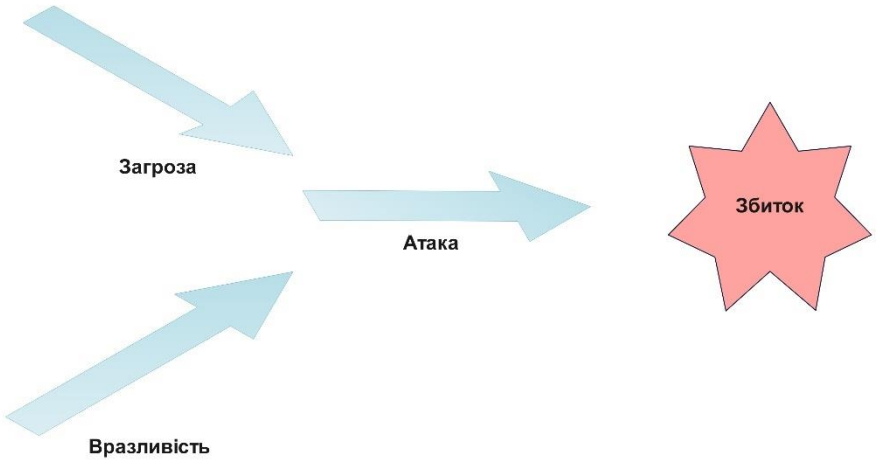


Рис. 1.5. Логічний зв'язок між поняттями «вразливість», «загроза», «атака», «збиток»

Тобто цілком можлива ситуація, коли система має певну вразливість, але ця вразливість ще не стала відомою зловмисникам – в даному випадку відповідна

загроза відсутня, а значить, і атака не може бути проведена. Аналогічно, існування загальновідомої загрози не тягне ніякої небезпеки для системи, в якій немає відповідної вразливості. Наприклад, поява інформації про деяку помилку в коді ОС Windows, може породити загрозу, але атака не здійсниться, якщо ця вразливість буде швидко усунена.

Таким чином, будь-яка загроза спрямована на пошук і/або використання вразливостей системи. У деяких випадках зловмисник працює «на дотик», намагаючись виявити той чи інший дефект системи. Система реагує на такого роду загрози відображенням повідомлень про дрібні, але дивні неполадки, а також флуктуаціями в статистичних характеристиках роботи системи, на підставі яких адміністратор мережі або фахівець з безпеки може запідозрити підготовку атаки.

Інші загрози виражаються в чіткій послідовності дій і мають формалізоване втілення у вигляді **експлойта** (Exploit – експлуатувати) – це програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака). Особлива небезпека експлойта полягає в тому, що, маючи його в своєму розпорядженні, навіть малопідготовлений хакер здатний провести успішну атаку. Для цього йому досить зайти на один з численних сайтів, що постачають всіх бажаючих своєю «продукцією». Більш того, на додачу до інструкцій і програм в Інтернеті можна знайти навіть пропозиції про здачу в оренду цілих бот-мереж, готових до реалізації потужних кібератак.

Бот-мережа, або **ботнет** (Botnet) – це організована сукупність комп'ютерів, пов'язаних через Інтернет і здатних узгоджено вирішувати завдання, поставлені перед ними зловмисником.

У той же час, наявність у експлойтів фіксованих ознак, таких, наприклад, як специфічні кодові послідовності, полегшує розпізнавання і відображення відповідних атак.

Загрози можуть виходити як від легальних користувачів мережі, так і від зовнішніх зловмисників. В останні роки в статистиці порушень безпеки зафіксований різкий зсув від зовнішніх до внутрішніх загроз. Приблизно дві третини від загального числа всіх найбільш серйозних інцидентів, пов'язаних з безпекою, складають порушення або помилки легальних користувачів мережі: співробітників і клієнтів підприємств, студентів, які мають доступ до мережі навчального закладу, та ін.

Загрози з боку легальних користувачів можуть бути як навмисними, так і ненавмисними. До **навмисних** загроз відносяться, наприклад, доступ і

викрадення конфіденційних даних, моніторинг системи з метою отримання інформації про її будову, відвідування заборонених веб-сайтів, винос за межі підприємства знімних носіїв і т. п. Безпека може бути порушена і в результаті **ненавмисних** порушень користувачів і обслуговуючого персоналу – помилок, що призводять до пошкодження мережевих пристроїв, даних, програмного забезпечення, ОС і додатків, безпечності в забезпеченні таємності паролів і ін. Відомо, що правильне конфігурування пристроїв є одним з потужних засобів забезпечення безпеки. Але будучи виконаною з помилками, ця операція здатна обернутися загрозою. Так, деякі «атаки» на ІС були насправді не атаками, а помилками адміністраторів мереж при виконанні конфігурації елементів системи.

Загрози зовнішніх зловмисників, яких називають також **хакерами**, за визначенням є навмисними і зазвичай кваліфікуються як злочини. Серед зовнішніх порушників безпеки зустрічаються люди, що займаються цією діяльністю професійно або просто з хуліганських спонукань.

1.4. Збиток та ризик. Управління ризиками.

Відомо, що абсолютна безпека інформаційної системи не може бути забезпечена ніякими засобами: завжди є ймовірність появи помилок і проведення нових атак з боку зловмисників. Тому, метою забезпечення інформаційної безпеки є не виняток, а мінімізація можливого негативного впливу, який можуть надати на систему існуючі загрози. З цього також випливає, що треба якимось чином ранжувати загрози, щоб вирішити, якими з них можна знехтувати, а на які звернути основну увагу.

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

В якості збитку розглядаються не тільки і не стільки втрати, що пов’язані з відновленням роботи ІС, зокрема серверів, файлової системи або системи автентифікації, – головна увага має бути приділена втратам, які в результаті цих порушень понесло підприємство, яке будує свій бізнес на базі цієї ІС.

Найважливішим завданням забезпечення інформаційної безпеки є управління ризиками. **Ризик** визначається як оцінка збитку від атаки з урахуванням ймовірнісної природи атаки. Іншими словами, ризик характеризується парою:

{Збиток від атаки, Імовірність атаки}.

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.

Управління ризиками включає три укрупнених етапи (рис 1.6.):

1. Аналіз вразливостей.
2. Оцінка ризиків.
3. Управління ризиками, або ризик-менеджмент (прийняття конкретних заходів).

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.). Перелік загроз формулюється приблизно, тобто з використанням ймовірнісних категорій.

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.

Ризик-менеджмент – по кожному ризику вживаються заходи з наступного списку:

- **Ухвалення ризику**. Цей варіант стосується неминучих атак, що завдають прийнятний збиток.
- **Усунення ризику**. Даний варіант має місце, коли існуючий ризик можна звести нанівець усуненням або вразливості (наприклад, зробити код комерційного програмного продукту відкритим), або загрози (встановити антивірусну систему).
- **Зниження ризику**. Якщо ризик неможливо ні прийняти, ні усунути, вдаються до дій щодо його зниження. Наприклад, завжди існує певна ймовірність проникнення зловмисників в систему шляхом підбору паролів. В такому випадку ризик несанкціонованого доступу можна знизити, встановивши більш суворі вимоги до довжини і змінюваності паролів.
- **Перенаправлення ризику**. Якщо ризик неможливо ні прийняти, ні усунути, ні навіть істотно знизити, то ризик може бути перенаправлений страховій компанії.

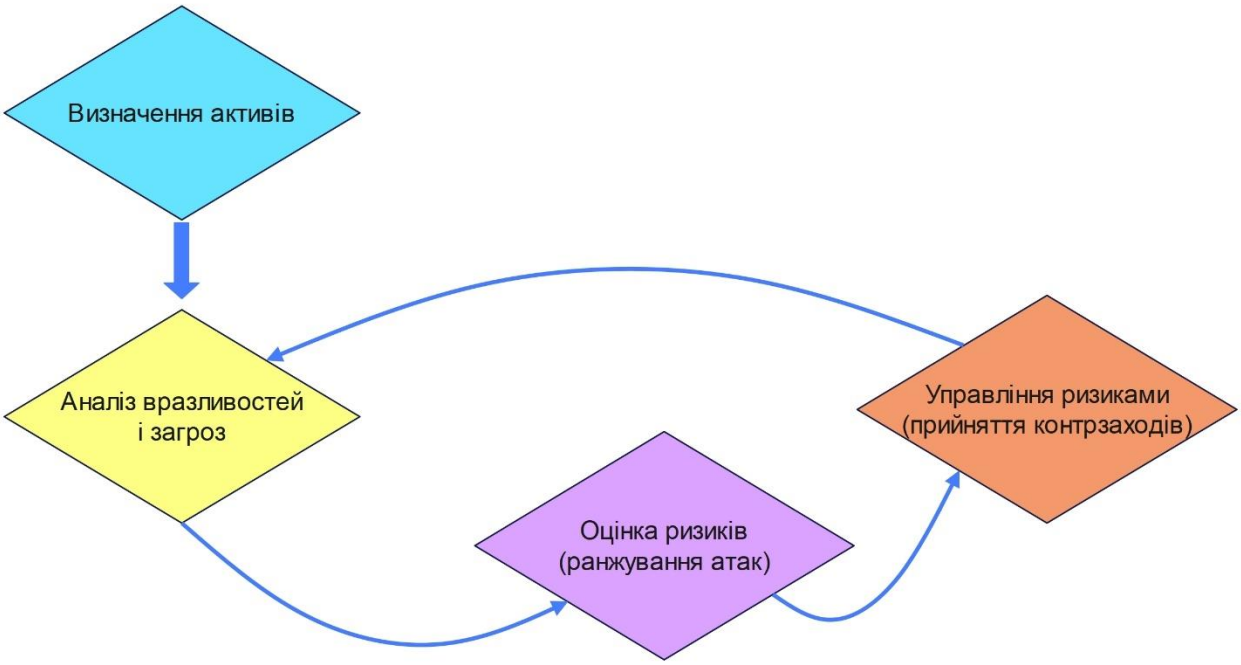


Рис. 1.6. Управління ризиками

1.5. Типи і приклади атак

1.5.1. Пасивні і активні атаки

Атаки поділяють на активні і пасивні.

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.

Багато активних кібератак відносять до типу **зламування** (breaking-in). Після виконання таких атак залишаються сліди «злому»: наприклад, змінюється вміст пам’яті, надходять дивні діагностичні повідомлення, додатки починають виконуватися неправильно, уповільнено або взагалі зависають, в характеристиках мережевого трафіку і в інших статистичних даних про роботу системи з’являються незрозумілі сплески активності. Однак, бувають випадки, коли в інформаційній системі ретельно підготовлена активна атака може пройти непоміченою, якщо фахівці, що відповідають за її безпеку, погано інформовані про можливі наслідки такого роду атак.

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.

На практиці рідко мають справу з активною або пасивною атакою «в чистому вигляді». Найчастіше атака включає підготовчий етап збору інформації про атаковану систему (пасивна атака), а потім на основі зібраних даних здійснюється активне втручання в її роботу (активна атака). До корисної для хакера інформації відносяться типи ОС і додатків, IP-адреси, номера портів, імена і паролі користувачів. Частина такого роду інформації може бути отримана при аналізі відкритої інформації або простому спілкуванні з персоналом (це називають **соціальним інжинірингом**), а частина – за допомогою певних програм. В останньому випадку використовується інша послідовність етапів: спочатку виконується активна фаза впровадження на атаковану систему прослуховуючої програми, потім період пасивного збору інформації (наприклад, паролів користувачів), а потім знову активна фаза проникнення в систему.

Розглянемо кілька типів популярних атак: відмова в обслуговуванні, спуфінг, впровадження коду, крадіжка особистості, фішинг, мережева розвідка. Більш детально ці, а також інші типи атак розглянемо на наступних лекціях.

1.5.2. Відмова в обслуговуванні

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.

При DoS-атаці використовується той простий факт, що комп'ютер під'єднаний до мережі – саме це є, в даному випадку, вразливістю.

На жаль, для більшості сучасних користувачів усунути цю вразливість простим від'єднанням комп'ютера від Інтернету не можна, хоча в деяких випадках, які потребують особливо високого рівня безпеки, так і чинять.

Зловмисник може багаторазово посилити ефект від проведення DoS-атаки шляхом крадіжки чужої обчислювальної потужності. Для цього він отримує контроль над атакуючим комп'ютером, завантажує в нього шкідницьке програмне забезпечення і активує його. Таким чином зловмисник непомітно для власника «розгалужує» частину обчислювальної потужності. При цьому власникові комп'ютера не завдається ніякої іншої шкоди, крім зниження продуктивності його комп'ютера. Для проведення потужної атаки зловмисник захоплює контроль над деякою кількістю комп'ютерів, організовує їх узгоджену роботу і направляє сумарний потік запитів на комп'ютер-жертву.

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.

При проведенні атак зловмисникові важливо не лише досягти своєї мети, що полягає в заподіянні шкоди атакованому об'єкту, але і знищити всі сліди своєї участі в цьому. Одним з основних прийомів, що використовується зловмисниками для «замітання слідів», є підміна вмісту пакетів, або **спуфінг** (spoofing). Зокрема, для приховування місця джерела шкідливих пакетів (наприклад, при DoS-атаці) зловмисник змінює значення поля адреси відправника в заголовках пакетів. Оскільки адреса відправника генерується автоматично системним програмним забезпеченням, зловмисник вносить зміни у відповідні програмні модулі так, щоб вони давали йому можливість

відправляти зі свого комп'ютера пакети з будь-якими IP-адресами. Ще важче визначити адресу джерела розподіленої атаки, так як безпосередніми виконавцями виступають «зомбовані» комп'ютери і саме їх адреси містяться в полі адреси відправника пакетів, що бомбардують комп'ютер-жертву. І хоча власники комп'ютерів-виконавців нічого не підозрюють, вони, тим не менше, стають учасниками розподіленої атаки, і тому велика частина відповідальності лягає і на них. Адже саме їх недоробки в справі забезпечення безпеки власних систем уможливили цю атаку.

Отже, існує два типи DoS/DDoS-атак, і найбільш поширена з них заснована на ідеї флуду, тобто завалення жертви величезною кількістю пакетів.

Технічний флуд (його ще називають IRC flood) є розподіленою DDoS-атакою на певний ресурс (у вигляді великої кількості запитів), яке викликає відмову в обслуговуванні.

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.

Ботнет (botnet від robot і network) – це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами – автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмиснику виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай, вони використовуються для протиправної діяльності – розсилки спаму, перебору паролів на віддаленій системі, DoS-атак, отримання персональної інформації про користувачів, крадіжка номерів кредитних карт та паролів доступу.

Флешмоб (flash mob – спалахуючий натовп) – це заздалегідь спланована масова акція, зазвичай організована через Інтернет або інші засоби комунікації, у якій велика кількість людей оперативно збирається у громадському місці, протягом декількох хвилин виконує заздалегідь узгоджені дії (сценарій), і потім швидко розходяться.

1.5.3. 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 троянські та шпигунські програми, руткіти, черв'яки, віруси, спам, логічні бомби і ін.

Ці програми можуть проникати на атаковані комп'ютери різними шляхами. Найпростіший з них – «самодоставка», коли користувач завантажує файли з неперевірених джерел (знімних носіїв або веб-сайтів) або безтурботно відкриває підозрілий файл, який прийшов до нього як додаток по електронній пошті. Існують і більш складні представники шкідливих програм, що володіють власними механізмами «розмноження», копії таких програм поширюються по комп'ютерах мережі без участі користувачів.

Одним із прикладів шкідливих програм є **шпигунські програми** (Spyware), які таємно (як правило, віддалено) встановлюються зловмисниками на комп'ютери користувачів, щоб відстежувати і фіксувати всі їхні дії. У число таких дій може входити введення імені і пароля під час логічного входу в систему, відвідування тих чи інших веб-сайтів, обмін інформацією з зовнішніми і внутрішніми користувачами мережі та ін. Зібрана інформація пересилається зловмисникові, який застосовує її в злочинних цілях.

В якості шпигунських програм можуть використовуватися не лише створені спеціально для цих цілей шкідливі програми, але і програми легального призначення. Так, небезпечним засобом шпигунства можуть стати легальні системи моніторингу мережі, такі, наприклад, як популярні мережеві монітори Wireshark або Microsoft Network Monitor. Основне призначення цих програм полягає в тому, щоб надати адміністратору мережі можливість стежити за вхідними та вихідними даними, зокрема захоплювати пакети, використовуючи механізм фільтрації, переглядати їх вміст, збирати статистику по завантаженню пристроїв. В руках зловмисника така програма перетворюється в потужний інструмент злому мережі, який дозволяє перехоплювати пакети з паролями і іншою секретною інформацією.

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. До цієї категорії входять програми, що здійснюють різні несанкціоновані користувачем дії: збір інформації і її передачу зловмисникові, її руйнування або

зловмисну модифікацію, порушення працездатності комп'ютера, використання ресурсів комп'ютера в непристойних цілях.

Троянські програми поширюються людьми – або безпосередньо завантажуються в комп'ютерні системи зловмисниками-інсайдерами, або спонукають користувачів завантажувати і/або запускати їх на своїх системах.

Для досягнення останнього троянські програми поміщаються зловмисниками на відкриті або індексовані ресурси (файл-сервери і системи файлообміну), носії інформації, надсилаються за допомогою служб обміну повідомленнями (наприклад, електронною поштою), потрапляють на комп'ютер через недосконалість безпеки або завантажуються самим користувачем з адрес, отриманих одним з перерахованих способів.

Руткіт (Root Kit – набір root-a) – програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі. Цей набір, як правило, включає всілякі утиліти для «замітання слідів» вторгнення в систему, сніфери, сканери, кейлогери, троянські програми і ін. Даний механізм дозволяє зловмиснику закріпитися в зламаній системі і приховати сліди своєї діяльності шляхом приховування файлів, процесів, а також самої присутності руткіта в системі.

Кейлогер (Keylogger – скорочення від key – клавіша та logger — реєструючий пристрій) – це програмний продукт або апаратний пристрій, що реєструє кожне натиснення на клавішу клавіатури комп'ютера.

Мережевий черв'як – шкідлива програма, яка самостійно розповсюджується через локальні і глобальні комп'ютерні мережі.

Всі механізми поширення хробаків діляться на дві великі групи:

- Використання вразливостей і помилок адміністрування в програмному забезпеченні, встановленому на комп'ютері. Наприклад, шкідлива програма Conficker для свого поширення використовувала вразливість в операційній системі Windows; черв'як Морріса підбирав пароль по словнику. Такі черв'яки здатні поширюватися автономно, вибираючи і атакуючи комп'ютери в повністю автоматичному режимі.
- Використовуючи засоби соціальної інженерії, провокується запуск шкідливої програми самим користувачем. Щоб переконати користувача в тому, що файл безпечний, можуть підключатися недоліки інтерфейсу користувача програми – наприклад, черв'як VBS.LoveLetter використовував той факт, що Outlook Express приховує розширення файлів. Даний метод широко застосовується в спам-розсилках, соціальних мережах і т. д.

Іноді зустрічаються черв'яки з цілим набором механізмів поширення, стратегій вибору жертви, і навіть експлойтів під різні операційні системи.

Логічна бомба (Logic bomb) – програма, яка запускається при певних часових або інформаційних умовах для здійснення шкідливих дій (як правило, несанкціонованого доступу до інформації, спотворення або знищення даних).

Багато шкідливих програм, такі як віруси або черв'яки, часто містять логічні бомби, які спрацьовують в заздалегідь заданий час (логічні бомби з часовими механізмами) або при виконанні певних умов, наприклад, в п'ятницю 13-го, день сміху або в річницю аварії на Чорнобильській АЕС (CIH вірус).

До логічних бомб, як правило, відносять код, який призводить до неповідомлених заздалегідь наслідків для користувачів. Таким чином, відключення певної функціональності або закінчення роботи умовно-безкоштовних програм, після завершення встановленого періоду, не рахується логічної бомбою.

Комп'ютерний вірус (Computer Virus) – шкідлива програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Необізнані користувачі помилково відносять до комп'ютерних вірусів також інші види зловмисного ПЗ – програми-шпигуни чи навіть спам. За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні поширення комп'ютерних вірусів переслідується і карається відповідно до Кримінального кодексу (статті 361, 362, 363).

Спам (Spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів.

1.5.4. Соціальний інжиніринг

У міру розвитку послуг, що надаються через Інтернет, все більш популярними стають афери, коли одна людина видає себе за іншу. Адже в цьому випадку не потрібна особиста присутність в офісі, і індивідуум доводить свою ідентичність, передаючи обслуговуючому центру свої персональні дані по телефону або використовуючи інтерактивну систему веб-сайту. Зловмисник

вирішує видати себе за іншого, щоб, наприклад, взяти кредит на чуже ім'я, отримати доступ до чужого рахунку, розрахуватися за купівлю чужою карткою, отримати іменне запрошення на закритий захід. Таку пасивну атаку, яка полягає в зборі даних про іншу людину, називають **крадіжкою особистості** (Identity Theft).

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. Шахраї використовують усілякі механізми, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані. Людина може відповісти на телефонний дзвінок, і зловмисник, який представився співробітником банку або державної податкової інспекції, працівником ЖКГ або представником провайдера мобільного зв'язку, починає випитувати критичні дані про неї. Загроза може прийти і по електронній пошті, наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

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.

Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно іменується «**антифішинг**».

Наступним винаходом стали спливаючі вікна. Припустимо, клієнт отримує доступ до сайту свого банку (справжньому) в результаті проходження стандартної процедури ідентифікації і автентифікації. Він переглядає сторінки сайту – немає ніяких сумнівів, що це реальний сайт. У якийсь момент на екрані з'являється спливаюче вікно, яке стилістично виглядає як невід'ємна частина сайту. У цьому вікні розміщено інтерактивну форму, яка запитує персональні дані. Клієнт відчуває себе в цілковитій безпеці і вводить всі запитувані критичні дані. Однак справжній сайт банку є тільки фоном, на якому розташовуються вікна-пастки зловмисника.

Метою фішерів сьогодні є клієнти банків і електронних платіжних систем. І якщо перші листи відправлялися випадково, в надії на те, що вони дійдуть до

клієнтів потрібного банку або сервісу, то зараз фішери можуть визначити, якими послугами користується жертва, і застосовувати цілеспрямовану розсилку. Частина останніх фішингових атак була направлена безпосередньо на керівників і інших людей, що займають високі пости в компаніях.

Соціальні мережі також представляють великий інтерес для фішерів, дозволяючи збирати особисті дані користувачів. За оцінками фахівців, понад 70% фішингових атак в соціальних мережах – успішні

За даними компанії PhishMe, станом на березень 2016 року 93% всіх фішингових листів намагались заразити комп'ютер жертви шкідливими програмами криптографічного здирництва (ransomware) – вони шифрують дані на жорсткому диску та вимагають гроші від жертви за їхнє розшифрування.

1.6. Ієрархія засобів захисту від інформаційних загроз

1.6.1. Засоби безпеки законодавчого рівня

Зазвичай перше, що асоціюється з інформаційною безпекою (ІБ), – це антивірусні програми, фаєрволи, системи шифрування, автентифікації, аудиту та інші технічні засоби захисту. Безперечно, роль цих засобів у забезпеченні безпеки велика, проте не менше, а іноді і більший вплив на безпеку системи надають засоби, побудовані на якісно іншій основі.

Відеокамера і надійний замок в офісі, продумана процедура прийому співробітників на роботу, закон, що загрожує хакеру кримінальним переслідуванням, стандарт, що допомагає провести аналіз можливих збитків через дії порушника, – всі ці, мало схожі між собою засоби, однаково важливі для забезпечення безпеки.

Успіх в області інформаційної безпеки може принести тільки системний підхід, при якому засоби захисту різних типів застосовуються спільно і під централізованим управлінням.

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 (рис. 1.7).

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. Наприклад, вихід Закону «Про персональні дані», що регламентує заходи щодо забезпечення безпеки персональних даних при їх обробці, вимагає від багатьох підприємств перегляду та внесення принципових змін в процедури і

інфраструктуру обробки інформації. Не менш принциповими можуть виявитися вимоги сертифікації засобів захисту даних, які передбачається використовувати в проектованій системі забезпечення безпеки, або необхідність отримання ліцензії для обраного виду діяльності.

Рис. 1.7. Багаторівнева модель засобів захисту від інформаційних загроз

Інформаційні технології пронизують наше життя, тому цілком природно, що правовідносини в даній сфері вже давно регулюються розвиненим законодавством. Учасниками правовідносин є суб'єкти правовідносин, до яких в області інформаційної безпеки можна віднести власників та споживачів інформації, власників інтернет-сайтів, провайдерів телекомунікаційних мереж, розробників програмних і апаратних засобів інформаційних технологій та ін.

Права і обов'язки суб'єктів правовідносин визначаються по відношенню до об'єктів правовідносин, до яких належать, наприклад, ІС (державні і приватні), засоби захисту інформації (алгоритми шифрування, апаратні ключі, які використовуються для автентифікації, і т. п.), послуги, що надаються в області ІБ, інформація обмеженого доступу, в тому числі інформація, яка становить державну, комерційну, банківську, сімейну таємницю, таємницю листування, персональні дані та ін.

Необхідність захисту інформаційних ресурсів і підтримуючої їх інфраструктури диктується як нашими правами на захист (наприклад, кожному громадянину має бути забезпечений захист від розкриття його персональних даних), так і обов'язками її захищати (кожна організація, що оперує персональними даними, зобов'язана захищати їх від розкриття).

Нормативно-правовий акт – це офіційний документ, прийнятий компетентним правотворчим органом і встановлює загальнообов'язкове державне розпорядження, розраховане на багаторазове застосування. Сукупність усіх нормативно-правових актів, що діють на території країни, прийнятих законодавчим (представницьким) органом, називається **законодавством**.

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).

До числа порушень законодавства в області ІБ відносять як традиційні «комп'ютерні» злочини, такі як порушення доступності даних (DoS-атаки), використання шкідливого ПЗ, перевищення привілеїв, несанкціонований доступ та ін., так і порушення регламентуючих правил, наприклад відсутність ліцензії на певний вид діяльності в області захисту інформації, використання несертифікованих продуктів там, де це вимагається законом (наприклад, засобів шифрування при роботі з інформацією, що становить державну таємницю).

Важливим напрямком законодавства в області безпеки є стандартизація.

Стандарти регулюють найрізноманітніші сфери і аспекти забезпечення інформаційної безпеки, в тому числі теоретичні концепції та алгоритми, вимоги до програмних і апаратних засобів, методики обстеження систем і порядок документування результатів, адміністративні процедури. Стандартні процедури оцінки систем дають можливість їх співставлення і порівняння, на підставі чого може виконуватися сертифікація систем на відповідність певним вимогам. Стандарти безпеки визначають перелік тих властивостей і функцій, наявність яких є необхідною для того, щоб певна система обробляла інформацію безпечним чином.

До числа найвідоміших сертифікаційних стандартів відносять **Помаранчеву книгу** (формальна назва цього стандарту: «Міністерство оборони США. Критерії оцінки довірених комп'ютерних систем»). Цей популярний стандарт оцінює ступінь захищеності ОС, а також дозволяє формалізувати процедуру оцінки, для чого в ньому визначаються формальні критерії віднесення системи до певного класу безпеки. Вперше цей стандарт був опублікований в 1985 році в складі так званої райдужної серії стандартів інформаційної безпеки, що видавалася в період з 1980 по 1990 рік під егідою Міністерства оборони США. Всі 37 книг цієї серії мали обкладинки різних кольорів. Саме колір обкладинки дав другу, неформальну, назву – «Помаранчева книга».

Сьогодні 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).

Слід згадати також **Червону книгу** – ще один стандарт з «кольорової» серії, який являє собою інтерпретацію Помаранчевої книги для конфігурації мережі. Однак обидва ці стандарту не є міжнародними, до того ж їх застосовність обмежена тільки операційними системами. Ці обмеження певною мірою знімає міжнародний стандарт, відомий під короткою (неофіційною) назвою **Загальні критерії** і дозволяє оцінювати і сертифікувати програмні продукти різних класів.

1.6.2. 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.

При побудові інформаційного захисту не можна цілком покладатися на технічні засоби – ніякі найсучасніші фаєрволи, системи виявлення вторгнень, сканери вразливостей, централізовані сервери автентифікації не захистять організацію, якщо не буде вироблена керівна ідея, яка перетворює набір окремих потужних, але часто не дуже ефективних інструментів і методів в інтегровану систему, що працює на досягнення спільної мети.

Політика – це загальне керівництво, яке встановлює головні напрямки, в яких потрібно рухатися, щоб найбільш раціональним шляхом досягти поставленої мети. Зміст політики виражається в її цілях, програмах і цінностях, у проблемах і завданнях, які вона вирішує, в мотивах, механізмах, способах і методах прийняття і реалізації рішень.

Сферою застосування політики може бути будь-яка цілеспрямована діяльність, в тому числі політика інформаційного захисту підприємства, яку прийнято називати **політикою безпеки** (ПБ). У сфері інформаційних технологій застосовують політики і в інших більш вузьких сферах: наприклад, політика інформаційної захисту комп'ютерних систем підприємства, політика використання коштів комунікацій, політика використання корпоративної електронної пошти і т. п.

Як і будь-яка політика, ПБ покликана відігравати організуючу і дисциплінуючу роль. Процес вироблення ПБ призводить до більш чіткого усвідомлення цілей і шляхів побудови стратегії забезпечення інформаційної безпеки (СЗІБ).

Політика безпеки розробляється із залученням вищого керівництва. Тим самим керівники демонструють свою підтримку пропонованої стратегії забезпечення інформаційної безпеки, що має велике значення, так як її реалізація може зажадати залучення значних фінансових коштів і ресурсів підприємства. Будучи прийнятою, ПБ стає «законом», обов'язковим для виконання всіма співробітниками підприємства. Персонал підприємства повинен бути ознайомлений з положеннями ПБ, в тому числі з відповідальністю, яка визначена за її порушення.

Політика безпеки фіксується в документах. Часто під політикою розуміють саме її документальне вираз. Таким чином, можна дати наступне визначення:

Політика безпеки – це сукупність документованих правил, процедур, практичних прийомів або керівних принципів в області безпеки інформації, якими керується організація у своїй діяльності.

Рішення, які повинні бути прийняті в рамках розробки політики безпеки підприємства, а також документи, які їх описують, можуть бути віднесені до верхнього, середнього або нижнього рівня.

Верхній рівень політики безпеки включає рішення, що стосуються підприємства в цілому. Вони приймаються вищим керівництвом, носять загальний характер, можуть бути описані компактним документом. На цьому рівні виконується всебічне обстеження підприємства: виявляються критично важливі активи, які найбільше потребують захисту, встановлюються правила розмежування доступу до інформаційних ресурсів, визначаються найбільш ймовірні загрози, оцінюються можливі втрати, приймаються концептуальні рішення щодо методів забезпечення захисту. Тобто, *значна частина ПБ базується на результатах аналізу ризиків*. На верхньому рівні приймаються організаційно-адміністративні рішення, а саме: визначаються посадові позиції (ролі), створюються адміністративні підрозділи, комітети, робочі групи, функціями яких є втілення політики безпеки в життя, встановлюються межі відповідальності всіх цих адміністративних одиниць. ПБ верхнього рівня може містити вказівки на прихильність підприємства певним стандартам і нормативно-правовим актам, принципи навчання персоналу, порядок реагування на порушення режиму безпеки та ін.

До **середнього рівня** політики безпеки відносять рішення і відповідні документи, що стосуються приватних аспектів інформаційної безпеки, таких, наприклад, як політика використання засобів криптографічного захисту, політика антивірусного захисту, політики моніторингу та менеджменту інцидентів інформаційної безпеки, політика захисту комунікаційних каналів, політика фізичного захисту та ін. У порівнянні з верхнім рівнем розробка ПБ середнього рівня вимагає більшої участі технічних фахівців (з числа керівників). Зазвичай, в ПБ середнього рівня існують повідомлення про заборонені дії і покарання за них. Наприклад, в рамках ПБ комп’ютерної інфраструктури підприємства передбачаються заходи, що захищають мережу від вірусів і інших шкідливих програм. Для цього в ПБ включаються пункти про заборону персоналу встановлювати і запускати ПЗ без його попереднього тестування, про необхідності його регулярного оновлення, про регламентацію використання в корпоративній мережі власного обладнання співробітників (ноутбуків, планшетів, USB-накопичувачів, флеш- карт) та інші подібні заходи.

Політика безпеки **нижнього рівня** визначає дії щодо забезпечення безпеки на рівні мережевих сервісів і може являти собою керівництва, інструкції, регламенти і правила, пов’язані з адмініструванням і використанням сервісів. На відміну від двох верхніх рівнів, багато положень яких носять загальний характер,

на нижньому рівні наводяться більш детальні, більш формалізовані рекомендації, що враховує особливості конкретного сервісу.

Кожен документ вищого рівня розкривається і доповнюється одним або декількома документами нижчого рівня. Чим вищий рівень документа, тим більш компактним і декларативним він є. Кордон між рівнями є умовним: так, наприклад, документи середнього рівня ПБ, що описують приватні реалізації політики, можуть частково включати в себе політику захисту сервісів, тобто політику нижнього рівня.

1.6.3. 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.

Будь-який аспект інформаційної безпеки передбачає використання коштів процедурного рівня. Навіть просте підтримання нормального режиму роботи інформаційної системи здійснюється за рахунок виконання безлічі повсякденних процедур: резервного копіювання, управління програмним забезпеченням, профілактичних робіт і т. п. Багато процедур включають в себе застосування технічних засобів. Наприклад, завдання обліку різних ресурсів (документації, програм, обладнання та ін.), як правило, вирішується із залученням спеціально розроблених для цих цілей програм. До засобів процедурного рівня відноситься також фізичний захист: пропускний режим на територію підприємства, охорона кордонів території і ін.

У загальному випадку **процедура** – це взаємопов’язана послідовність дій, спрямована на вирішення деякої задачі. Процедура може бути формальною, як, наприклад, при її поданні у вигляді алгоритму або програми на мові програмування, так і неформальної, у вигляді певної міри розпливчастих вказівок. Формальні процедури можуть бути реалізовані механічними або електронними пристроями. В умовах неформальних процедур, коли неможливо абсолютно однозначно визначити всі деталі процедури, а саме така більшість процедур безпеки (підтримка працездатності системи, управління персоналом, фізичним захистом, управління документацією і ін.), може діяти лише людина.

Саме тому між рівнями стратегій безпеки і технічних засобів (здатних реалізовувати тільки формальні процедури) за необхідності з’являється проміжний рівень неформальних процедур, які приводяться в дію людиною.

Виконавцями процедур є IT-фахівці, співробітники відділів інформаційної безпеки, користувачі і інші співробітники, що пов’язані з інформаційним захистом.

Управління персоналом включає підбір персоналу, прийом на роботу, звільнення, поточний контроль і ін. Кожна з перерахованих дій має відношення до безпеки. При підборі працівників слід перевіряти минуле кандидатів, їх рекомендації, в деяких випадках потрібна додаткова перевірка професійних сертифікатів, кредитної історії, записів в базах даних про злочинців, інші більш ретельні перевірки.

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. Приклад такої процедури – доступ до банківського сейфу, який відкривається двома ключами: ключем власника вмісту комірки і ключем представника банку.

Правило обов’язкової відпустки, крім турботи про здоров’я співробітника, дає можливість в його відсутність ґрунтовно перевірити, чи немає порушень в його роботі (однією з непрямих ознак цього може служити зникнення певної проблеми одночасно з його виходом у відпустку), а також чи не використовує деякий зловмисник його обліковий запис (доказом цього служать записи в журналі реєстрації подій, пов’язані з обліковим записом співробітника, після його виходу у відпустку).

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.

1.6.4. 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.

1.7. Криптографія

1.7.1. Основні визначення

Криптографія (від грецького *kryptós* – прехований і *gráphein* – писати) – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Виникла з практичної потреби передавати важливі відомості надійним методом. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри.

Термінологія:

Відкритий (вихідний) текст – дані (не обов’язково текстові), які передаються без використання криптографії.

Шифрування – процес застосування криптографічного перетворення відкритого тексту (інформацію, над якою виконуються процедури шифрування і дешифрування умовно будем називати «текстом») на основі алгоритму і ключа, в результаті якого виникає шифрований текст.

Дешифрування – процес застосування криптографічного перетворення для шифрованого тексту, щоб привести його у вихідний стан.

Шифротекст, шифрований (закритий) текст – дані, отримані після застосування криптосистеми (зазвичай з деяким вказаним ключем).

Ключ – параметр шифру, визначальний вибір конкретного перетворення цього тексту. У сучасних шифрах криптографічна стійкість шифру цілком визначається секретністю ключа (принцип Керкгоффса).

Шифр, криптосистема – сімейство зворотних перетворень відкритого тексту в шифрований.

Асиметричний шифр – шифр, що є асиметричною криптографічною системою.

Криптоаналіз – наука, що вивчає математичні методи порушення конфіденційності і цілісності інформації.

Криптоаналітик – людина, що створює і застосовує методи криптоаналізу.

Криптографічна стійкість – здатність криптографічного алгоритму протистояти криптоаналізу.

Шифрування є наріжним каменем усіх служб інформаційної безпеки, будь то система автентифікації або авторизації, захищений канал або засоби безпечного зберігання даних.

Пара процедур – шифрування і дешифрування – називається **криптосистемою**. Зазвичай криптосистема передбачає наявність спеціального елемента – **секретного ключа**.

В якості ключа може виступати деякий предмет, число або малюнок.

Криптосистема вважається розкритою, якщо знайдена процедура, що дозволяє підібрати ключ за реальний час. Методи розкриття криптосистеми, процедури виявлення вразливості криптографічних алгоритмів, з'ясування секретного ключа називають **криптоаналізом**, або зломом шифру. Спробу розкриття конкретного шифру із застосуванням методів криптоаналізу називають **криптографічною атакою**.

Наприклад, класичним методом криптоаналізу, що застосовується для розкриття шифрів, заснованих на перестановці або заміні букв, є частотний аналіз. Для текстів, написаних певною мовою, що відносяться до певної сфери знань, існують стійкі статистичні дані про частоту, з якою зустрічається в тексті та чи інша буква або послідовність літер, включаючи деякі слова. Володіючи такими даними і провівши статистичний аналіз зашифрованого тексту, можна виконати зворотну заміну символів.

Складність алгоритму розкриття є однією з важливих характеристик криптосистеми і називається **криптостійкістю**. У криптографії прийнято **правило Керкгоффса**, яке полягає в тому, що *стійкість шифру повинна визначатися тільки секретністю ключа*. Так, всі стандартні алгоритми шифрування (наприклад, AES, DES, PGP) широко відомі, їх детальний опис міститься в легкодоступних документах, але від цього їх ефективність не знижується. Система залишається захищеною, навіть якщо зловмиснику відомо все про алгоритм шифрування, але він не знає секретний ключ.

Існує два класи криптосистем – **симетричні** і **асиметричні**. У симетричних схемах шифрування (класична криптографія) секретний ключ шифрування збігається з секретним ключем дешифрування. В асиметричних

схемах шифрування (криптографія з відкритим ключем) ключ шифрування не збігається з ключем дешифрування.

1.7.2. Історія криптографії

Історія криптографії налічує близько 4 тисяч років. В якості основного критерію періодизації криптографії можливо використовувати технологічні характеристики методів шифрування.

Перший період (приблизно з 3-го тисячоліття до н. е.) характеризувався пануванням **моноалфавітних шифрів** (основний принцип – заміна алфавіту початкового тексту іншим алфавітом через заміну букв іншими буквами або символами). Основними типами класичних шифрів того періоду були **перестановочні шифри**, які змінювали порядок літер в повідомленні, та **підстановочні шифри**, які систематично замінювали літери або групи літер іншими літерами або групами літер. Прості варіанти обох типів пропонували слабкий захист від досвідчених супротивників. Стеганографія також була розроблена в давні часи. Одна з перших згадок про її застосування датується V століттям до н. е.

Стеганографія – (з грецької steganos (секрет, таємниця) і graphy (запис)) – тайнопис, при якому повідомлення, закодоване таким чином, що не виглядає як повідомлення – на відміну від криптографії. Таким чином, звичайна людина принципово не може розшифрувати повідомлення — бо не знає про факт його існування.

Якщо криптографія приховує зміст повідомлення, то стеганографія приховує сам факт існування повідомлення.

До сучасних прикладів стеганографії належать невидимі чорнила, мікрокрапки, цифрові водяні знаки, що застосовуються для приховування інформації.

Другий період (з IX століття на Близькому Сході (Аль-Кінді) і з XV століття в Європі (Леон Баттіста Альберті) - до початку XX століття) ознаменувався введенням поліалфавітних шифрів.

Шифротексти, отримані від класичних шифрів, завжди видають деяку статистичну інформацію про текст повідомлення, що може бути використано для зламу. Після відкриття частотного аналізу (арабським вченим Аль-Кінді) в IX столітті, майже всі такі шифри стали більш-менш легко зламними досвідченим фахівцем.

Частотний аналіз – вид криптоаналізу, який ґрунтується на частоті появи знаків шифротексту.

Майже всі шифри залишались беззахисними перед частотним аналізом до винаходу Леона Баттіста Альберті, приблизно в 1467 році, поліалфавітного шифру. Винахід Альберті полягав в тому, щоб використовувати різні шифри (наприклад, алфавіти підстановки) для різних частин повідомлення.

Поліалфавітний шифр – симетричний алгоритм шифрування, який використовує більше ніж один алфавіт.

Прикладом такого шифру може служити **шифр Віженера**. В поліалфавітному шифрі Віженера, алгоритм шифрування використовує ключове слово, яке керує підстановкою літер в залежності від того, яка літера ключового слова використовується. В середині 1800-тих, Чарльз Беббідж показав, що поліалфавітні шифри цього типу залишились частково беззахисними перед частотним аналізом.

Третій період (з початку і до середини XX століття) характеризується впровадженням електромеханічних пристроїв в роботу шифрувальників. При цьому тривало використання поліалфавітних шифрів.

Декілька механічних шифрувально/дешифрувальних приладів було створено і запатентовано на початку XX століття, серед них роторні машини – найвідомішою серед яких була Енігма, автомат, що використовувався Німеччиною з кінця 20-тих і до кінця Другої світової війни. Поява комп'ютерів після Другої світової війни зробило можливим появу складніших шифрів, оскільки вони дозволяли шифрувати будь-які дані, які можна представити у двійковому виді, на відміну від класичних шифрів, які розроблялись для шифрування письмових текстів. Це зробило непридатними для застосування лінгвістичні підходи в криптоаналізі. Багато комп'ютерних шифрів можна характеризувати за їхньою роботою з послідовностями бінарних бітів (інколи в блоках або групах), на відміну від класичних та механічних схем, які, зазвичай, працюють безпосередньо з літерами. Однак, комп'ютери також знайшли застосування у криптоаналізі, що, в певній мірі, компенсувало підвищення складності шифрів. Тим не менше, хороші сучасні шифри залишались попереду криптоаналізу.

Четвертий період (з середини до 70-х років XX століття) – період переходу до математичної криптографії. У роботі Шенона з'являються строгі математичні визначення кількості інформації, передачі даних, ентропії, функцій шифрування. Обов'язковим етапом створення шифру вважається вивчення його вразливості до різних відомих атак – лінійному і диференціальному криптоаналізам. Проте, до 1975 року криптографія залишалася «класичною», або ж, коректніше, криптографією з секретним ключем.

Сучасний період розвитку криптографії (з кінця 1970-х років до теперішнього часу) відрізняється зародженням і розвитком нового напряму – криптографія з відкритим ключем.

Її поява знаменується не лише новими технічними можливостями, але і порівняно широким поширенням криптографії для використання приватними особами (у попередні епохи використання криптографії було винятковою прерогативою держави).

Сучасна криптографія утворює окремий науковий напрям на стику математики і інформатики – роботи в цій області публікуються в наукових журналах, організовуються регулярні конференції. Практичне застосування криптографії стало невід'ємною частиною життя сучасного суспільства – її використовують в таких галузях як електронна комерція, електронний документообіг (включаючи цифрові підписи), телекомунікації і інших.

1.8. Симетричне шифрування

1.8.1. Модель симетричного шифрування

При симетричному шифруванні вимагається, щоб усі сторони, що мають право на читання інформації, мали однаковий ключ. Це дозволяє звести загальну проблему безпеки інформації до проблеми забезпечення захисту ключа. Симетричне шифрування є широко використовуваним методом шифрування. Він забезпечує конфіденційність інформації і гарантію того, що інформація залишається незмінною в процесі передачі.

Симетричне шифруванням також називається **шифруванням з секретним ключем**, оскільки для шифрування і дешифрування даних використовується один і той самий ключ.

Симетричне шифрування забезпечує конфіденційність інформації в зашифрованому стані. Розшифрувати повідомлення можуть тільки ті особи, яким відомий ключ. Будь-яка зміна в повідомленні, внесена під час передачі, буде виявлена, оскільки після цього не вдасться правильно розшифрувати повідомлення. Шифрування з секретним ключем не забезпечує автентифікацію, оскільки будь-який користувач може створювати, шифрувати і відправляти повідомлення.

На рис 1.8 приведена модель симетричної криптосистеми. У даній моделі три учасника: два абонента, охочих, обмінюватися шифрованими повідомленнями, і зловмисник, який хоче перехопити і будь-яким чином розшифрувати повідомлення, що передаються.

При поясненні алгоритмів шифрування тут і далі будем називати учасників обміну Алісою і Бобом, а зловмисника, який намагається перехопити їх повідомлення, – Євою. Ці імена традиційно використовуються в криптографії.

У розпорядженні Аліси і Боба є незахищений канал передачі повідомлень, який в принципі може прослуховуватися зловмисником. Тому вони домовляються використовувати шифрування, і для цього їм потрібен секретний ключ, відомий тільки їм обом. Цей ключ їм був переданий (або один з них послав його іншому) заздалегідь по іншому каналу – надійному. Боб і Аліса, отримавши ключ, знаходяться в абсолютно однаковому (симетричному) положенні, кожен з них може як посилати шифровані повідомлення, так і отримувати і розшифровувати їх. Для визначеності на малюнку показана схема передачі повідомлень з боку Боба.

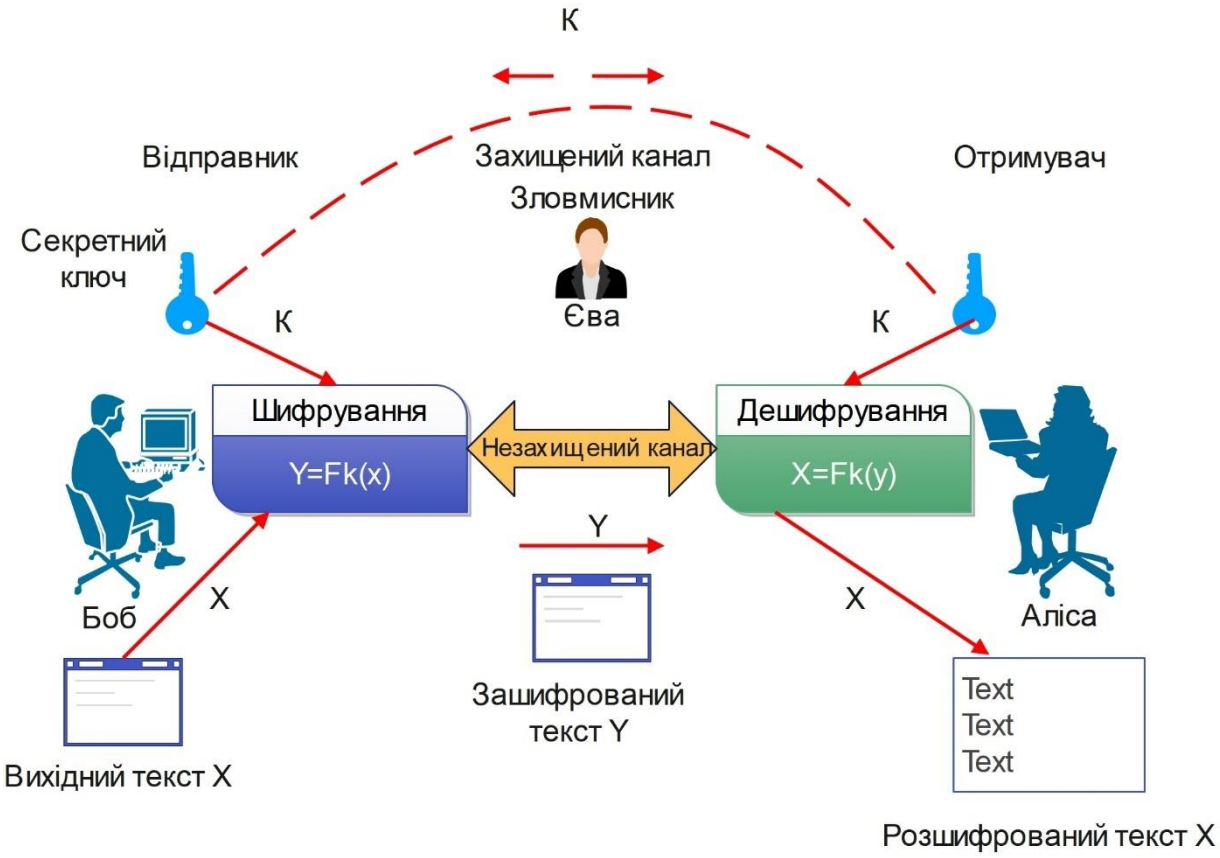


Рис. 1.8 Модель симетричного шифрування

Боб зашифровує своє повідомлення – відкритий текст X – функцією шифрування F з секретним ключем K і передає у відкритий канал, результат – шифрований текст Y. Аліса отримує Y і передає його на вхід функції дешифрування F', яка виконує в зворотному порядку всі дії, виконані раніше функцією F. Це може бути зроблено, тільки якщо на вхід функції збуде подано те ж саме значення параметра – значення ключа K. Аліса має секретний ключ і

тому отримує розшифроване значення. При необхідності передавати шифровані повідомлення Бобу Аліса повинна діяти аналогічним чином.

Загалом, шифрування з секретним ключем швидко і легко реалізується за допомогою апаратних або програмних засобів. Нижче описано основні алгоритми симетричного шифрування.

1.8.2. Основні алгоритми симетричного шифрування

Перестановочні шифри

Перестановочний шифр – алгоритм шифрування, який полягає у перестановці знаків відкритого тексту згідно з певним правилом, яке є ключем.

Наприклад, текст «знак», зашифрований ключем «3421», буде виглядати так: «акнз».

Криптоаналіз перестановочного шифру виконується за два етапи:

1. Визначається довжина ключа, після чого шифротекст записується у вигляді стовпців від 1 до n, де n — довжина ключа.

2. Виконуються перестановки шляхом перебору значень. Для ключа довжиною n необхідно виконати n! перестановок. Це ефективно при $n<12$. Якщо ж $n>12$, доцільно використовувати розміщення перших 2-3 елементів перестановки.

Така методика дозволяє відновити ключі до $n<10^7$. Це означає, що не можливо створити стійкий шифр застосовуючи тільки перестановки.

Підстановочні шифри

Підстановочний шифр – алгоритм шифрування, який полягає у заміні знаків відкритого тексту іншими знаками, які є ключем.

Наприклад, зашифруємо ключем «а-x, б-y, в-z, г-n ... і т. д.» слово «гав», отримаємо шифротекст «nxz».

Підстановочні шифри існують вже близько 2500 років. Самим раннім прикладом є шифр Атбаш. Він виник приблизно в 600 році до н.е. і полягав у використанні єврейського алфавіту в зворотному порядку.

Юлій Цезарь використовував підставний шифр, який так і називався, – **шифр Цезаря**. Цей шифр полягав в заміщенні кожної букви іншою буквою, розташованою в алфавіті на три букви далі від шифрованої. Таким чином, буква A перетворювалася в D, B перетворювалася в E, а Z перетворювалася в C.

Підставні шифри мають один великий недолік – незмінна частота букв в початковому алфавіті. У англійській мові, наприклад, буква «Е» є найчастіше вживаною. Якщо замінити її іншою буквою, то найчастіше використовуватиметься нова буква (при розгляді великого числа повідомлень). За допомогою такого аналізу підставний шифр може бути зламаний.

Шифр Вернама (Одноразові блокноти)

Шифр Вернама (інша назва: **Одноразові блокноти** (One-time Pad, OTP) – система симетричного шифрування, для якої доведена абсолютна криптографічна стійкість.

Для утворення шифротексту повідомлення об'єднується операцією «виключаюче АБО» з ключем (називають одноразовим блокнотом або шифроблокнотом). При цьому ключ повинен володіти трьома критично важливими властивостями:

1. Бути справді випадковим;
2. Збігатися з розміром з заданим відкритим текстом;
3. Застосовуватися тільки один раз.

Шифр названий на честь телеграфіста AT&T Гільберта Вернама, що в 1917 році побудував телеграфний апарат, який виконував шифрування автоматично.

Вернам запропонував використовувати для кодування повідомлень особливості телетайпного коду, в якому знак, що кодується виражається у вигляді п'яти елементів. Кожен з цих елементів символізує наявність («плюс») або відсутність («мінус») електричного струму в лінії зв'язку. Наприклад, літера «А» відповідає комбінація «+ - - - -». Підготовлене до відправки повідомлення набивається на перфострічці: отвору відповідає «плюс» коду, його відсутність - «мінус».

Для шифрування Вернам запропонував заздалегідь готувати «гаму» (перфострічку з випадковими знаками) і потім електромеханічно складати її імпульси з імпульсами знаків відкритого тексту. Отримана сума представляла собою шифротекст. На приймальному кінці імпульси, отримані по каналу зв'язку, складалися з імпульсами тієї ж самої «гами», в результаті чого відновлювалися вихідні імпульси повідомлення. А якщо повідомлення перехопити, то без «гами» розшифрувати його було неможливо, зловмисник бачив тільки нічого не значущу послідовність «плюсів» і «мінусів».

Подальше вдосконалення даного методу належить майбутньому начальнику зв'язку військ США Джозефу Моборну. Ідея Моборна полягала в тому, що кожна випадкова «гама» повинна використовуватися один, і тільки один раз. При цьому для шифрування кожного знаку всіх текстів, які вже передані або будуть передані в найближчому майбутньому, повинен

застосовуватися абсолютно новий і такий, що не піддається передбаченню знак «гами».

Широко відома **шифромашина «Енігма»**, якою були оснащені німецькі війська часів Другої світової війни, є типовим прикладом пристрою з використанням шифрів Вернама. «Енігма» – це пристрій, що складається з комутаційних дисків та механізму зміни їх кутових положень. За обома сторонами комутаційного диска розміщені контакти, що відповідають алфавіту відкритого та шифрованого тексту. Контакти ці з'єднуються між собою відповідно до деякого правила підстановки, що зветься комутацією диска. Ця комутація визначає заміну літер в початковому кутовому положенні. При зміні кутового положення диска змінюється і правило підстановки. Таким чином, ключ шифрування містить кілька невідомих: схему з'єднання контактів і початкове кутове положення.

1949 році Клод Шеннон опублікував роботу, в якій довів абсолютну стійкість шифру Вернама. Інших шифрів з цією властивістю не існує. Це по суті означає, що шифр Вернама є найбезпечнішою криптосистемою з усіх можливих. При цьому умови, яким повинен задовольняти ключ, настільки жорсткі, що практичне використання шифру Вернама є важко здійсненним. Тому він використовується тільки для передачі повідомлень найвищої секретності.

Для роботи шифру Вернама необхідна дійсно випадкова послідовність нулів та одиниць (ключ). За визначенням, послідовність, отримана з використанням будь-якого алгоритму, є не зовсім випадковою, а псевдовипадковою. Тобто, потрібно отримати випадкову послідовність неалгоритмічно (наприклад, використовуючи радіоактивний розпад ядер, створений електронним генератором білий шум або інші досить випадкові події). Щоб зробити розподіл гранично близьким до рівномірного, випадкову послідовність, зазвичай, пропускають через хеш-функцію, наприклад MD5.

Проблемою є таємна передача послідовності та збереження її в таємниці. Якщо передавати ключ системи Вернама за допомогою іншого шифру (наприклад, DES), то отриманий шифр буде захищеним рівно настільки, наскільки захищений DES.

DES (Data Encryption Standard)

DES (Data Encryption Standard) — це симетричний алгоритм шифрування даних, розроблений компанією IBM і затверджений правлінням США в 1977 році як офіційний стандарт (FIPS 46-3). Алгоритм піддавався подальшій модифікації.

DES використовує ключ завдовжки 56 біт. Використовуються 7 біт з байту, восьмий біт кожного байту використовується для контролю парності. DES є блоковим алгоритмом шифрування, який обробляє одночасно один 64-бітовий

блок відкритого тексту. У алгоритмі DES виконуються 16 циклів шифрування з різним підключем в кожному з циклів. Ключ піддається дії свого власного алгоритму для утворення 16 підключів (рис. 1.9).

Даний стандарт шифрування передбачає спеціальне переупорядковування бітів для кожної перестановки. Те ж саме відноситься до алгоритму генерації підключа.

Алгоритм DES може функціонувати в чотирьох режимах.

- Режим **електронної кодової книги** (Electronic Code Book, **ECB**). Це базовий алгоритм блокового шифрування, в якому текст і ключ об'єднуються і утворюють шифрований текст. У цьому режимі ідентичний вхід утворює ідентичний вихід.

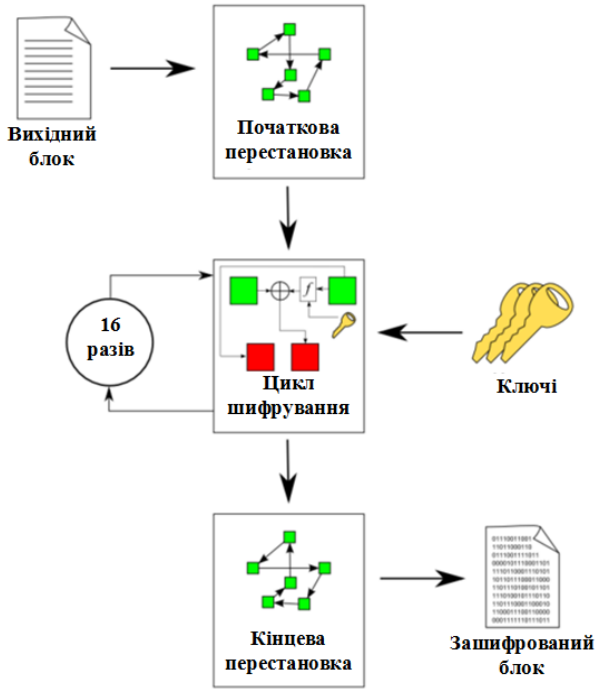


Рис. 1.9. Схема шифрування алгоритму DES

- Режим **ланцюга блоків** (Cipher Block Chaining, **CBC**). У цьому режимі кожен блок шифрується як в режимі електронної кодової книги, але з додаванням третього компонента, отриманого з попереднього виходу. В даному випадку, ідентичний вхід (відкритий текст) не утворює ідентичний вивід.
- Режим **зворотного зв'язку за шифрованим текстом** (Cipher Feed Back, **CFB**). У цьому режимі в якості вхідних даних DES використовується раніше згенерований шифрований текст. Після цього вихідні дані комбінуються з відкритим текстом і утворюють новий шифротекст.

- Режим **зворотного зв'язку по виходу** (Output Feed Back, **OFB**). Цей режим аналогічний зворотному зв'язку за шифрованим текстом, проте тут використовуються вихідні дані DES і не відбувається побудова ланцюга з шифротексту.

Зараз DES вважається ненадійним в основному через малу довжину ключа (56 біт) та розмір блоку (64 біти). У 1997 році організація EFF (Electronic Frontier Foundation) анонсувала комп'ютерну систему, яка дешифрувала ключ DES за чотири дні. Створення цієї системи коштувало 250000 доларів. За допомогою сучасного обладнання можна визначити ключ DES за 5 хвилин. Вважається, що алгоритм достатньо надійний для застосування у модифікації 3-DES, хоча існують розроблені теоретичні атаки.

Потрійний DES (Triple DES)

Triple DES (TDES, 3DES**)** – симетричний блоковий алгоритм шифрування даних, створений Вітфілдом Діффі, Мартіном Хеллманом і Уолтом Тачманном в 1978 році на основі алгоритму DES, з метою усунення головного недоліку останнього – малої довжини ключа (56 біт), який може бути зламаний методом повного перебору ключа.

На рис. 1.10 показана схема роботи алгоритму TDES.

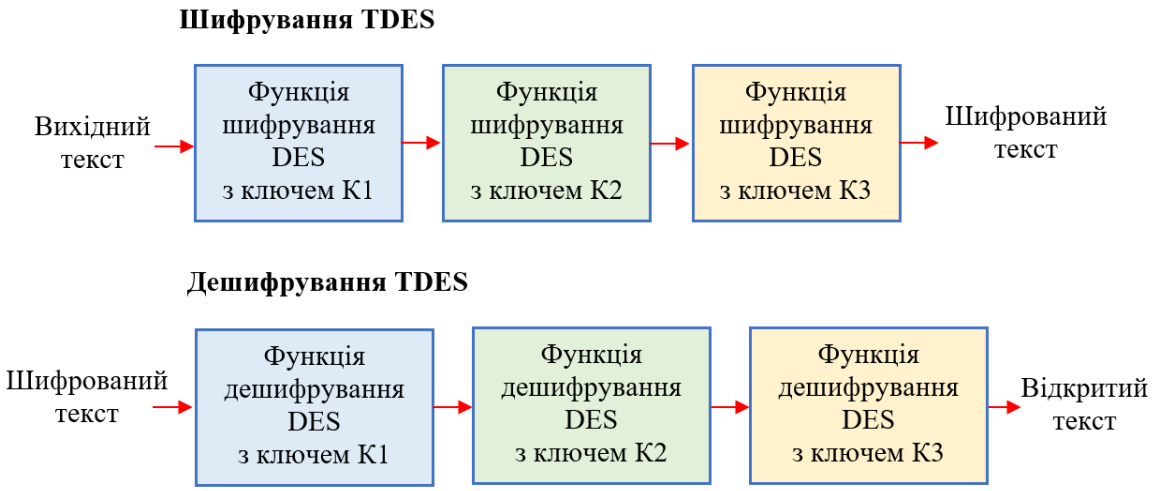


Рис. 1.10. Блок-схема алгоритму шифрування/дешифрування TDES

Потрійний DES використовується або з двома, або з трьома ключами. При використанні двох ключів ключ K3 ідентичний K1. TDES є відносно швидким алгоритмом, оскільки його можна реалізувати апаратно. Його функціонування займає в три рази більше часу, чим у DES, оскільки мають місце три операції шифрування DES. У більшості додатків рекомендується використовувати TDES замість простого DES.

3DES з трьома ключами реалізований в багатьох додатках, орієнтованих на роботу з Інтернет, у тому числі в PGP і S/MIME. Потрійний DES є досить популярною альтернативою DES і використовується при управлінні ключами в стандартах ANSI X9.17 і ISO 8732 і в PEM (Privacy Enhanced Mail). Відомих криптографічних атак, застосовних на практиці, на 3DES не існує.

3DES поступово витісняється алгоритмом AES Rijndael, що з 2002 року є стандартом США. Rijndael, реалізований програмно і працює в шість разів швидше. Тому 3DES більше підходить для апаратних реалізацій.

Розширений стандарт шифрування (AES)

AES (Advanced Encryption Standard**)**, також відомий під назвою **Rijndael** (Рендал) — симетричний алгоритм блочного шифрування, який був розроблений бельгійськими криптографами Д. Деймоном та В. Ріджменом. Державний інститут стандартів і технологій США (National Institute of Standards and Technology, **NIST**) 26 травня 2002 року оголосив AES стандартом шифрування. На сьогоднішній день AES є одним із найпоширеніших алгоритмів симетричного шифрування.

Rijndael є блоковим шифром, що використовує ключі і блоки завдовжки 128, 192 або 256 біт. На сьогодні така довжина ключів забезпечує практичну нездійсненність атак із застосуванням грубої сили. Алгоритм складається з 10-14 циклів, залежно від розмірів блоку відкритого тексту і розміру ключа. Оскільки цей стандарт був схвалений, Rijndael почав з’являтися в багатьох системах. Цей алгоритм можна вважати гідною альтернативою алгоритму TDES.

Крипостійкість всіх симетричних алгоритмів залежить від якості ключа, це висуває підвищені вимоги до служби генерації ключів, а також до надійності каналу обміну секретними ключами між учасниками секретних переговорів.

1.8.3. Проблема розподілу ключів

Симетричний підхід до шифрування несе в собі очевидну проблему, що називається проблемою **розподілу ключів** (Key Distribution), яка полягає в наступному. Відправник і отримувач хочуть обмінюватися секретними повідомленнями, але в їх розпорядженні є незахищений відкритий канал. Тому вони змушені використовувати шифрування, але щоб послати зашифроване повідомлення, потрібно попередньо обмінятися секретною інформацією про значення ключа. Однак секретний ключ не можна передати по відкритому каналу. Якщо його зашифрувати іншим ключем, то знову виникає проблема доставки другого ключа. Виходить замкнуте коло.

Єдиним, по-справжньому надійним вирішенням цієї проблеми є передача ключа при особистій зустрічі абонентів. Однак при активному обміні потрібно часто міняти ключі, щоб не дати можливості криптоаналітику зібрати велику кількість шифрованого матеріалу, - відомо, що чим більше зашифрованих повідомлень виявиться в руках криптоаналітика, тим легше йому розкрити криптосистему. Крім того, якщо зловмисник перехоплює і зберігає повідомлення, зашифровані одним і тим же ключем, то при розкритті даного ключа вони все виявляться скомпрометовані. Отже, необхідні часті особисті зустрічі абонентів для обміну ключами, що, по-перше, не завжди можливо, а по-друге, взагалі робить безглуздим обмін даними по каналу зв'язку – навіщо шифрувати дані, якщо їх можна особисто передати при зустрічі.

Менш надійним способом розподілу ключів є використання кур'єрів або інших варіантів захищеної доставки ключів, але це рішення теж має очевидні недоліки. Існують і інші прийоми, які не вирішують, але зменшують проблему розподілу ключів. Наприклад, у абонента може бути кілька секретних ключів, які він повинен використовувати по різному призначенню. Один ключ видається йому на довгий термін, цей ключ застосовується тільки для шифрування (дешифрування) інших ключів – короткочасних, кожен з яких дійсний тільки на час одного сеансу зв'язку. І хоча в цьому випадку все одно залишається проблема доставки довготривалого ключа, вже немає необхідності його частої зміни, так як цей ключ використовується відносно рідко і шифрує невеликі порції даних – сеансові ключі.

Незважаючи на різні удосконалення процедури розподілу ключів, вони не можуть повністю усунути корінний недолік симетричних методів – необхідність доставки секретного ключа по незахищеному каналу.

Якщо проблема з ключами виникає в системі з двома абонентами, то вона багаторазово посилюється в системі з великим числом абонентів. Нехай, наприклад, n абонентів хочуть обмінюватися секретними даними за принципом «кожен з кожним», в цьому випадку буде потрібно $n(n–1)/2$ ключів, які повинні бути згенеровані і розподілені надійним чином. Тобто кількість необхідних ключів пропорційна квадрату кількості абонентів, що при великій кількості абонентів робить задачу надзвичайно складною. Але саме така ситуація спостерігається у всіх сучасних мережах зв'язку – телефонних, радіо і комп'ютерних. Все це зробило надзвичайно актуальною проблему розподілу ключів.

1.8.4. Метод Діффі-Хеллмана передачі секретного ключа по незахищеному каналу

В середині 70-х років американські вчені Мартін Хеллман і Уілтфілд Діффі знайшли метод, за допомогою якого абоненти могли безпечно обмінюватися секретними ключами без передачі їх по каналу зв'язку. Особливість цього відкриття полягає в тому, що воно суперечить всім інтуїтивним уявленням людини, робить можливим те, що здається «очевидно» неможливим.

Метод Діффі-Хеллмана базується на використанні властивостей односторонніх функцій.

Одностороння функція (one-way function) – це функція $y=F(x)$, яка легко обчислюється для будь-якого вхідного значення x, але зворотне завдання – визначення x по заданому значенню функції y – вирішується дуже важко. Прикладом односторонньої функції може служити найпростіша функція двох аргументів $F(p,q) = p \times q$, що являє собою добуток двох простих чисел p і q, вона обчислюється порівняно просто, навіть якщо числа q і q дуже великі. Але надзвичайно складно вирішити зворотну задачу (яка називається факторизацією) – за добутком підібрати вихідні два простих числа. Інший приклад – функція $Y(x) = D^x \bmod P$, яка при деяких обмеженнях на параметри D і P є односторонньою, тобто, знаючи Y, а також параметри D і P, не можна без екстраординарних обчислювальних зусиль знайти аргумент x.

Отже, нехай Аліса і Боб вирішили обмінюватися шифрованими повідомленнями, але в їх розпорядженні є тільки незахищений відкритий канал зв'язку, при цьому ніяких можливостей зустрітися або передати секретний ключ через будь-кого іншого у них немає. У відповідності з алгоритмом Діффі-Хеллмана для успішного вирішення завдання Аліса і Боб повинні виконати наступні дії. Попередньо вони відкрито домовляються про те, що будуть використовувати одностороннюю функцію $Y(x)=D^x \bmod P$. Потім вони домовляються про значення параметрів D і P. Нехай, наприклад, вони домовилися, що D=7 і P=13, тобто функція має вигляд $Y=7^x \bmod 13$. Відповідно з алгоритмом Діффі-Хеллмана вся ця інформація не є секретною, і навіть якщо переговори будуть підслухані Євою, це не дасть їй можливості прочитати повідомлення Аліси і Боба. Подальші дії учасників обміну описуються в табл. 1.1.

В результаті описаної процедури на кроці 4 Аліса і Боб отримали одне й те саме число 3. Математичні перетворення показують, що обчислення Аліси і Боба завжди будуть давати однакові результати. Отримані в результаті числа вони можуть використовувати в якості відомого тільки їм ключа для різних симетричних методів шифрування.

Подивимося, чи може Єва підібрати поділюваний секретний ключ Аліси і Боба. Нехай на кроці 3, коли Аліса і Боб пересилали один одному свої відкриті ключі $a(10)$ і $b(9)$, Єва змогла перехопити ці числа (адже канал є відкритим) і

тепер намагається обчислити поділюваний секретний ключ. Знаючи число *a*, яке Аліса послала Бобу, Єва хоче повторити дії Боба і обчислити поділюваний секретний ключ за формулою $10^B \bmod 13$. Для цього їй потрібно закритий ключ Боба *B*, який він, проте, зберігає таємно від усіх. Зате Єва знає, що Боб використовував свій закритий ключ B, коли обчислював значення свого відкритого ключа – *b*.

Таблиця 1.1. Дії Аліса і Боба у відповідності з алгоритмом Діффі-Хеллмана

№	Дії Аліси		Дії Боба	
1	Аліса секретним чином вибирає довільне число *A* (закритий ключ Аліси)	Нехай, наприклад, *A*=2	Боб також секретно вибирає довільне число *B* (закритий ключ Боба)	Нехай, наприклад, *B*=4
2	Аліса обчислює значення *a* односторонньої функції *Y*, використовуючи в якості аргументу своє секретне число *A*: тобто $a=D^A \bmod P$ (відкритий ключ Аліси)	$a=7^2 \bmod 13= =49 \bmod 13 =10$	Боб також обчислює значення *b* односторонньої функції *Y*, використовуючи в якості аргументу своє секретне число *B*: тобто $b=D^B \bmod P$ (відкритий ключ Боба)	$b=7^4 \bmod 13= =2401 \bmod 13= =9$
3	Аліса пересилає Бобу свій відкритий ключ *a*		Боб пересилає Алісі свій відкритий ключ *b*	
4	Аліса, отримавши від Боба число *b*, обчислює по формулі $K=b^A \bmod P$ (поділюваний секретний ключ)	$K=9^2 \bmod 13= =81 \bmod 13=3$	Боб, отримавши від Аліси число *a*, обчислює по формулі $K=a^B \bmod P$ (поділюваний секретний ключ)	$K=10^4 \bmod 13 = =10000 \bmod 13= =3$
5	По правилах модульної математики: $b^A \bmod P =$	*K*=3	По правилах модульної математики: $a^B \bmod P =$	*K*=3

	$= (D^B \bmod P)A \bmod P =$ $= D^{BA} \bmod P$		$= (D^A \bmod P)B \bmod P =$ $= D^{BA} \bmod P$	

Тобто, завдання буде вирішено, якщо Єва зможе підібрати таке значення B, щоб значення $7^B \bmod 13$ дорівнювало 9. Але саме це обчислити практично неможливо, оскільки функція $7^B \bmod 13$ є односторонньою. Таким чином, Аліса і Боб дійсно отримали секретний ключ.

Для того щоб ускладнити вирішення оберненої задачі, тобто відновлення закритого ключа Аліси або Боба з відкритого, на параметри алгоритму накладаються деякі обмеження, в тому числі такі:

- всі параметри D, P, A, B повинні бути цілими додатними числами;
- A і B повинні бути великими числами порядку 10^{100};
- P має бути великим простим числом близько 10^{300}, причому бажано, щоб $(P-1)/2$ також було простим числом;
- число D не обов'язково має бути великим, зазвичай воно вибирається менше 10.

Хоча алгоритм Діффі-Хеллмана став проривом в області криптографії, в його вихідному стані він представляв скоріше теоретичну, ніж практичну цінність. Усунувши перешкоду у вигляді необхідності надійного закритого каналу для передавання ключа, цей метод не зняв проблеми квадратичної залежності числа ключів від числа абонентів. Рішення прийшло дуже скоро: вже через рік після появи алгоритму Діффі-Хеллмана була теоретично доведена можливість принципово нового підходу до шифрування – асиметричного шифрування, при використанні якого (окрім інших переваг) кардинально спрощується задача розподілу ключів.

1.9. Асиметричне шифрування

1.9.1 Концепція асиметричного шифрування

До недавнього часу поняття «симетричне шифрування» не існувало просто тому, що всі методи, які використовувалися людством протягом декількох тисяч років, за сучасною класифікацією могли бути віднесені до класу симетричних, інших просто не було. Більше того, всі ці тисячі років існувала тверда переконаність, що в принципі ніколи не може бути інших схем, крім

симетричної, коли відправник шифрує за допомогою секретного ключа, одержувач за допомогою цього ж ключа розшифровує.

Революція відбулася в кінці 60-х – середині 70-х, коли з різницею в кілька років дві групи вчених, одна з яких – Діффі і Хеллман, а інша – співробітники секретної урядової лабораторії Великобританії Елліс, Кокс і Вільямсон, незалежно один від одного винайшли принципово новий підхід до шифрування, що відкриває глобальні перспективи в області сучасних комунікацій (відомо, що історично першими були британські криптографи, які відкрили асиметричне шифрування на 6 років раніше, ніж Діффі і Хеллмана, проте до 1997 року вони не змогли оприлюднити свої результати, так як їх робота мала гриф секретності).

Гранично спрощуючи, цей підхід можна описати фразою: «відправник шифрує повідомлення за допомогою одного ключа, а одержувач розшифровує його за допомогою іншого ключа». Як бачимо, тут на двох сторонах обмінного каналу використовуються різні ключі, тобто присутня асиметрія, відповідно всі методи, засновані на такому підході, стали називати «асиметричними».

Це дивно, що за кілька тисяч років не було жодної відомої науці спроби винаходу асиметричного методу шифрування, і раптом, практично одночасно, дві незалежні групи вчених роблять це відкриття! Можливо, причина криється в тому, що до кінця 60-х років співпало дві обставини: по-перше, виникла гостра потреба в новому типі шифрування, по-друге, з’явилися технічні можливості реалізації цієї ідеї.

Потреба була продиктована розвитком таких видів масових комунікацій, як телефон, радіо, комп’ютерні мережі, для яких, по-перше, дуже багато значить секретність через слабку захищеність публічних засобів зв’язку, а по-друге, є неприйнятними обмеження традиційних методів шифрування, що виражаються в необхідності обміну секретною ключем для кожної пари абонентів. До кінця 70-х років стали чітко вимальовуватися перспективи використання Інтернету як світової мережі зв’язку, і одночасно з цим стало приходити усвідомлення того, що глобальна публічна мережа може виконати свою місію тільки в тому випадку, якщо мільйонам її користувачів нададуть можливість захищеного обміну повідомленнями. Ці теми особливо хвилювали військових різних країн, яких дуже приваблювала можливість розподіленого управління збройними силами, але лякала неможливість гарантувати таємність переданих директив.

До цього часу дозріли технічні можливості реалізації обчислювальноємних алгоритмів шифрування, до яких можуть бути віднесені асиметричні алгоритми. Масове поширення набули комп’ютери, що володіли великою обчислювальною потужністю, якої досі могли похвалитися тільки унікальні моделі суперкомп’ютерів. Це зробило шифрування повсякденного операцією, яка могла бути виконана на звичайному персональному комп’ютері.

Ось на такому історичному фоні була запропонована концепція асиметричної криптосистеми, звана також **шифруванням з відкритим ключем**.

Шифрування з відкритим ключем — це асиметрична схема, у якій застосовуються пара ключів: **відкритий** (Public Key), що зашифровує дані, і відповідний йому **закритий** (Private Key), що їх розшифровує. Відкритий ключ разом з інформацією вільно поширюється по мережі, у той час як закритий прихований в таємниці. Будь-яка людина з копією вашого відкритого ключа може зашифрувати інформацію, яку тільки ви зможете прочитати.

На рис. 1.11 представлена модель асиметричної криптосистеми. Так само як і в моделі симетричного шифрування (рис. 1.8), тут показані три учасники: відправник (Боб), одержувач (Аліса) і зловмисник (Єва). На відміну від симетричної схеми шифрування, в якій наявність поділюваного секретного ключа автоматично означає можливість двостороннього захищеного обміну, тут існує окрема процедура для передачі зашифрованих повідомлень в кожну зі сторін. На рисунку показаний варіант, коли зашифровані повідомлення можуть бути послані тільки Бобом в сторону Аліси, але не навпаки.

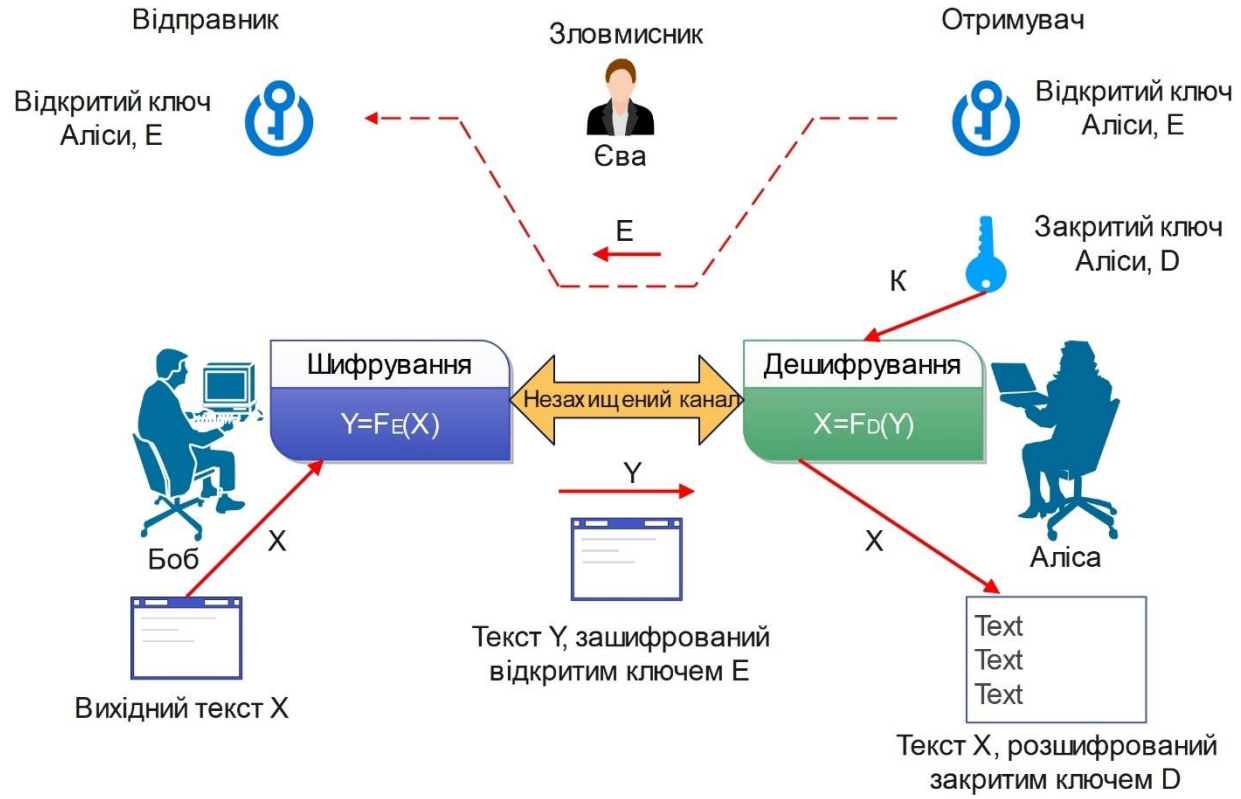


Рис. 1.11. Схема асиметричного шифрування

Отже, Аліса побажала, щоб Боб посилав їй зашифровані повідомлення. Для цього вона згенерувала пару ключів: відкритий ключ (відкритий ключ) E і закритий ключ (закритий ключ) D. Для шифрування тексту служить відкритий

ключ, але розшифрувати цей текст можна тільки за допомогою закритого ключа. Аліса не хоче, щоб хто-небудь читав її пошту, тому вона зберігає закритий ключ D (часто званий також особистим ключем) в секреті. Відкритий же ключ E Аліса вільно передає всім, від кого хоче отримувати зашифровані повідомлення. Відкритий ключ не представляє ніякого секрету, Аліса може помістити його на своїй сторінці в соціальній мережі або оприлюднити в рекламі на телебаченні. Всі, хто хочуть посилати Алісі зашифровані повідомлення, використовують один і той же ключ E, але при цьому ніхто з них не може прочитати повідомлення один одного.

1. Аліса передає Бобу свій відкритий ключ E по незахищеному каналу в незашифрованому вигляді.
2. Боб шифрує своє повідомлення X відкритим ключем Аліси E і посилає зашифрований текст $Y=F_E(X)$ по відкритому каналу. Ніхто не може прочитати це повідомлення. Навіть сам Боб, якби йому раптом захотілося перечитати, що він там написав, не зміг би цього зробити, тому що для цього потрібен закритий ключ Аліси, якого у нього немає.
3. Аліса отримує зашифроване повідомлення $Y=F_E(X)$ і розшифровує його своїм закритим ключем D: $X=F'_D(Y)$.

Для того щоб в мережі все n абонентів мали можливість не тільки приймати зашифровані повідомлення, але і самі посилати такі, кожен абонент повинен мати власну парою ключів E і D. Всього в мережі буде 2^n ключів: n відкритих ключів для шифрування і n секретних ключів для дешифрування. Таким чином вирішується проблема масштабованості: квадратична залежність кількості ключів від числа абонентів в симетричних алгоритмах замінюється лінійною залежністю в асиметричних алгоритмах.

Вирішується і проблема доставки ключа, оскільки тепер він не є секретом, його можна без побоювання передавати по відкритому каналу. Зловмиснику немає сенсу прагнути заволодіти відкритим ключем, оскільки це не дає можливості розшифрувати текст або обчислити закритий ключ.

1.9.2. Алгоритм асиметричного шифрування RSA

Відкривачі асиметричного підходу до шифрування показали концептуальну можливість існування функцій, що дозволяють побудувати криптографічну систему,
в якій текст шифрується одним ключем, а розшифровується – іншим. Вони також окреслили ті перспективи, які відкриває цей підхід в справі вирішення проблеми розподілу ключів. Ними були сформульовані дві принципові вимоги, яким повинні задовольняти функції асиметричної криптосистеми:

- зашифроване повідомлення має бути результатом обчислень односторонньої функції, так щоб ніхто не міг виконати зворотні перетворення і отримати вихідний текст;
- ця одностороння функція повинна бути побудована таким чином, щоб у неї був певний секретний елемент, знаючи який одержувач шифровки міг би легко виконати зворотне перетворення.

Функції, які задовольняють цим вимогам, назвали **односторонніми функціями з потайним входом** (trapdoor function). Деякий час вченим не вдавалось знайти функції, що задовольняють цим критеріям, тому ідея асиметричного шифрування не знаходила практичного застосування. Нарешті, в 1978 році троє американських вчених, Рональд Райвест, Аді Шамір і Леонард Адлеман, запропонували довгоочікуваний **алгоритм асиметричного шифрування RSA**, названий так по першим буквах їх прізвищ – Rivest, Shamir і Adleman.

Безпека алгоритму RSA побудована на принципі складності факторизації. Алгоритм використовує два ключі – **відкритий** (public) і **секретний** (private), разом відкритий і відповідний йому секретний ключі утворюють **пару ключів** (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем.

У табл. 1.2 описуються основні кроки алгоритму RSA.

Єві для того, щоб прочитати перехоплене повідомлення C, потрібен закритий ключ Аліси (D, N). Але в її розпорядженні є тільки відкритий ключ (E, N). Теоретично, знаючи відкритий ключ, можна обчислити значення закритого ключа. Однак, необхідною проміжною дією в цьому перетворенні є знаходження простих чисел P і Q, для чого потрібно розкласти на прості множники дуже велике число N, а це є надзвичайно трудомісткою процедурою. Таким чином, тут використовується одностороння функція $N = P \times Q$. Але для Аліси ця ж дія – розкладання великого числа на два простих множника – не представляє ніяких труднощів, оскільки вона знає, як побудоване це число N, вона сама його знайшла, довільно вибравши два співмножники. Іншими словами, Алісі відомий «потайний вхід» цієї односторонньої функції. Саме з величезною обчислювальною складністю розкладання великого числа N на прості множники P і Q пов'язана висока криптостійкість алгоритму RSA.

Отже, базовий алгоритм, що дозволяє забезпечити конфіденційність даних, дуже простий.

Шифрований текст = (відкритий текст) $E \bmod N$

Відкритий текст = (шифрований текст) $D \bmod N$

Секретний ключ = {D, N}
Відкритий ключ = {E, N}

Таблиця 1.2. Послідовність дій учасників обміну даними у відповідності з алгоритмом RSA

Дії Аліси і Боба	**Числовий приклад**
Аліса довільно вибирає два випадкових числа *P* і *Q*. Вони повинні бути дуже великими – від цього залежить стійкість алгоритму шифрування	Для простоти розрахунків беруться дуже малі числа. Нехай *P*=7 і *Q*=13
Аліса обчислює два добутки $N=P\times Q$ $M=(P-1)\times(Q-1)$	$N = 91$ $M = 6\times12=72$
Аліса вибирає випадкове ціле число *E*, яке менше *M* і не має з ним спільних співмножників	$E = 3$
Пара (*E, N*) – це відкритий ключ Аліси, який вона передає усім, від кого хоче отримувати шифровані повідомлення. Аліса надсилає Бобу і усім іншим, з ким вона бажає вести захищену переписку, свій відкритий ключ (*E, N*)	(5, 91)
Аліса знаходить *D* таке, що $1 = D\times E \bmod M$. Пара (*D, N*) – це закритий ключ Аліси, який вона не показує нікому. З цього моменту вона готова отримувати зашифровані повідомлення від Боба.	$1 = D\times5 \bmod 72$ $D = 29$ (це число легко знаходиться підбором, якщо враховувати признаки поділу на 5)
Боб отримав відкритий ключ від Аліси і також, як усі інші, що мають доступ до цього ключа, може надсилати Алісі зашифровані повідомлення. Він представляє своє повідомлення в будь-якому цифровому форматі і розбиває його на блоки *X* таким чином, щоб $0<X<N$	Нехай секретний текст, який надсилає Боб, містить лише один символ *R*, який в коді ASCII має значення 1010010, або 82 в десятковому коді

Боб шифрує повідомлення X відкритим ключем (E, N): $C=X^E \bmod N$ і надсилає Алісі зашифроване повідомлення C	$C = 82^5 \bmod 91 = 10$ Обчислення модуля від степені числа спрощується при використанні наступного правила: $(Y^{a+b+c}) \bmod P = (Y^a \bmod P \times Y^b \bmod P \times \times Y^c \bmod P) \bmod P$
Аліса отримує повідомлення C і розшифровує його своїм закритим ключем (D, N): $X=C^D \bmod N$	$X = 10^{29} \bmod 91 = \{10^1 \bmod 91 \times \times 10^4 \bmod 91 \times 10^6 \bmod 91 \ldots\} \bmod 91$ всередині фігурної дужки чотири рази повторюється останній співмножник – $10^6 \bmod 91$) $10 \bmod 91 = 10$; $10^4 \bmod 91 = 81$; $10^6 \bmod 91 = 1$ $X = \{10 \times 81 \times 1\} \bmod 91 = 82$
Результат розшифровки X=82 співпадає з вихідним секретним повідомленням	

Також слід зауважити, що алгоритм може бути обернений для забезпечення автентифікації відправника. В цьому випадку алгоритм матиме наступний вигляд.

Шифрований текст = (відкритий текст) D mod *N*

Відкритий текст = (шифрований текст) E mod *N*

Секретний ключ = {D, N}

Відкритий ключ = {E, N}

Число N називається модулем, а числа E і D – відкритою й секретною експонентами, відповідно. Пари чисел (N, E) є відкритою частиною ключа, а (N, D) — секретною. Числа P і Q після генерації пари ключів можуть бути знищені, але в жодному разі не повинні бути розкриті.

Для генерації P і Q необхідно використовувати криптографічно надійний генератор випадкових чисел. У зловмисника не має бути можливості одержати будь-яку інформацію про значення цих чисел. P і Q не повинні бути занадто близькими одне до одного, інакше можна буде знайти їх, використовуючи метод факторизації Ферма.

Хоча інформація про відкритий ключ не є секретною, її потрібно захищати від підробок, щоб зловмисник під ім’ям легального користувача не нав’язав свій відкритий ключ, після чого за допомогою свого закритого ключа він міг би розшифровувати всі повідомлення, що посилаються легальному користувачеві, і відправляти свої повідомлення від його імені. Рішення проблеми дає технологія

цифрових сертифікатів – електронних документів, які пов'язують конкретних користувачів з конкретними відкритими ключами.

1.10. Хеш-функції. Односторонні функції шифрування.

В області інформаційної безпеки особливе місце займає спеціальний клас односторонніх функцій, які називаються хеш-функціями.

Хеш-функцією (hash function) називають таку односторонню функцію, яка, будучи застосованою до деяких даних, дає в результаті значення, що складається з фіксованого порівняно невеликого і не залежного від довжини вихідних даних числа байтів. Результат роботи хеш-функції називають **хеш-кодом**, або **дайджестом**.

Хеш-функції називають також **односторонніми функцій шифрування** (ОФШ), де в якості шифрованого представлення вихідних даних виступає дайджест. При цьому знання дайджесту не дозволяє і навіть не припускає відновлення вихідних даних. Односторонні функції шифрування використовують в різних цілях, в тому числі і для забезпечення цілісності та автентичності інформації. Нехай, наприклад, потрібно забезпечити цілісність повідомлення, що передається по мережі. Відправник і одержувач домовилися, що вони будуть використовувати односторонню функцію H з секретним числом – ключем K – в якості параметра. Перш ніж відправити повідомлення X, відправник обчислює для нього дайджест $M=H(X, K)$ і відправляє його разом з повідомленням X адресату (рис. 1.12).

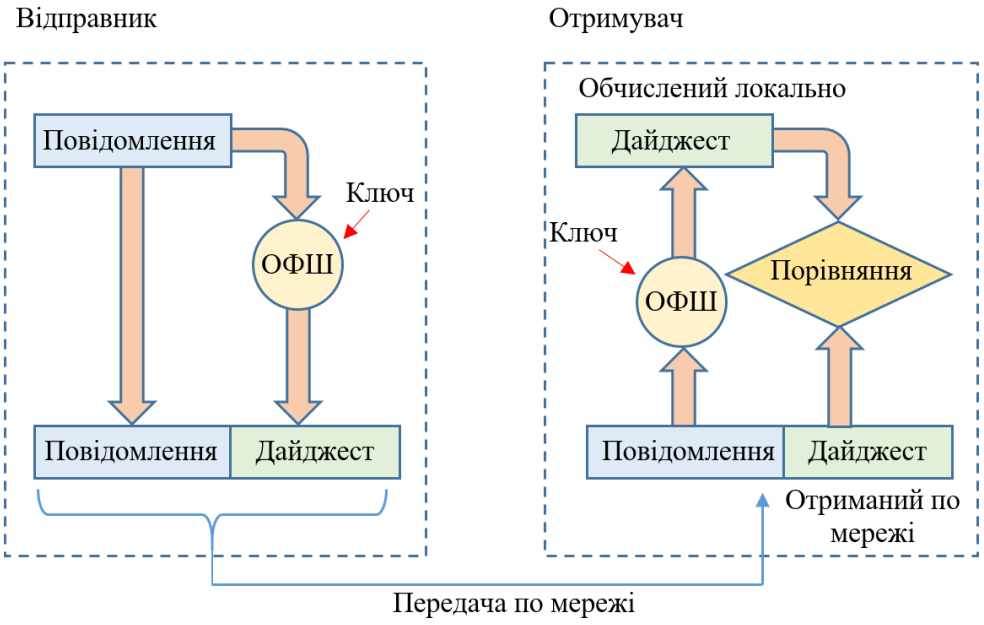


Рис. 1.12. Використання параметричної односторонньої функції шифрування для контролю цілісності

Адресат, отримавши дані *X* і *M*, застосовує ту ж саму ОФШ до переданого у відкритому вигляді вихідного повідомлення *X*, використовуючи відомий йому секретний ключ *K*: *M'=H(X, K).* Якщо значення дайджестів, обчисленого локально і отриманого по мережі *M* збігаються, значить, вміст повідомлення не було змінено під час передачі.

Хеш-функції широко використовуються в мережевих протоколах, в алгоритмах електронно-цифрового підпису, в механізмах автентифікації на основі паролів. Для цих цілей потрібно використання безпечних хеш-функції. Хеш-функція може називатися безпечною, якщо:

- функція є односторонньою. Іншими словами, функція створює контрольну суму з інформації з неможливістю відновлення інформації по контрольній сумі;
- складно сконструювати два фрагменти інформації з отриманням однакової контрольної суми при виконанні функції.

Другу умові не так легко задовольнити. Дані контрольні суми мають бути менші за розміром ніж інформація, для забезпечення простоти підписування, зберігання і передачі інформації. Якщо ця умова задовольняється, то одній і тій же контрольній сумі повинно відповідати велике число різних фрагментів інформації. Безпека функцій забезпечується способом зв'язку усіх бітів в вихідних даних з усіма бітами контрольної суми. Таким чином, якщо один біт інформації змінюється, то також змінюється велика кількість бітів в контрольній сумі.

Безпечні хеш-функції повинні забезпечувати створення контрольної суми завдовжки, принаймні, в 128 біт. Найбільш популярними в системах безпеки в даний час є серія хеш-функцій MD2, MD4, MD5. Всі вони генерують дайджести фіксованої довжини в 16 байт (128 біт). Адаптованим варіантом MD4 є американський стандарт SHA, довжина дайджесту в якому складає 20 байт (160 біт). Компанія IBM підтримує односторонні функції MDC2 і MDC4, що базуються на алгоритмі шифрування DES. Існує безліч інших хеш-функцій, проте велика їх частина визнана небезпечними.

2. Віртуальні локальні мережі

2.1. Призначення віртуальних локальних мереж

Важливою властивістю комутатора локальної мережі є здатність контролювати передачу кадрів між сегментами мережі. З різних причин (дотримання прав доступу, політика безпеки і т. д.) деякі кадри не слід передавати за адресою призначення. Обмеження такого типу можна реалізувати за допомогою користувацьких фільтрів – **списків контролю доступу** (Access Control List, **ACL**). Однак, користувацький фільтр може заборонити комутатору передачу кадрів тільки за конкретними адресами, а широкотрансляційний трафік він зобов'язаний передати всім сегментам мережі. Так вимагає алгоритм його роботи. Тому, мережі, що побудовані на основі комутаторів, іноді називають плоскими – через відсутність бар'єрів на шляху широкотрансляційного трафіку. 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. 2.1). І навпаки, пристрої, що знаходяться в різних VLAN, невидимі один для одного на канальному рівні, навіть якщо вони під'єднані до одного комутатора, і зв'язок між цими пристроями можливий тільки на мережевому і більш високих рівнях.

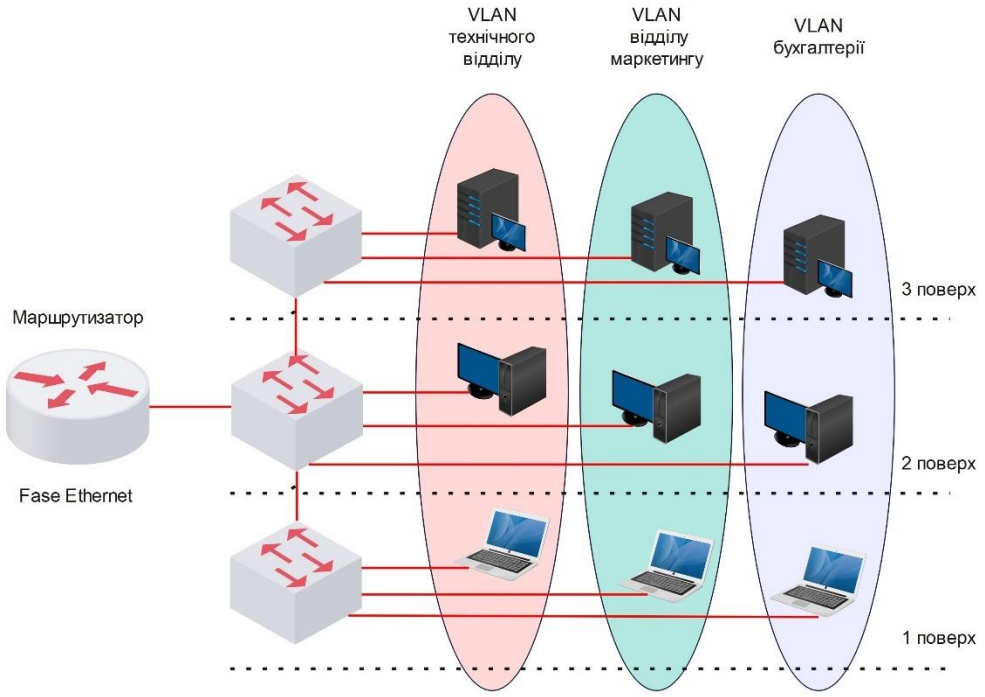


Рис. 2.1. Приклад використання VLAN

Це означає, що передача кадрів між різними віртуальними мережами на основі адреси канального рівня неможлива незалежно від типу адреси (unicast, multicast або broadcast). Всередині віртуальної мережі кадри передаються за технологією комутації, тобто лише на той порт, який пов'язаний з адресою призначення кадру.

Застосування віртуальних локальних мереж дозволяє розділити мережу канального рівня на безліч логічних мереж, які матимуть низькі затримки передачі і географічне положення вузлів не впливатиме на те, в якій IP-мережі вони знаходитимуться. Такі мережі простіше адмініструвати, вони мають більш високі показники безпеки. Оскільки кожна VLAN є окремим широкотрансляційним доменом, мережа матиме більшу продуктивність за рахунок зменшення впливу широкотрансляційних штормів.

Віртуальна мережа утворює **домен широкотрансляційного трафіку** (broadcast domain) по аналогії з доменом колізій (collision domain), який утворюється концентраторами мереж Ethernet.

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.

Перевагою технології віртуальних мереж є те, що вона дозволяє створювати повністю ізольовані сегменти мережі шляхом логічного конфігурування комутаторів, не вдаючись до зміни фізичної структури.

Для зв'язування віртуальних мереж в загальну мережу потрібне залучення засобів мережевого рівня. Це може бути реалізовано за допомогою окремого маршрутизатора або завдяки програмному забезпеченню комутатора, який тоді стає комбінованим пристроєм – **комутатором 3-го рівня (L3 switch)**.

Технологія віртуальних мереж довгий час не стандартизувалась хоча і була реалізована в широкому спектрі моделей комутаторів різних виробників. Положення змінилося після прийняття в 1998 році стандарту IEEE 802.1Q, який визначає базові правила побудови віртуальних локальних мереж, які не залежать від протоколу канального рівня, що підтримується комутатором.

2.2. Методи побудови віртуальних мереж

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. 2.2). При цьому кожен порт призначається в певну віртуальну мережу. Кадр, що надійде від порту, що належить, наприклад, віртуальній мережі VLAN1, ніколи не буде переданий порту, який не належить цій віртуальній мережі. Порт можна призначити декільком віртуальним мережам, хоча на практиці так роблять рідко – пропадає ефект повної ізоляції мереж.

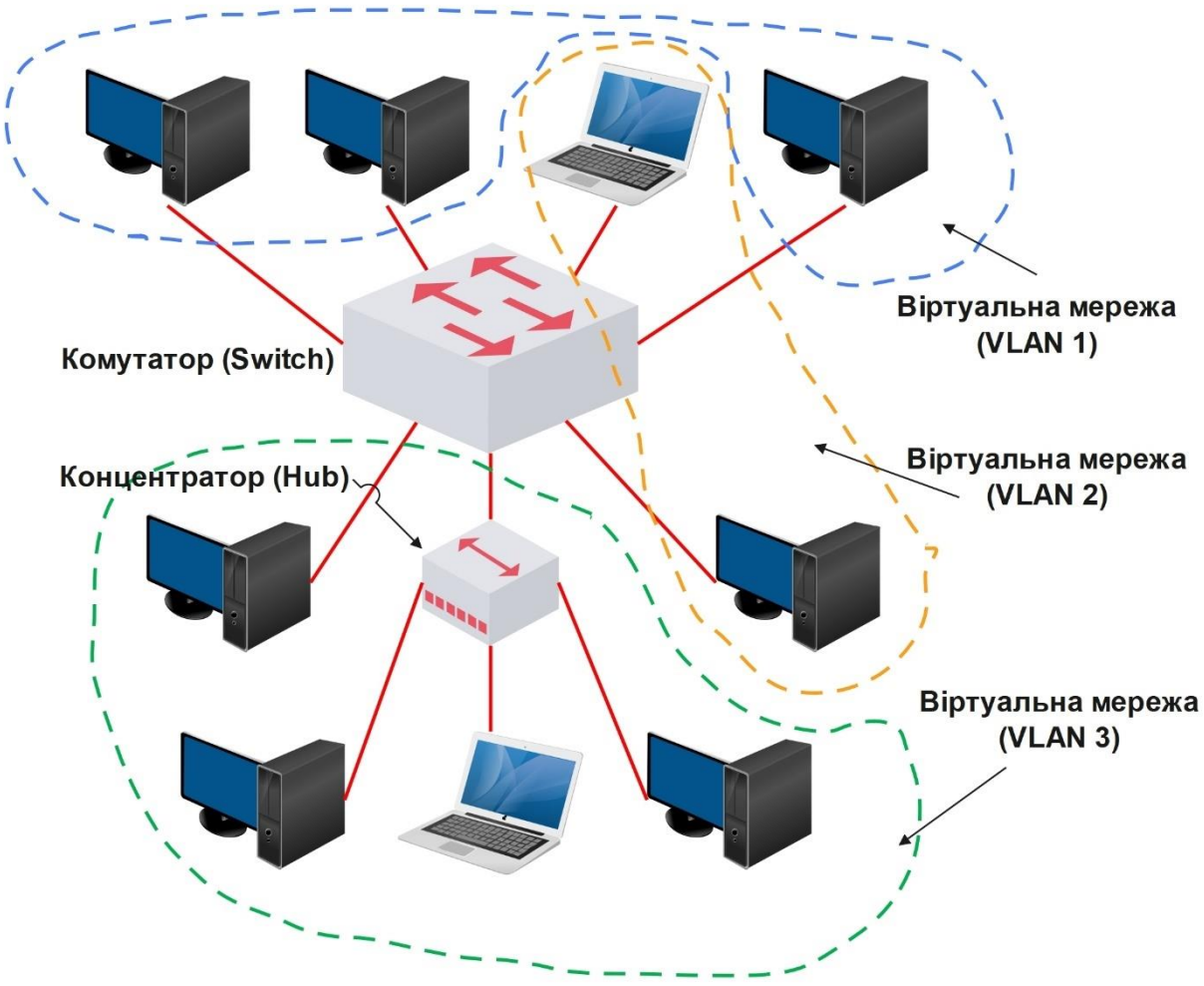


Рис. 2.2. Віртуальні мережі, побудовані на одному комутаторі

Створення віртуальних мереж методом port-based VLAN не вимагає від адміністратора великого обсягу ручної роботи – досить кожен порт призначити до однієї з декількох заздалегідь створених віртуальних мереж.

Такий спосіб непогано працює коли комутатор один, але при використанні декількох комутаторів виникає проблема – для з'єднання між комутаторами потрібно використати декілька портів, по одному на кожну VLAN. Рисунок 2.3 ілюструє проблему, що виникає при створенні віртуальних мереж на основі декількох комутаторів, що підтримують техніку групування портів.

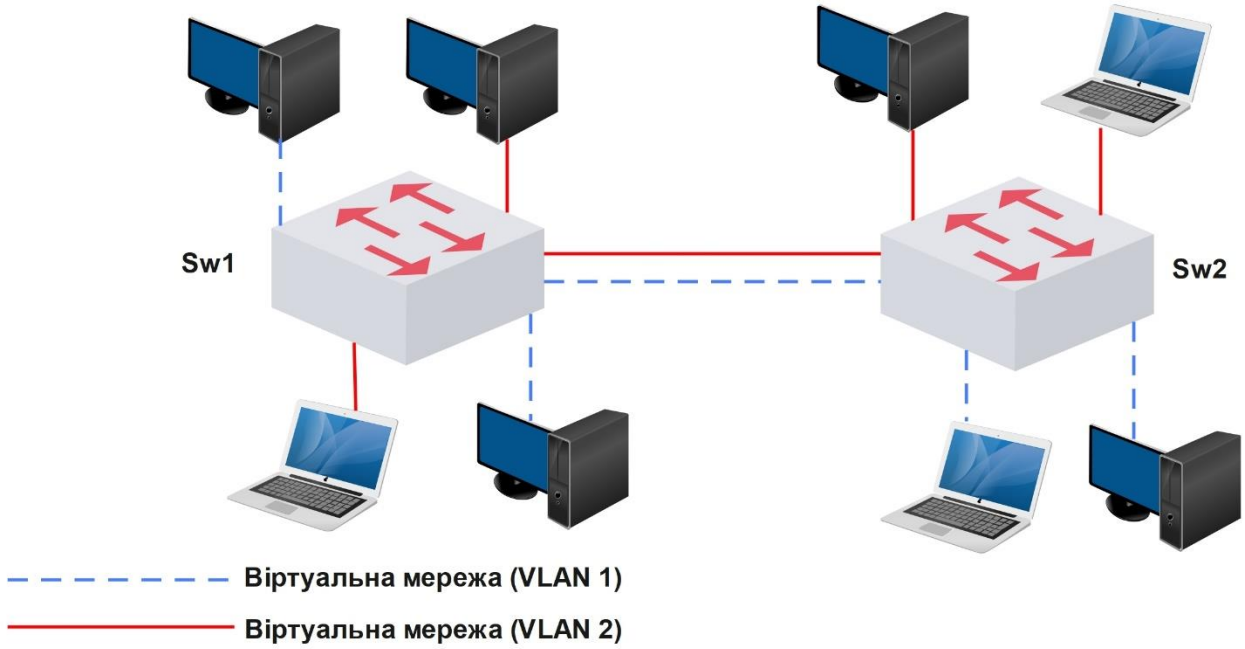


Рис. 2.3. Віртуальні мережі, побудовані на двох комутаторах за методом port-based VLAN

Якщо вузли будь-якої віртуальної мережі під'єднані до різних комутаторів, то для під'єднання кожної такої мережі на комутаторах повинна бути виділена спеціальна пара портів. Таким чином, при використанні методу групування портів (port-based VLAN), комутатори з вимагають для свого з'єднання стільки портів, скільки віртуальних мереж вони підтримують. В цьому випадку неефективно використовуються кабелі і порти комутаторів. Крім того, при з'єднанні віртуальних мереж через маршрутизатор для кожної віртуальної мережі виділяється окремий кабель і окремий порт маршрутизатора, що також призводить до великих накладних витрат.

Другий метод утворення віртуальних мереж базується на **групуванні MAC-адрес**. Він припускає ручне заповнення таблиці відповідності MAC-адрес вузлів

і віртуальних мереж, яким вони належать. Кожна MAC-адреса, яка вивчена комутатором, призначається певній віртуальній мережі. При існуванні в мережі великої кількості вузлів цей спосіб вимагає від адміністратора значного обсягу ручної роботи. Однак, при побудові віртуальних мереж на основі декількох комутаторів він виявляється більш гнучким, ніж групування портів.

Описані два методи базуються лише на додаванні додаткової інформації до адресних таблиць комутатора і в них відсутня можливість додавання в кадр інформації про приналежність його певній віртуальній мережі.

Тому, широке розповсюдження отримав метод tag-based VLAN, що базується на введені в кадр додаткового поля, яке зберігає інформацію про приналежність кадру до певної віртуальної мережі при його переміщеннях між комутаторами мережі. При цьому немає необхідності запам’ятовувати в кожному комутаторі про приналежність всіх MAC-адрес мережі віртуальним мережам. Метод tag-based VLAN описаний в стандарті IEEE 802.1Q або **VLAN Tagging**.

Стандарт IEEE 802.1Q вводить в кадрі Ethernet додатковий 4-х байтовий підзаголовок канального рівня, який називається **тегом віртуальної локальної мережі**. Кадри з такими заголовками передаються і в каналах, що сполучають комутатори, при цьому потік інформації називають «тегованим», а порти, що передають такий трафік – **транками** (trunks).

Додаткове поле з позначкою про номер віртуальної мережі використовується тільки тоді, коли кадр передається від комутатора до комутатора, а при передачі кадру кінцевому вузлу воно, зазвичай, видаляється. При цьому модифікується протокол взаємодії «комутатор-комутатор», а програмне і апаратне забезпечення кінцевих вузлів залишається незмінним. До прийняття стандарту IEEE 802.1Q існувало багато фірмових протоколів цього типу, але всі вони мали один недолік – обладнання різних виробників при утворенні VLAN виявлялося несумісним.

На рис. 2.4. 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**).

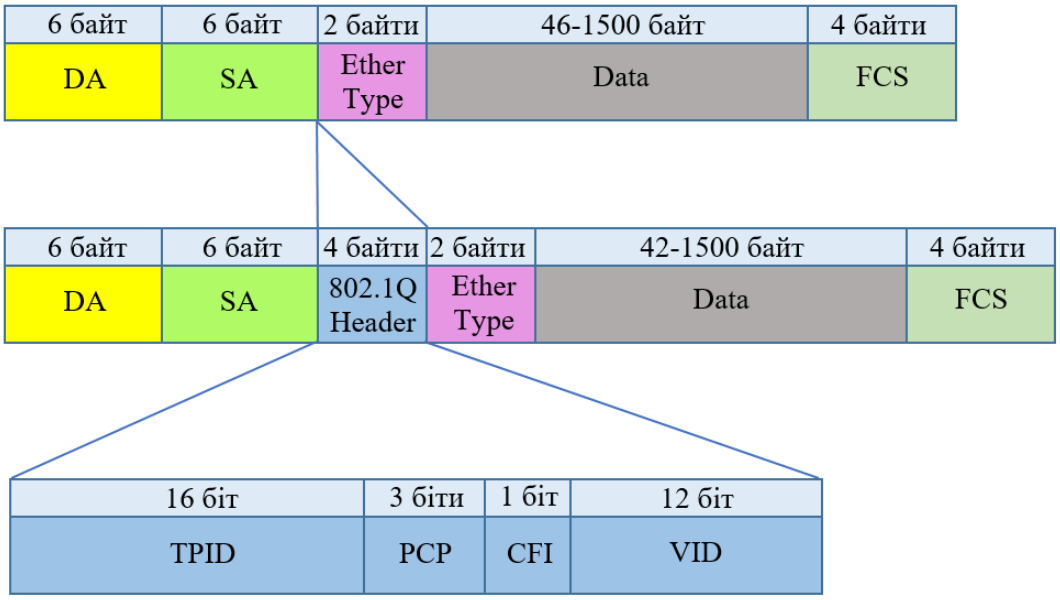


Рис. 2.4. Додавання заголовку 802.1Q в кадр Ethernet

Поле TCI містить в собі поля PCP, CFI та VID.

- **PCP** (Priority Code Point – код пріоритету) – вказує пріоритет кадру. Допустимі значення від 1 (найнижчий пріоритет) до 7 (найвищий). Ці значення застосовуються для пріоритезації трафіку (передача голосу, відео, даних, та ін.).
- **CFI** (Canonical Format Indicator – ідентифікатор канонічного формату) – використовується для забезпечення сумісності між мережами Ethernet та Token Ring. Для комутаторів Ethernet завжди встановлений в 0.
- **VID** (VLAN Identifier – ідентифікатор VLAN) – 12-бітний ідентифікатор VLAN, до якого належить кадр. Значення 0 вказує на те, що кадр не належить до жодного VLAN; у цьому разі тег 802.1Q вказує тільки пріоритет.

Розрядність поля VID дозволяє комутаторам створювати до 4096 віртуальних мереж. Для позначення VLAN використовується 4094 значення, оскільки номер 0 означає відсутності номера VLAN, а 4095 зарезервований. Інші номери поділяються на два діапазони: **звичайні** (normal) і **розширені** (extended).

Звичайні номери VLAN позначаються від 1 до 1005, при цьому останні номери з 1002 по 1005 зарезервовані для мереж Token-Ring і FDDI. Віртуальні мережі з номерами 1, 1002-1005 створюються автоматично, і не можуть бути

видалені. На комутаторах Cisco інформація про звичайні VLAN зберігається у файлі vlan.dat.

Розширений діапазон – з 1006 по 4094, використовується в основному провайдерами, і зберігається в конфігураційному файлі комутатора. Комутатори Cisco, залежно від моделі підтримують обмежене число віртуальних мереж. Наприклад, модель 2960 підтримує 255 активних VLAN, серії 3560, 3650 і 3750 до 1005 активних VLAN, комутатори 4900 – 2048, а 4500 і 6500 підтримують максимально можливе число – 4094 VLAN.

2.3. Варіанти реалізації VLAN

Хости в різних VLAN на одному комутаторі

По замовчуванню, 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. 2.5, налагоджено дві VLAN, усі порти налагоджені як нетеговані (access-порти в термінології Cisco) у відповідних VLAN.

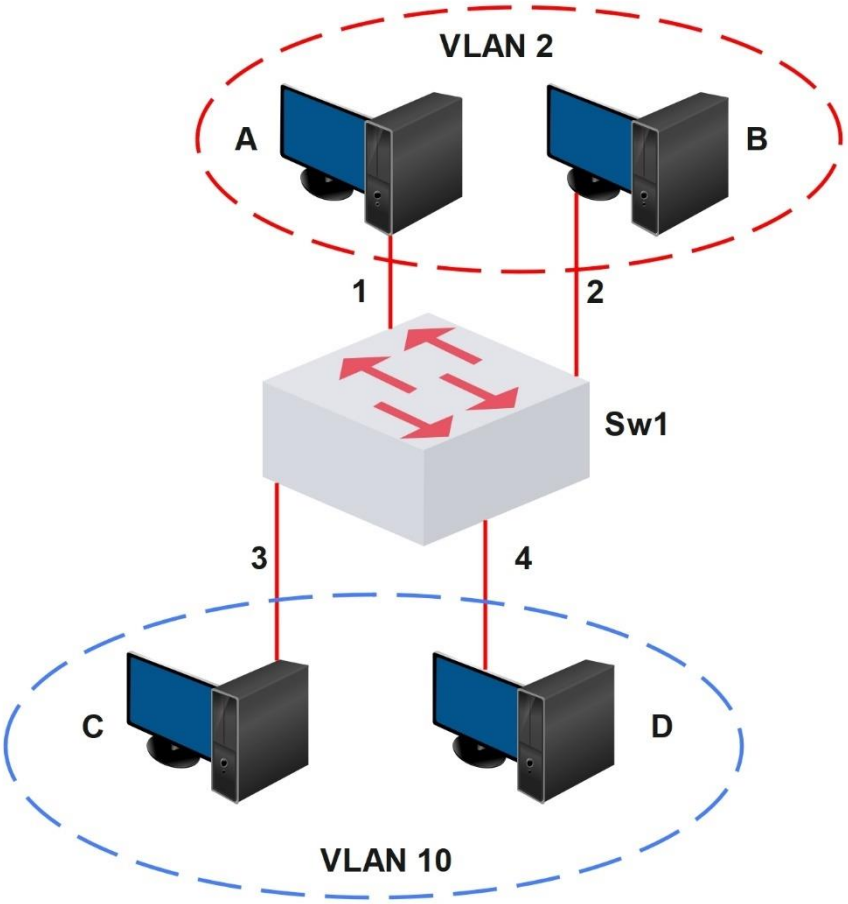


Рис. 2.5. Хости в різних VLAN на одному комутаторі

Після цього на комутаторі існують дві таблиці комутації.

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

Усі базові механізми комутатора залишаються такими ж як і до призначення VLAN, але вони застосовуються лише в межах відповідного VLAN. Наприклад, якщо хост з VLAN10 відправляє широкотрансляційний фрейм, то він буде відправлений тільки на порти VLAN10.

Хости в різних VLAN на різних комутаторах

Нехай до вказаної вище топології додано комутатор Sw2 і два хоста E і F (рис. 2.6).

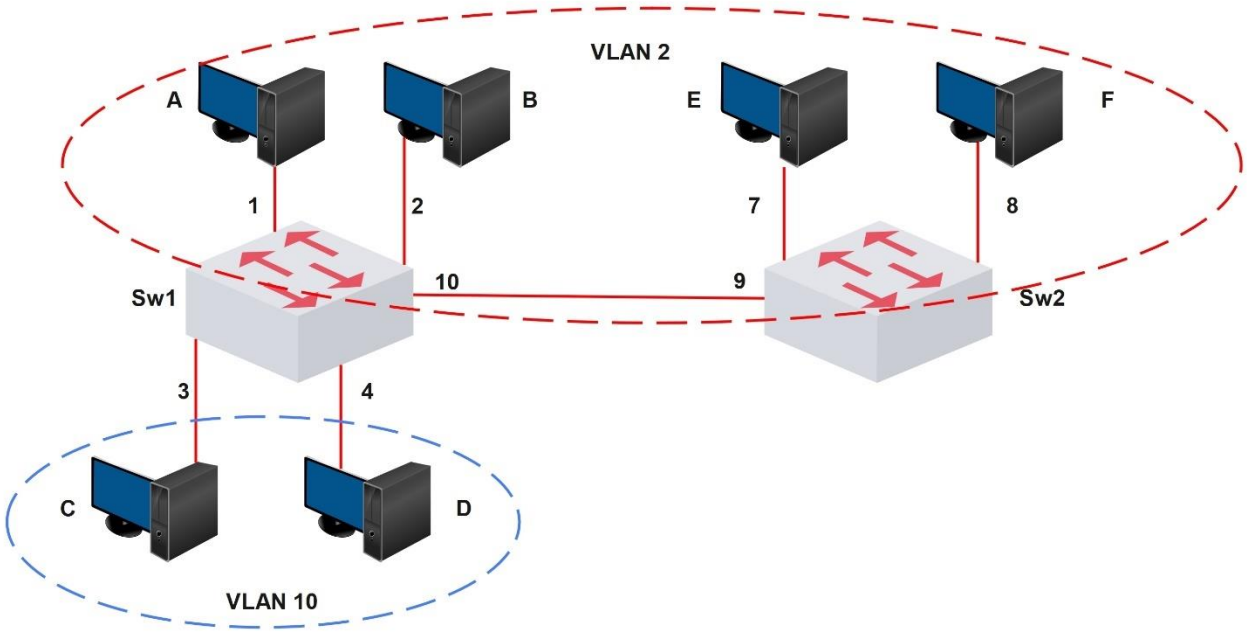


Рис. 2.6. Хости в різних VLAN на різних комутаторах

Якщо розглядати два комутатори окремо (не з’єднані між собою), то на комутаторі Sw1 залишилася колишня таблиця комутації, а на комутаторі Sw2 таблиця наступна:

Таблиця комутації Sw2:

Порт комутатора	**MAC-адрес хоста**
7	E
8	F

Для того, щоб хости A, B, E, F «побачили» один одного вони повинні знаходитися в одній VLAN. Тобто, необхідно певним чином вказати комутаторам, що ще на одному порту є хости у відповідній VLAN. Для вказаного прикладу досить додати на комутаторі Sw1 порт 10 в VLAN2, а на комутаторі Sw2 порт 9 в VLAN2. Після цього на комутаторах в таблицях комутації додадуться нові порти і відповідні MAC-адреси хостів. Тепер чотири хоста на різних комутаторах знаходяться в одному широкотрансляційному сегменті.

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

Тепер нехай до комутатора Sw2 додано два хоста G і H в VLAN10 (рис. 2.7). Для того, щоб хости C і D з VLAN10 на комутаторі Sw1, могли обмінюватися інформацією з хостами G і H з VLAN10 на комутаторі Sw2, додано ще один канал (лінк) між комутаторами. Логіка аналогічна додаванню хостів в VLAN2.

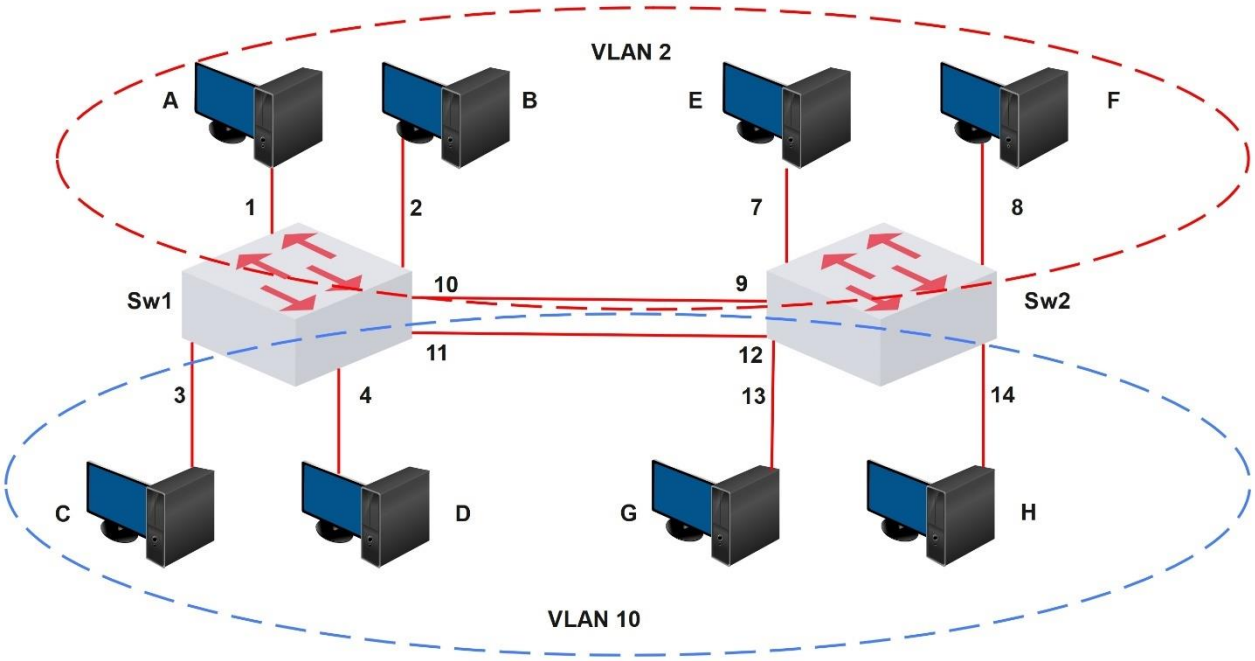


Рис. 2.7. До комутатора Sw2 додано два хоста G і H

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. 2.8).

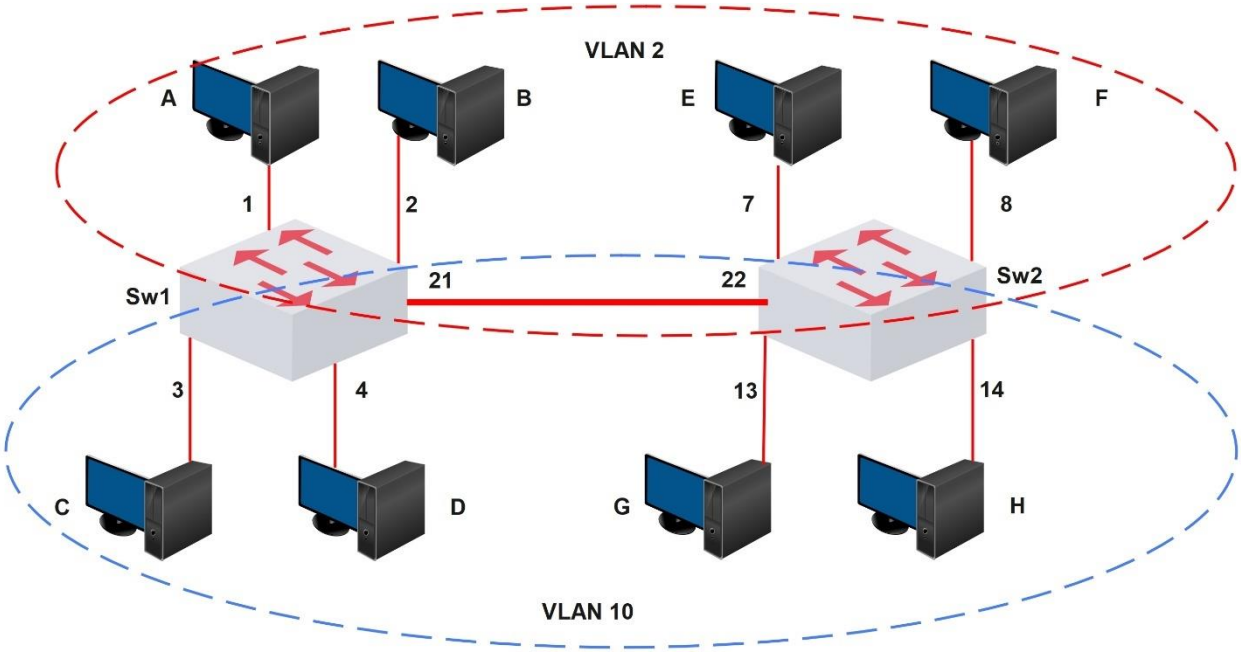


Рис. 2.8. Використання тегованих портів

Тегований порт дозволяє комутатору передати трафік декількох VLAN через один порт і зберегти при цьому інформацію про те, в межах якої саме VLAN передається фрейм. На комутаторах Sw1 і Sw2 порти 21 і 22 – це теговані порти. Для того, щоб комутатори розпізнавали котрій VLAN належить фрейм, і використовували відповідну таблицю комутації для його обробки, виконується тегування фрейму.

Наприклад (рис. 2.9), якщо хост E передає фрейм хосту A, то комутатор Sw2 перевіряє свою таблицю комутації і бачить, що хост A доступний через порт 22. Оскільки порт налаштований як тегований, то коли фрейм виходить з порту 22 в ньому проставляється тег, який вказує якому VLAN належить цей фрейм. В даному випадку проставляється тег з VLAN2. Комутатор Sw1 отримує тегований фрейм через тегований порт 21. Для того, щоб визначити на який порт його передавати далі, комутатор Sw1 використовує таблицю комутації для VLAN2 (оскільки цей VLAN був вказаний в тегу).

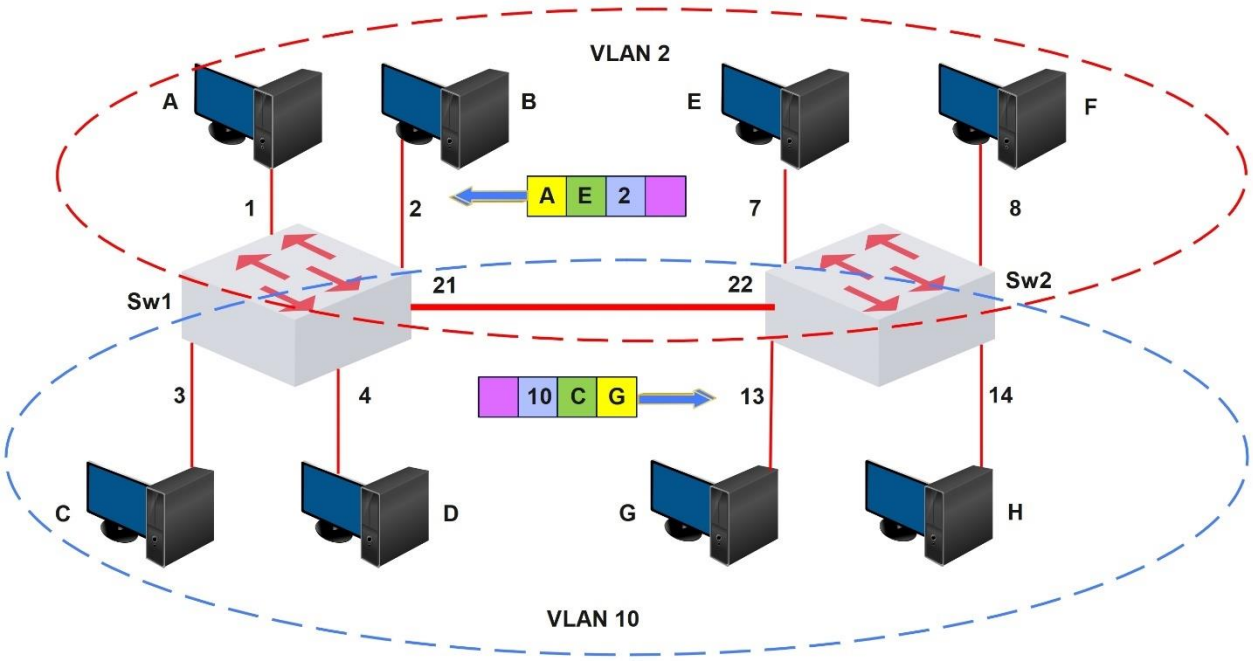


Рис. 2.9. Передавання тегованих фреймів

На комутаторі Sw1 порт 21 має бути налаштований як тегований для того, щоб комутатор не відкидав теговані фрейми, а зчитував інформацію тегу. Також, відповідно, щоб він позначав фрейм тегом, коли передаватиметься трафік комутатору Sw2.

Інші порти комутатора залишаються нетегованими. Для хостів операція тегування, яку виконують комутатори, абсолютно прозора. Хости нічого не знають про теги і отримують звичайні фрейми.

Аналогічні дії виконуються, наприклад, при передачі фрейма від хоста C до хоста G.

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.

2.4. Налаштування VLAN на комутаторах Cisco

Віртуальні локальні мережі додаються в режимі глобальної конфігурації комутатора командою **vlan** *vlan-id*. Після цієї команди режим зміниться на режим конфігурації VLAN, де рекомендується задати ім'я VLAN. 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
```

Для видалення VLAN використовується команда **no vlan** *vlan-id*

Sw1(config)# no vlan 100

При видаленні VLAN всі пов'язані з нею порти деактивуються.

Для видалення порту з певної VLAN використовується команда **no switchport access vlan** *vlan-id:*

Sw1(config)#in f0/1

Sw1(config-if)# no switchport access vlan 100

Коли порт видаляється з певної VLAN, він повертається до VLAN1.

Транки VLAN

Для портів комутатора можна задати дві різні ролі. Порт може бути визначений як порт доступу або як транковий порт (рис. 2.10).

Порт доступу (access port) належить тільки одній VLAN. Як правило, окремі пристрої, такі як комп'ютери і сервери, під'єднуються до портів доступу. Якщо кілька комп'ютерів під'єднуються до одного порту доступу через концентратор, то всі ці пристрої будуть належати до однієї VLAN.

Транковий порт (trunk port) – це канал типу «точка-точка» між комутатором і іншим мережевим пристроєм. Транкові підключення служать для передачі трафіку декількох VLAN через один канал і забезпечують їм доступ до всієї мережі. Транкові порти необхідні для передачі трафіку декількох VLAN між пристроями при з'єднанні двох комутаторів, комутатора й маршрутизатора або комутатора і мережевого адаптера вузла з підтримкою транкінгу 802.1Q.

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. 2.11).

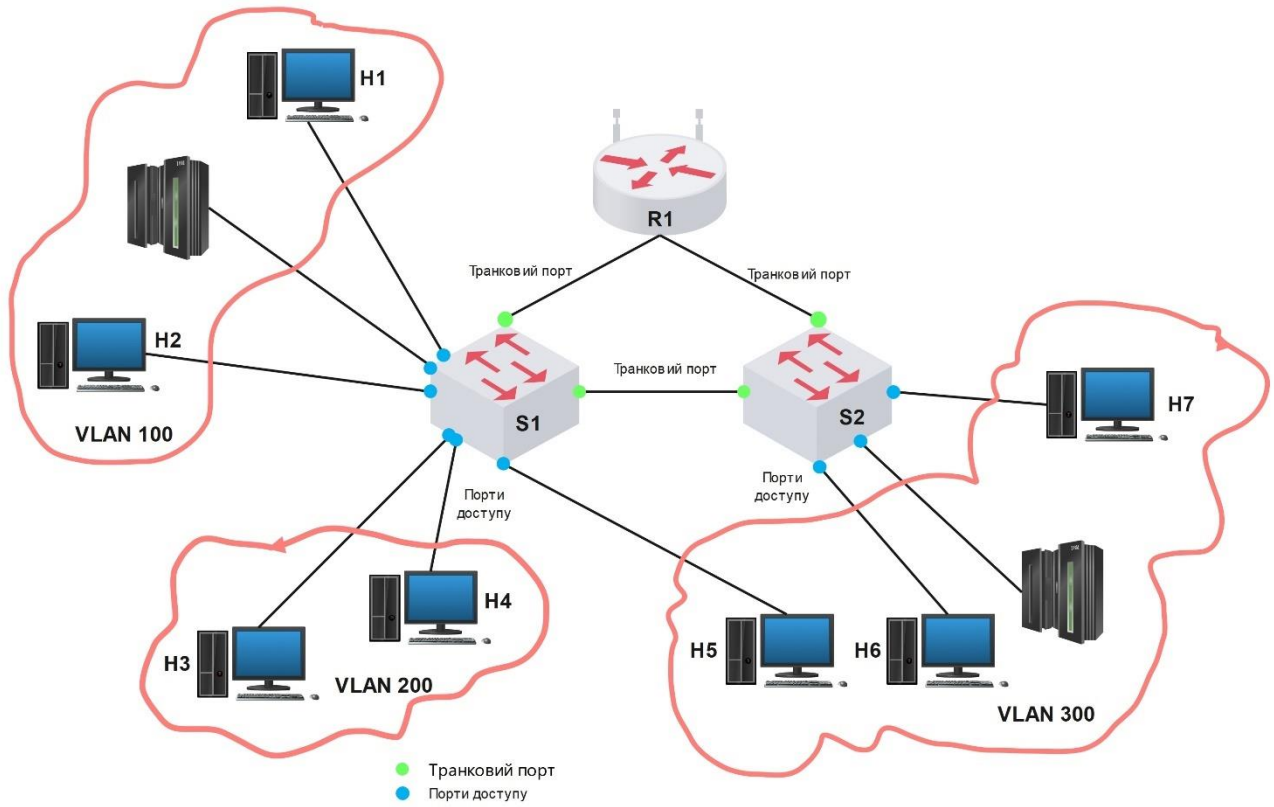


Рис. 2.10. Ролі портів VLAN

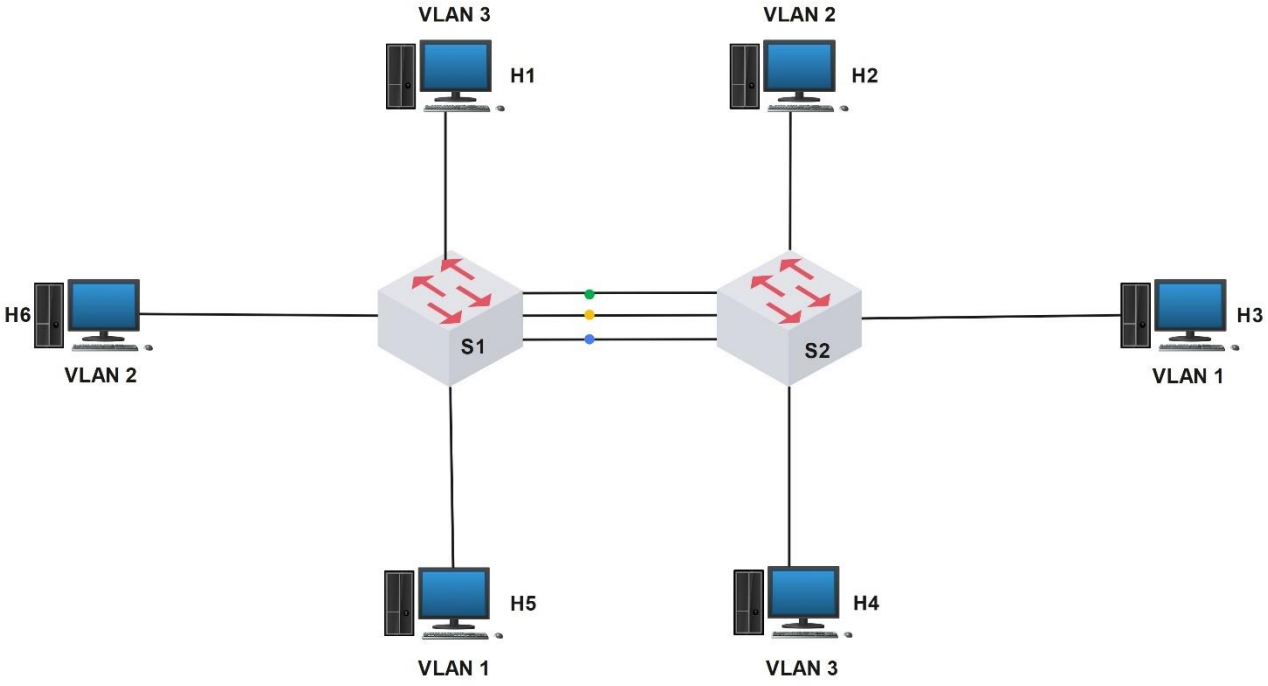


Рис. 2.11. Приклад об’єднання VLAN без транкінгу

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. 2.12).

Для передачі трафіку декількох VLAN через один канал необхідна їх ідентифікація. Транковий порт підтримує маркування кадрів. Маркування кадрів дозволяє додати до кадру дані VLAN.

IEEE 802.1Q – стандартний і затверджений метод маркування кадрів. Cisco розробила власний протокол маркування кадрів під назвою **протокол міжкомутаторного каналу** (Inter-Switch link, **ISL**). Комутатори більш високого класу, такі як Catalyst 6500, підтримують обидва протоколи маркування, проте більшість комутаторів локальної мережі, таких як 2960, підтримують тільки 802.1Q.

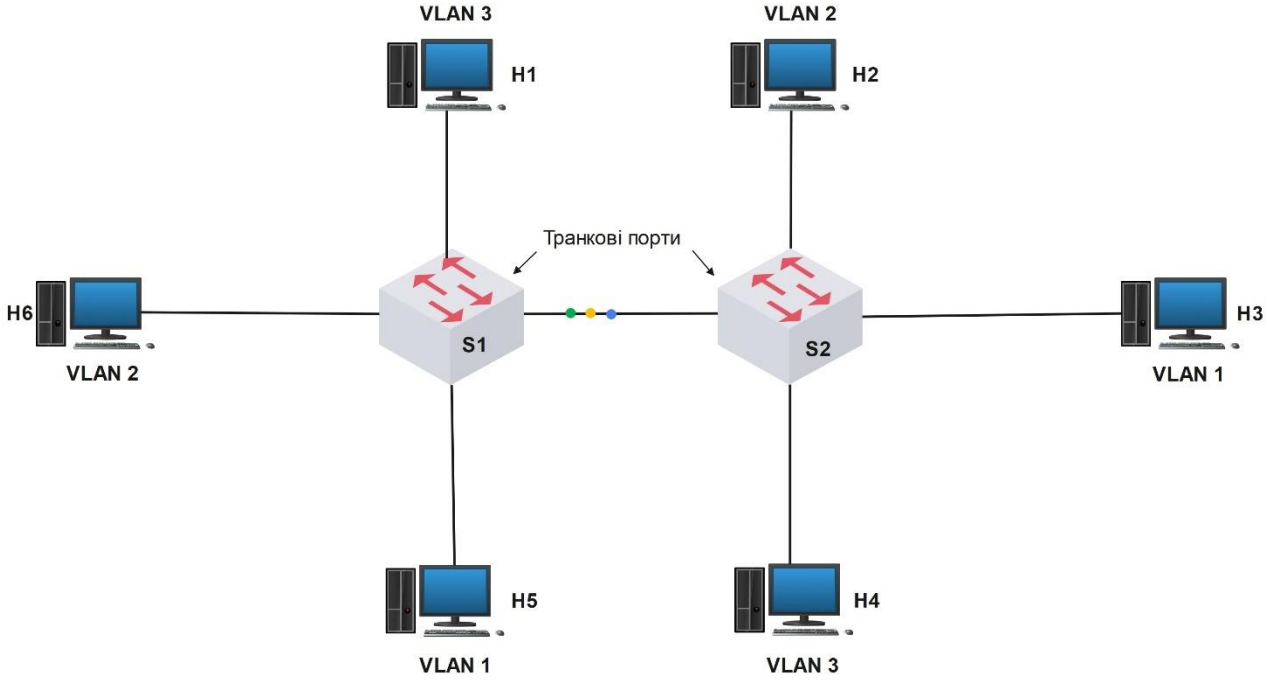


Рис. 2.12. Приклад об’єднання VLAN через транкові порти

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}
```

Комутатори, що підтримують і 802.1Q і ISL, вимагають останньої інструкції. Комутатор 2960 не вимагає цієї інструкції, оскільки підтримує лише 802.1Q.

Параметр **negotiate** (узгодження) використовується по замовчуванню на багатьох комутаторах Cisco. Він дозволяє пристрою автоматично виявляти тип інкапсуляції сусіднього комутатора.

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
```

Коли комутатор отримує тегований кадр на транковому порті, він видаляє мітку, перш ніж переслати кадр в порт доступу. Комутатор пересилає кадр, тільки якщо порт доступу відноситься до тієї ж VLAN, що і тегований кадр.

Проте, деякі типи трафіку повинні проходити через канал VLAN без ідентифікатора. Трафік без ідентифікатора VLAN називається **нетегованим**. Приклади нетегованого трафіку: CDP (Cisco Discovery Protocol), VTP і певні типи голосового трафіку. Нетегований трафік мінімізує затримку, пов’язану з перевіркою мітки ідентифікатора VLAN.

Для підтримки нетегованого трафіку використовується спеціальна VLAN, яка називається **власною VLAN** (**native VLAN**) (рис. 2.13). Нетеговані кадри, прийняті на порту 802.1Q, передаються у власну VLAN. На комутаторах Cisco Catalyst в якості власної VLAN, по замовчуванню, використовується VLAN1.

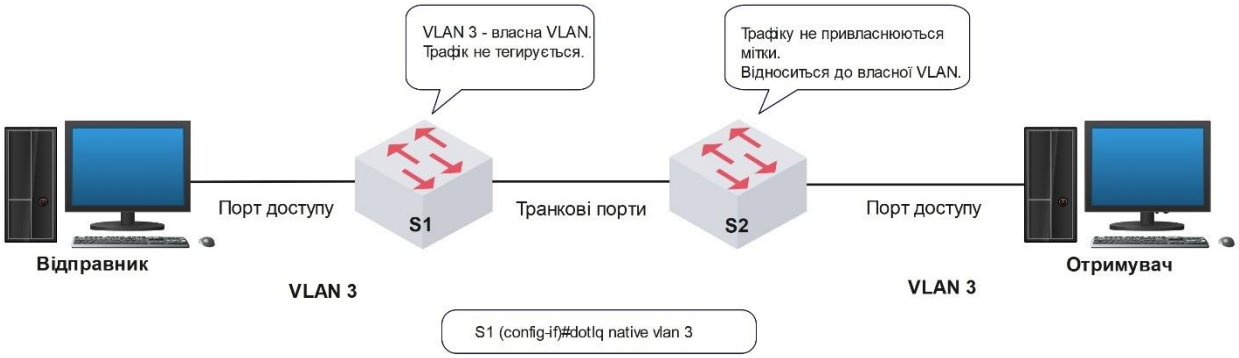


Рис. 2.13. Власні VLAN (native VLAN)

Будь-яку VLAN можна налаштувати в якості власної. Потрібно переконатись в тім, що власна мережа VLAN для транкового підключення 802.1Q однакова на обох сторонах каналу. В іншому випадку в топології STP можуть виникнути петлі.

Щоб призначити власну VLAN фізичному інтерфейсу потрібно ввести наступну команду для транкового підключення 802.1Q:

Switch(config-if)#dot1q native vlan 3

2.5. Налаштування маршрутизації між VLAN

Для зв’язку між різними мережами необхідні пристрої мережевого рівня. Таким пристроєм може виступати або окремий маршрутизатор, або комутатор 3-го рівня.

При використанні окремого маршрутизатора, можливі два варіанти реалізації – класичний метод, з використанням окремих інтерфейсів маршрутизатора в кожній з віртуальних мереж і транковий метод, з використанням одного фізичного інтерфейсу між маршрутизатором і комутатором і декілька віртуальних підінтерфейсів (subinterfaces) для кожної віртуальної мережі.

2.5.1. Класичний метод маршрутизації між VLAN

Топологія мережі при класичному методі маршрутизації між VLAN зображена на рис. 2.14. На приведеному рисунку є чотири віртуальних мережі (VLAN10, VLAN20, VLAN30 і VLAN40). Маршрутизатор має відповідно чотири інтерфейси FastEthernet, кожен з яких під’єднаний до відповідного порту комутатора, що знаходиться у своїй VLAN.

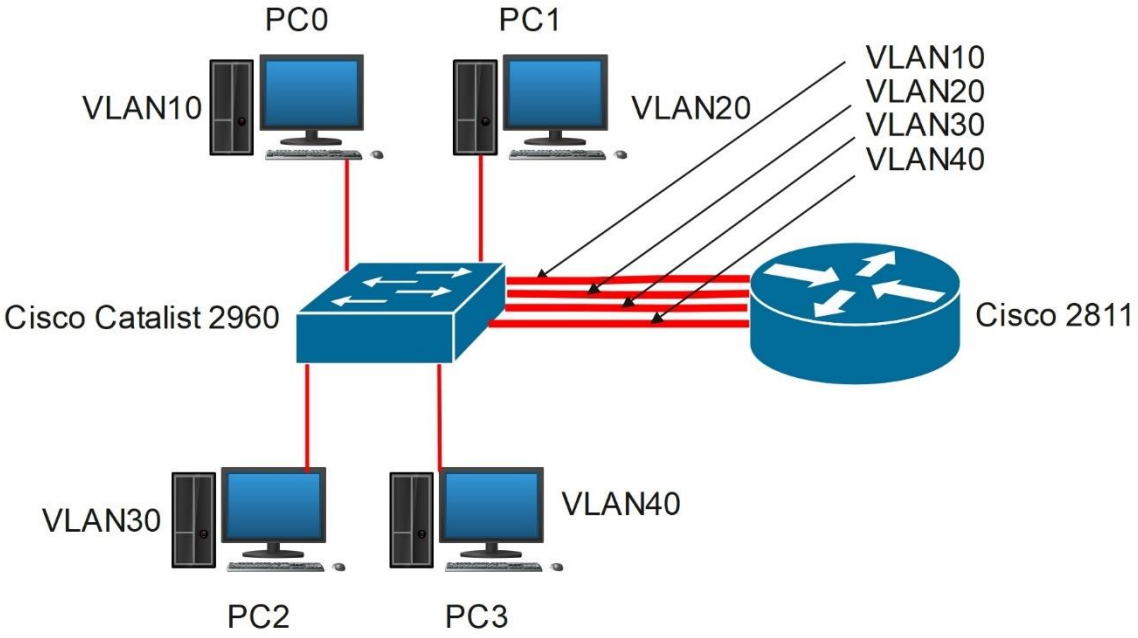


Рис. 2.14. Класичний метод маршрутизації між VLAN

Маршрутизатор повинне мати стільки портів, скільки в мережі застосовується VLAN. Порти комутатора, до яких підключається маршрутизатор в такій мережі, повинні працювати в режимі доступу і відповідно знаходиться в різних VLAN. Кожен порт маршрутизатора повинен мати налагоджену статичну IP-адресу, що належать відповідній віртуальній мережі. Ці адреси повинні використовуватися вузлами кожної віртуальної мережі в якості **шлюзу по замовчуванню (default gateway)**.

Комутатор в даному прикладі налаштовується наступними командами:
Спочатку потрібно створити віртуальні локальні мережі:

```
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
```

Далі призначаємо порти в ці віртуальні локальні мережі. До портів fa0/1, fa0/2, fa0/3, fa0/4 під'єднані комп'ютери, а порти fa0/5, fa0/6, fa0/7, fa0/8 під'єднані до маршрутизатора:

```
Switch(config)#int range fa0/1, fa0/5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)#int range fa0/2, fa0/6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)#int range fa0/3, fa0/7
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 30
Switch(config-if-range)#int range fa0/4, fa0/8
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 40
Switch(config-if-range)#^Z
Switch#
```

Перевіряємо результати конфігурування:

```
Switch#sh vlan bri
```

VLAN	Name	Status	Ports
1	default	active	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 Gigl/1, Gigl/2
10	VLAN0010	active	Fa0/1, Fa0/5
20	VLAN0020	active	Fa0/2, Fa0/6
30	VLAN0030	active	Fa0/3, Fa0/7
40	VLAN0040	active	Fa0/4, Fa0/8
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#

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#
```

Перевіряємо таблицю маршрутизації:

```
Router#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B –
       BGP,
```

```
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
        area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 4 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
C       10.1.2.0 is directly connected, FastEthernet0/1
C       10.1.3.0 is directly connected, FastEthernet1/0
C       10.1.4.0 is directly connected, FastEthernet1/1
Router#
```

Тепер залишилося лише налаштувати кінцеві вузли.

Можна побачити основний недолік застосування такої конфігурації – витрату портів як маршрутизатора, так і комутатора, до якого він підключається. Також проблема виникає при розширенні мережі – при додаванні нових віртуальних мереж, необхідно виділяти вільні порти на маршрутизаторі, що часто, при великій кількості мереж, проблематично.

2.5.2. Транковий метод маршрутизації між VLAN

Транковий метод маршрутизації між VLAN («Router on a stick») позбавлений попереднього недоліку – великої витрати портів (рис. 2.15).

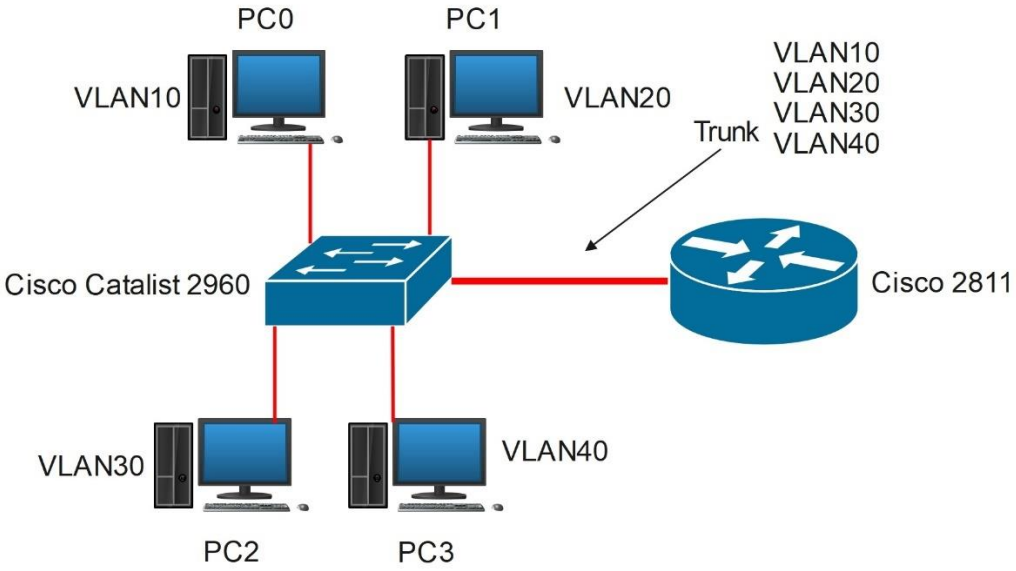


Рис. 2.15. Транковий метод маршрутизації між VLAN

Транковий метод використовує тільки один фізичний порт маршрутизатора і комутатора. При цьому порт комутатора працює в режимі транка (Trunk), по якому передається трафік всіх віртуальних мереж, який необхідно маршрутизувати. Порт маршрутизатора теж працює в режимі транка. При цьому фізичний інтерфейс приймає тегований трафік і розподіляє його між підінтерфейсами, які належать окремим VLAN. Такі інтерфейси є віртуальними і створюються для одного фізичного інтерфейсу. Кожен з них має IP-адресу, що належить відповідній віртуальній локальній мережі, і маршрутизатор передає трафік між ними згідно зі своєю таблицею маршрутизації.

Приклад конфігурації для цього типу маршрутизації.

Також як і в попередній конфігурації, створюємо віртуальні мережі і призначаємо в них інтерфейси, але тільки ті, до яких під'єднані кінцеві вузли. 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)#
```

Перевіряємо:

```
Switch#sh vlan bri

VLAN  Name                Status    Ports
1     default             active    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
                                    Gigl/1, Gigl/2
10    VLAN0010            active      Fa0/2
20    VLAN0020            active      Fa0/3
30    VLAN0030            active      Fa0/4
40    VLAN0040            active      Fa0/5
1002  fddi-default        active
1003  token-ring-default  active
1004  fddinet-default     active
1005  trnet-default       active
Switch#
```

Маршрутизатор в даному прикладі під’єднаний до інтерфейсу fa0/1, тому цей інтерфейс налаштовується як транк:

```
Switch(config-if)#int fa 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#^Z
Switch#
```

На маршрутизаторі створюємо віртуальні підінтерфейси, призначаємо для них тип інкапсуляції канального рівня IEEE 802.1Q, і задаєм номер віртуальної мережі командою режиму конфігурації підінтерфейсу encapsulation dot1q *vlan id*:

```
Router#conf t
Router(config)#int fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip addr 10.1.1.1 255.255.255.0
Router(config-subif)#int fa0/0.20
Router(config-subif)#ip addr 10.1.2.1 255.255.255.0
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#int fa0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip addr 10.1.3.1 255.255.255.0
Router(config-subif)#int fa0/0.40
Router(config-subif)#ip addr 10.1.4.1 255.255.255.0
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#int fa0/0
Router(config-if)#no sh
```

Перевіряємо таблицю маршрутизації:

```
Router#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B –
       BGP,
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
    10.0.0.0/24 is subnetted, 4 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0.10
C       10.1.2.0 is directly connected, FastEthernet0/0.20
C       10.1.3.0 is directly connected, FastEthernet0/0.30
C       10.1.4.0 is directly connected, FastEthernet0/0.40
Router#
```

Залишилось налаштувати кінцеві вузли.

Цей підхід до маршрутизації між VLAN має недолік – використання пропускної спроможності лише одного фізичного інтерфейсу для передачі

трафіку декількох віртуальних локальних мереж. Попередній підхід такого недоліку не мав, використання декількох незалежних інтерфейсів, навпаки, є його перевагою, оскільки віртуальні мережі не ділять пропускну спроможність одного каналу, а мають окремий канал до маршрутизатора. При виборі прийнятної схеми маршрутизації між VLAN, необхідно балансувати між пропускною спроможністю і вартістю, що виражається у використовуваних портах.

Існує ще й третій підхід, який пов'язаний із застосуванням комутаторів 3-го рівня. При застосування таких комутаторів потреба в зовнішніх маршрутизаторах відпадає. Комутатор має декілька **віртуальних інтерфейсів** (Switch Virtual Interface, **SVI**), які належать кожній з налаштованих VLAN і програмне забезпечення комутатора здійснює перенаправлення пакетів, що поступають на ці інтерфейси згідно з таблицею маршрутизації.

2.5.3. Пошук несправностей в конфігурації маршрутизації між VLAN

Помилки, що виникають при налаштуванні маршрутизації між VLAN можна умовно розділити на помилки в налаштуванні комутатора, помилки в налаштуванні маршрутизатора і помилки, пов'язані з неправильним призначенням адрес інтерфейсам.

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. Наприклад, інтерфейс маршрутизатора має адресу, що відповідає VLAN 10, а інтерфейс комутатора, до якого він підключений, знаходиться в VLAN 1. У такій ситуації трафік VLAN 10 не доходитиме до маршрутизатора і взаємодія цієї віртуальної мережі з іншими буде неможлива. Побачити якому VLAN належить порт, можна командою привілейованого режиму **interface *interface-id* switchport**. Для вирішення цієї проблеми необхідно відповідний порт комутатора додати в потрібну VLAN командою режиму конфігурації порту **switchport access vlan 10**.
- 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. Побачити чи являється порт транком, можна командою привілейованого режиму **interface *interface-id* switchport**. Виправляється подібна ситуація включенням транкового режиму на

потрібному інтерфейсі командою режиму конфігурації порту **switchport mode trunk**.

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. Ця проблема пов’язана з помилкою у фізичному під’єднані, і вирішується перепідключенням маршрутизатора в потрібний порт комутатора.
- У транковій конфігурації типовою помилкою є неправильне задання номера VLAN на підінтерфейсі при його конфігуруванні. У такій ситуації, при отриманні тегованого трафіку, маршрутизатор не матиме підінтерфейсу, якому його необхідно передавати далі. Побачити в якій віртуальній мережі знаходиться певний інтерфейс маршрутизатора, можна командою привілейованого режиму **show interface**. Вирішується така проблема виправленням номера VLAN підінтерфейсу.

Помилки, пов’язані з неправильним призначенням адрес інтерфейсам можуть відноситися до налаштування маршрутизатора або кінцевих вузлів.

2.6. Протокол VTP

2.6.1. Концепція VTP

Процес налаштування віртуальних мереж нескладний, якщо комутаторів їх небагато. Але при великій кількості комутаторів, завдання ручного налаштування списку віртуальних мереж дуже проблематичний. Для полегшення процесу налаштування віртуальних мереж на декількох комутаторах застосовується Cisco протокол **VLAN Trunking Protocol** – **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.

2.6.2. 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.

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.

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.

Інформація в самому повідомленні також залежить від його типу і містить декілька полів з інформацією глобального характеру – ім’я домена, ідентифікатор комутатора, що послав оголошення, цифровий підпис MD5 поточної конфігурації VLAN і формат кадру – ISL або IEEE 802.1Q.

У повідомленні може міститися наступна інформація про конфігурацію VLAN:

- VLAN ID.
- ім’я VLAN.
- тип VLAN.
- стан VLAN.
- додаткова інформація про налаштування VLAN.

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 мереж або перезавантаження комутатора.

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.

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**.

2.6.3 Конфігурування VTP

При налаштуванні комутаторів для використання VTP досить виконати декілька дій.

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)#
```

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.

З прикладу видно, що номер версії конфігурації 4, це говорить про відповідно чотирьох змінах у базі цих віртуальних мереж. Були створені 2 мережі і їм задано 2 імені. Створені мережі можна побачити командою **show vlan brief**.

```
Sw1#sh vlan bri
VLAN Name                        Status    Ports
1    default                     active    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, Gig1/1,
                                           Gig1/2

10 student                       active  Fa0/3
20 epmlovees                     active  Fa0/2, Fa0/4, Fa0/5
1002 fddi-default                active
1003 token-ring-default          active
1004 fddinet-default             active
1005 trnet-default               active
```

2.6.4. Пошук несправностей в роботі протоколу VTP

Типовими проблемами, з якими доводитися стикатися при налаштуванні протоколу VTP є несумісність версій VTP, неспівпадання паролів VTP, неправильно задане ім’я домена VTP, відсутність сервера (усі працюють як клієнти) і помилки пов’язані з версією конфігурації 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.

Приклад: Є домен VTP, в якому створені дві віртуальні мережі – vlan 10 і vlan 20. В ході налаштування, номер версії конфігурації збільшився до 10. В процесі розширення мережі до неї підключили комутатор, який деякий час не використовувався і в його конфігурації є присутнім правильний пароль і ім’я домена. При цьому, список його віртуальних мереж абсолютно інший – vlan 50 і vlan 60, а версія конфігурації має номер 15. Цей комутатор, в оголошеннях, що приходять до нього, визначить версію меншу, ніж є у нього і у своїх оголошеннях розішле свою конфігурацію, з більшим номером. Інші комутатори прийнявши оголошення з більшим номером, змінять інформацію у своїх базах віртуальних мереж, на ту, що вони отримають – vlan 10 і vlan 20 будуть видалені, а vlan 50 і vlan 60 додані. Таким чином, актуальна інформація буде видалена або спотворена.

Щоб уникнути такої ситуації, необхідно обнуляти номер версії конфігурації VTP. Виконується це налаштуванням нового імені домена VTP на комутаторі. При кожній зміні цього імені, версія конфігурації скидається до значення 0, і не впливатиме на інші комутатори домена.

3. Віртуальні приватні мережі

3.1. Послуги віртуальних приватних мереж

Сервіс **віртуальних приватних мереж** (Virtual Private Network, **VPN**) з'явився як більш економічна альтернатива сервісу виділених каналів, що використовується при побудові приватної комп'ютерної мережі. Канали віртуальної приватної мережі, так само як і виділені канали, з'єднують окремі мережі клієнта цієї послуги в єдину ізольовану мережу. Однак на відміну від виділених каналів, які будуються за допомогою техніки комутації каналів і мають фіксовану пропускну спроможність, канали віртуальної приватної мережі прокладаються всередині мережі з комутацією пакетів, такої як IP, MPLS або Ethernet.

На рис. 3.1 показаний приклад побудови корпоративної мережі клієнта А за допомогою сервісу віртуальної приватної мережі; канали являють собою з'єднання в мережах з комутацією пакетів операторів 1 і 2.

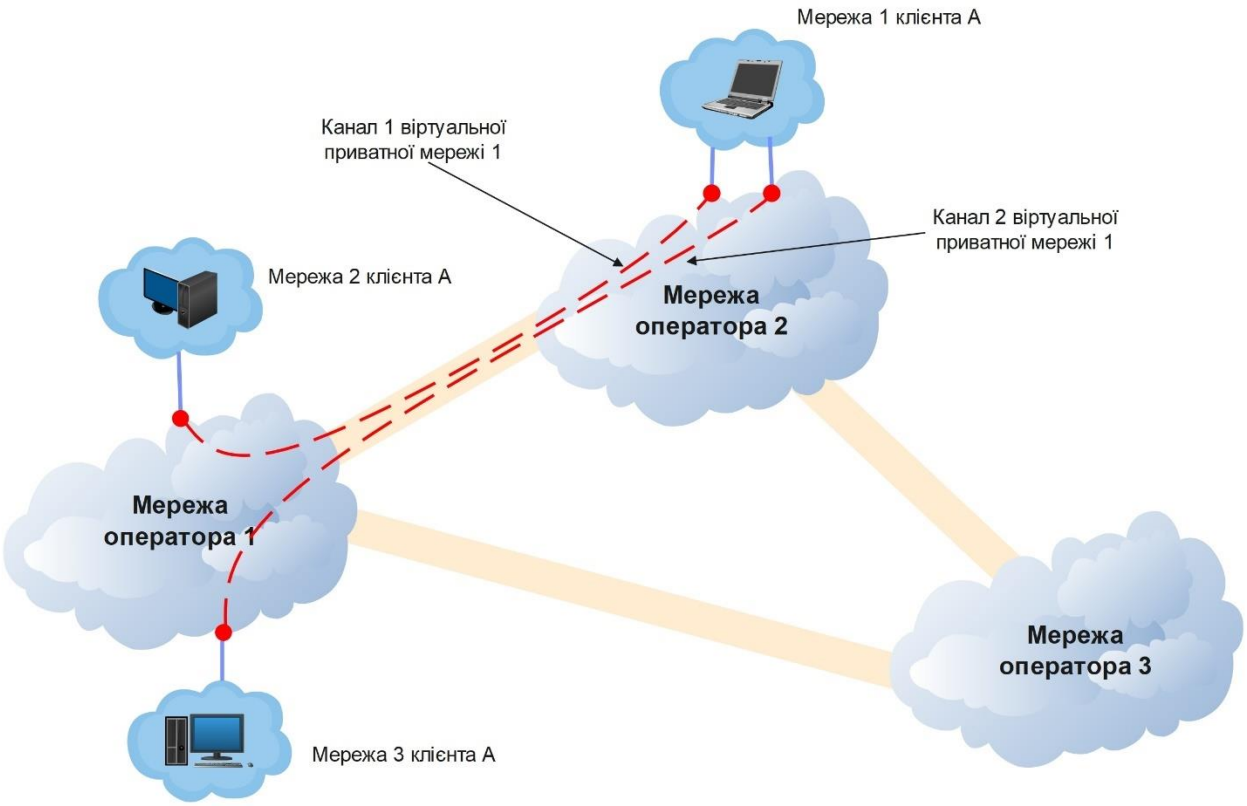


Рис. 3.1. Сервіс віртуальної приватної мережі

Технологія VPN дозволяє реалізувати сервіси, що наближаються до сервісів ізольованою приватної мережі за якістю, але на поділюваній між користувачами

інфраструктурі публічної мережі з комутацією пакетів.

Мережі користувача, які об'єднуються за допомогою послуги VPN називають також **сайтами**. Віртуальна приватна мережа імітує деякі властивості приватної мережі, що випливають з її ізольованості, використовуючи для цього інші технології. 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.

Різні технології VPN відрізняються набором властивостей приватної мережі, які вони імітують, а також ступенем наближення до якості цих властивостей. В залежності від того, хто реалізує послугу VPN, провайдер або клієнт, вони поділяються на два види.

У **підтримуваній клієнтом віртуальній приватній мережі** (Customer Provided Virtual Private Network, **CPVPN**) підтримку мережі VPN здійснює клієнт. Провайдер надає лише «прості» традиційні послуги загальнодоступної мережі по об'єднанню вузлів клієнта, наприклад доступ в Інтернет, а фахівці підприємства самостійно конфігурують засоби VPN і керують ними.

У **підтримуваній провайдером віртуальній приватній мережі** (Provider

Provisioned Virtual Private Network, **PPVPN**) провайдер послуг VPN на основі власної мережі відтворює приватну мережу для кожного свого клієнта, ізолюючи і захищаючи її від інших. Підтримувані провайдером мережі VPN зазвичай забезпечують більш ширший спектр імітованих властивостей приватної мережі, ніж підтримувані клієнтом. Це пояснюється тим, що провайдер має контроль над власною мережею і може застосувати в ній відповідну технологію і конфігурувати свої пристрої більш ефективно для надання послуг VPN. Клієнт такої можливості позбавлений, він може використовувати стандартний транспортний сервіс провайдера і надати йому властивості VPN завдяки спеціальній конфігурації своїх прикордонних пристроїв. Як правило, підтримувані клієнтом мережі VPN використовують шифрування трафіку і його тунелювання через Інтернет.

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.

Внутрішня реалізація VPN послуг другого рівня може бути різною, зараз провайдери найчастіше використовують в цих цілях такі технології, як Carrier Ethernet (тобто технології PB, PBB і PBB-TE) і MPLS. Ці дві популярні реалізації послуг VPN другого рівня отримали назви **Ethernet over Ethernet (EoE)** і **Ethernet over MPLS (EoMPLS)**. Наявність у цих послуг інтерфейсу Ethernet дає їм ще одну назву – **Ethernet VPN**.

Стандартизація послуг Ethernet VPN – це важливий напрямок робіт в області Ethernet операторського класу, що дозволяє провайдерам і користувачам однозначно описувати послуги, не вдаючись у деталі їх внутрішньої реалізації. Роботою по створенню специфікацій Ethernet VPN займається організація Metro Ethernet Forum (MEF).

У специфікаціях MEF вводиться три типи послуг віртуальних приватних мереж Ethernet, які відрізняються топологією зв'язків між сайтами користувачів. Для того, щоб формалізувати топологію зв'язків, вводиться поняття **віртуального з'єднання Ethernet** (Ethernet Virtual Circuit, **EVC**). Кожне з'єднання EVC пов'язує сайти користувачів в окрему віртуальну приватну мережу, об'єднуючи мережеві інтерфейси користувачів (UNI).

Відповідно є три типи з'єднань EVC (рис 3.2.):

- «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.

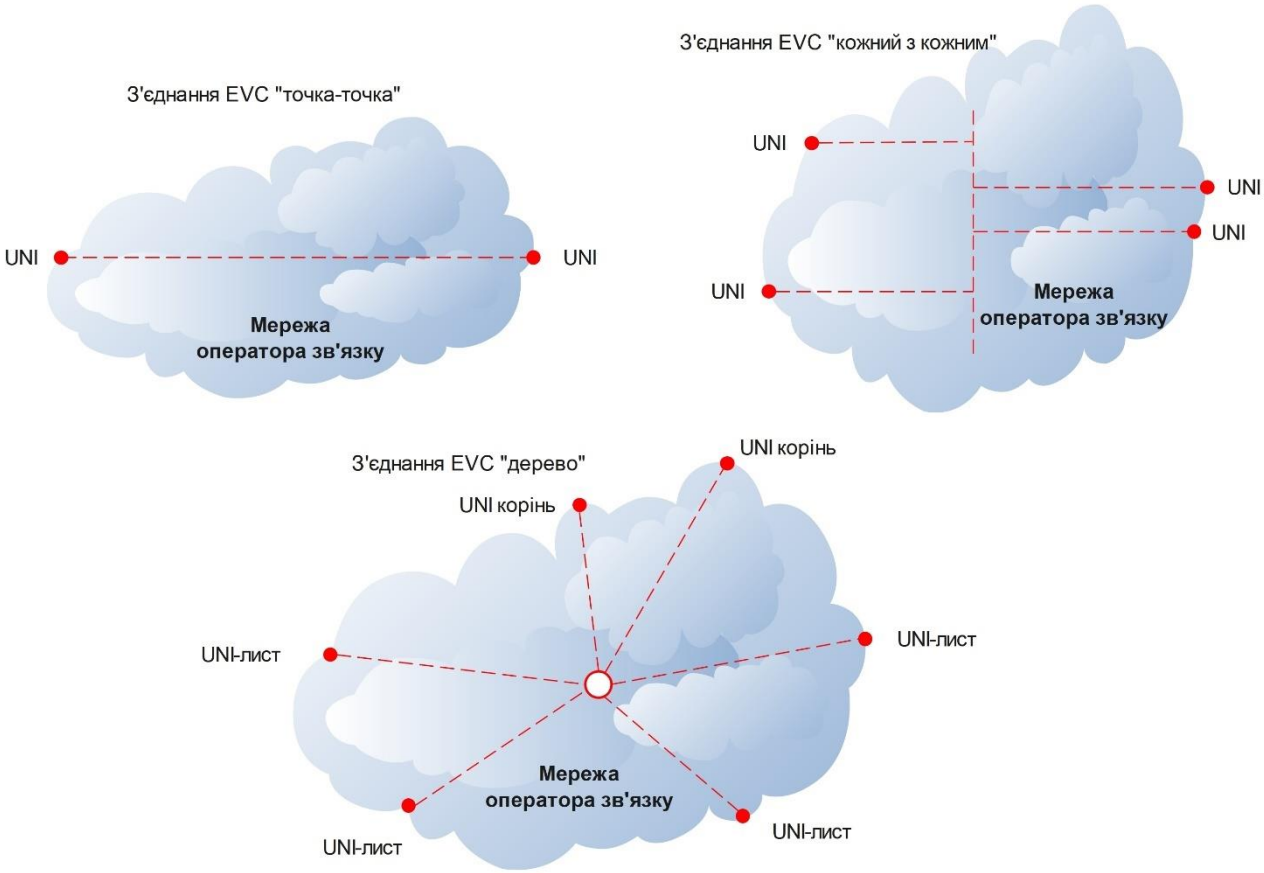


Рис. 3.2. Три типи з’єднань EVC

- **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.

Крім того, в специфікаціях MEF вводяться два варіанти кожного типу послуги. У першому варіанті користувацький сайт визначається як мережа, що під'єднана до окремого фізичного інтерфейсу UNI. Значення ідентифікаторів VLAN в користувацьких кадрах (тобто значення C-VID в термінології PB/PBB/PBB-TE) в розрахунок не приймаються. У назві цього варіанту послуги до назви типу додається термін «приватний» (private): наприклад, для послуги типу E-LINE цей варіант називають приватної лінією Ethernet (Ethernet Private Line, **EPL**), а для послуги E-LAN – приватною локальною мережею Ethernet (Ethernet Private LAN, **EPLAN**).

В другому варіанті послуги до одного і того ж фізичному інтерфейсу UNI можуть бути під'єднані різні користувацькі сайти. У цьому випадку вони розрізняються за значенням ідентифікатора VLAN (C-VID). Провайдер всередині своєї мережі зберігає поділ локальної мережі на VLAN, зроблене користувачем. У варіанті послуги з урахуванням VLAN додається назва «віртуальна приватна»: наприклад, для послуги типу E-LINE це буде віртуальна приватна лінія Ethernet (Ethernet Virtual Private Line, **EVPL**), а для послуги E-LAN – віртуальна приватна локальна мережа Ethernet (Ethernet Private LAN, **EVPLAN**).

Технології Carrier Ethernet Transport (PB, PBB і PBB-TE) надають послуги Ethernet VPN безпосередньо, без додаткових надбудов і механізмів, вони і розроблялись для цієї мети. Мережі PB і PBB можуть надавати послуги E-LINE (при з'єднанні двох користувацьких сайтів) і E-LAN (при з'єднанні більш ніж двох користувальницьких сайтів), а мережі PBB-TE – тільки послуги E-LINE. Послуги E-TREE жодна з цих технологій не підтримує.

3.2. Технологія MPLS VPN рівня другого

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.

3.2.1. Псевдоканали

Стандарти IETF описують два типи послуг Ethernet VPN, які будуються за допомогою технології MPLS: **VPWS** (Virtual Private Wire Service) і **VPLS** (Virtual Private LAN Service). Різниця між цими послугами полягає в тому, що VPWS емулює з'єднання Ethernet з двоточковою топологією, тобто канал Ethernet, а

VPLS емулює поведінку локальної мережі, тобто забезпечує з'єднання з повнозв'язною топологією як звичайна локальна мережа Ethernet. Якщо використовувати термінологію MEF, то послуга VPLS відповідає послузі E-LAN, а послуга VPWS – E-LINE.

Обидві послуги є послугами MPLS VPN другого рівня (**MPLS L2VPN**), так як вони дозволяють надавати послуги VPN, взаємодіючи з користувацькими мережами на другому рівні.

Дані послуги базуються на використанні **псевдоканалів** (pseudowire), які з'єднують прикордонні маршрутизатори провайдера. На рис. 3.3 показано три таких псевдоканали, що з'єднують між собою прикордонні маршрутизатори PE1-PE4 (PE – Provider Edge).

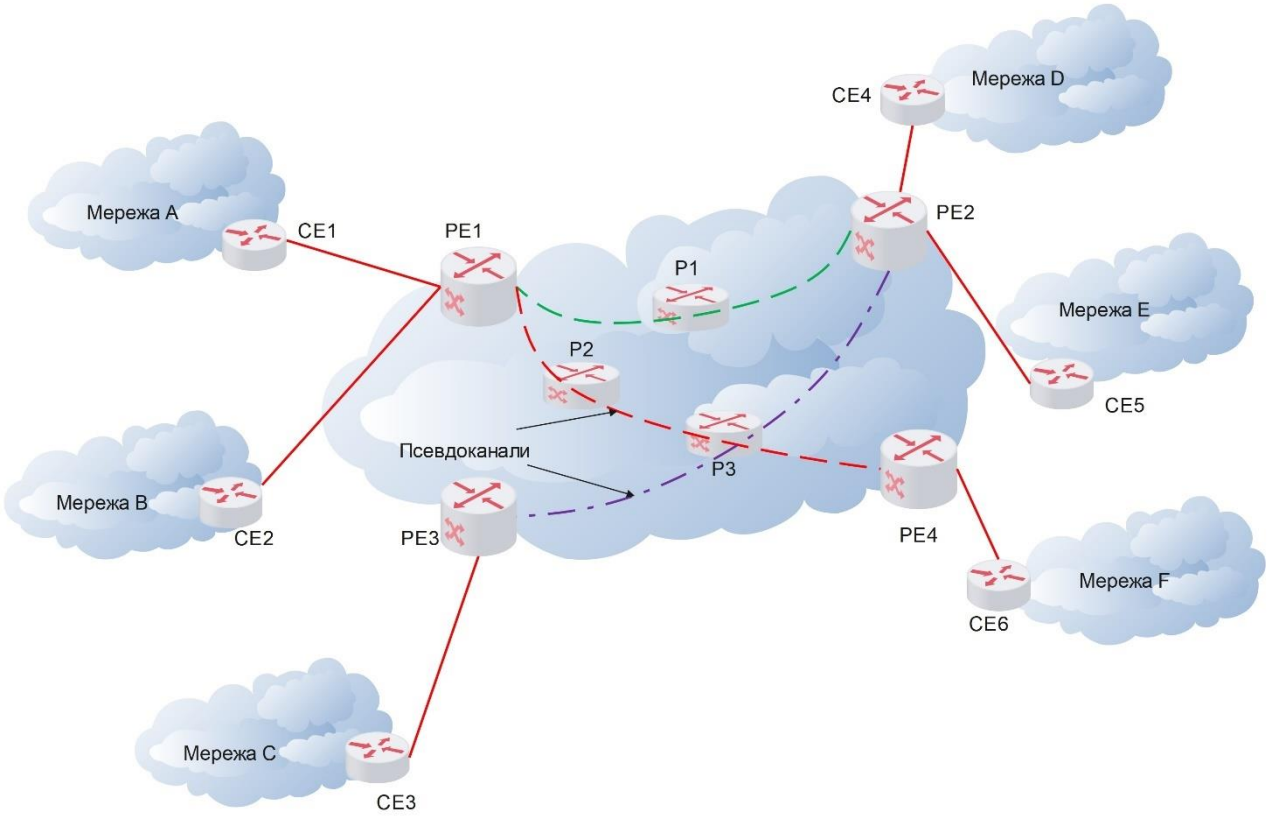


Рис. 3.3. Псевдоканали в мережі провайдера

Псевдоканали являють собою шляхи LSP другого рівня ієрархії (внутрішній рівень), прокладені всередині LSP першого (зовнішнього) рівня. Зазвичай, в якості LSP першого рівня ієрархії використовуються TE-тунелі MPLS. На рисунку шляхи LSP першого рівня не показані.

Псевдоканали – це логічні транспортні з'єднання, які фізично можуть проходити через проміжні магістральні маршрутизатори, однак для них вони прозорі. Тобто, в прикладі на рис. 11.3, маршрутизатори P1, P2 і P3 просто не

помічають існування псевдоканалів в мережі.

Псевдоканал – це механізм, який емулює властивості будь-якого телекомунікаційного сервісу через мережу з комутацією пакетів.

Одним з варіантів застосування псевдоканалів при емуляції послуг Ethernet є передача псевдоканалом трафіку одного користувача з'єднання, при цьому псевдоканал емулює кабельне з'єднання між мережами користувачів. У прикладі на рисунку псевдоканал PW2 служить для організації з'єднання між мережами A і F через мережу провайдера. При цьому кадри Ethernet, що відправляються мережею A в мережу F, інкапсулюються прикордонним маршрутизатором PE1 в дані псевдоканала і доставляються ним прикордонному маршрутизатору PE2, який витягує ці кадри і відправляє їх у мережу F в початковому вигляді.

Призначення псевдоканала ширше ніж просто емуляція Ethernet, – це може бути і емуляція сервісів виділених каналів технологій PDH або SDH, і емуляція віртуальних каналів ATM або Frame Relay; проте в будь-якому випадку емуляція такої послуги виконується через пакетну мережу. Тип пакетної мережі також не уточнюється, так що це може бути і класична мережу IP (без MPLS), і мережа IP/MPLS, і мережа ATM. Головне в цьому узагальненому визначенні те, що псевдоканал приховує від користувачів емульованого сервісу деталі пакетної мережі провайдера, поєднуючи користувацькі прикордонні пристрої (CE на рис. 10.3) таким чином, як ніби вони з'єднувалися за допомогою виділеного каналу або кабелю.

Технічно створити LSP другого рівня досить просто – для цього в маршрутизаторах, з'єднаних LSP першого рівня, потрібно задати значення мітки другого рівня, яке буде використовуватися, щоб розрізняти LSP другого рівня всередині LSP першого рівня. Цей процес ілюструє рис. 3.4. На ньому зображені два прикордонних маршрутизатори PE1 і PE2, з'єднані псевдоканалом PE57. Як видно з рисунку, замість одного шляху LSP першого рівня є два таких шляхи. Це пов'язано з тим, що двоточкові псевдоканали, які служать для емуляції Ethernet, за визначенням IETF завжди є двонаправленими, а MPLS LSP – це однонаправлений шлях. Тому, для створення двонаправленого псевдоканалу потрібно два однонаправлених шляхи другого рівня, вкладених в два однонаправлених шляхи першого рівня, що і показано на рисунку.

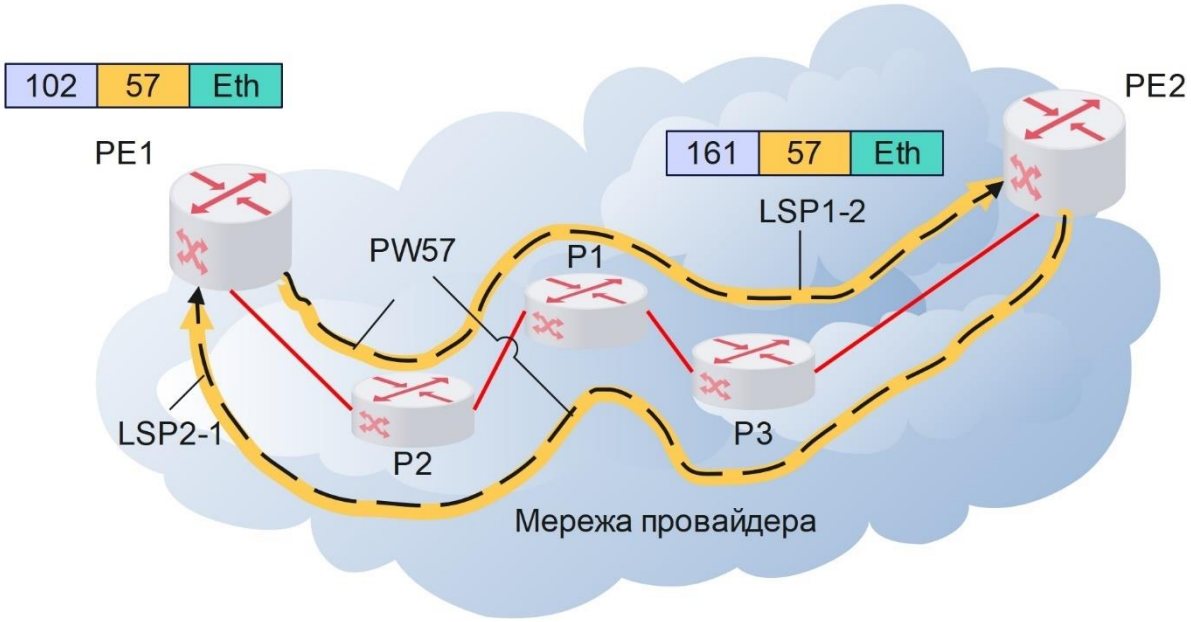


Рис. 3.4. Створення псевдоканалу всередині тунелей MPLS

Розглянутий в прикладі псевдоканал в напрямку від PE1 до PE2 ідентифікується міткою 57, а тунель, який використовує цей канал, – міткою 102. Тому, при відправці кадру Ethernet, призначеного для PE2, маршрутизатор PE1 поміщає початковий кадр Ethernet в кадр MPLS і адресує цей кадр двома мітками: зовнішньою міткою 102 і внутрішньою міткою 57. Зовнішня мітка застосовується потім магістральними маршрутизаторами P1, P2 і P3 для того, щоб доставити кадр прикордонному маршрутизатору PE2, при цьому в процесі передачі кадру відбувається звичайна комутація по мітках (на рисунку показано, що після проходження P1 зовнішня мітка отримала значення 161).

Внутрішня мітка 57 потрібно лише прикордонному маршрутизатора PE2, який знає, що ця мітка відповідає псевдоканалу PW57, необхідному для зв’язку з деякою користувацькою мережею.

Однією з суттєвих переваг псевдоканалів є те, що в мережі провайдера потрібно конфігурувати лише порівняно невелику кількість тунелів між прикордонними маршрутизаторами, а потім використовувати кожен з них для прокладки необхідної кількості псевдоканалів. Створення нового псевдоканала вимагає конфігурування, але тільки пари прикордонних маршрутизаторів, які є кінцевими точками псевдоканала. Подібна схема застосовується в мережах PBB і PBB-TE, де роль псевдоканалів відіграють з’єднання I-SID.

Іншою перевагою псевдоканалів є їх універсальність, тобто можливість їх застосування не тільки в мережах MPLS, але і в мережах інших типів, таких як

IP-мережі з тунелюванням і не лише при емуляції Ethernet, але і при емуляції інших сервісів (наприклад, каналів PDH).

3.2.2. 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. 3.5).

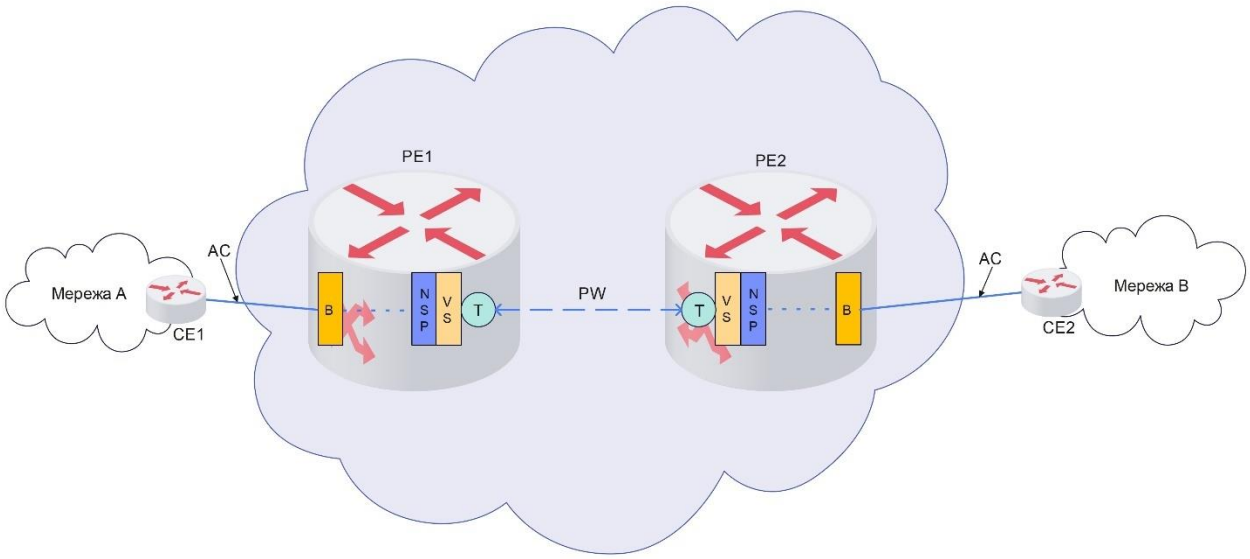


Рис. 3.5. Організація віртуально приватного каналу Ethernet

Найчастіше користувацькі мережі з'єднують ся з прикордонним маршрутизатором провайдера через виділений інтерфейс, який для глобальних послуг Ethernet повинен бути стандартним інтерфейсом Ethernet, наприклад 1000Base-LX. В цьому випадку послуга VPWS полягає в прозорому з'єднанні цих інтерфейсів, коли мережа провайдера передає всі кадри, які надходять на такий інтерфейс від мережі користувача. Іноді цей режим називають комутацією портів користувача. У термінології MEF це послуга EPL.

Можливий і інший варіант послуги VPWS, коли мережа провайдера з'єднує віртуальні користувацькі мережі, тобто по двоточковому з'єднанню передаються не всі кадри, що надходять через інтерфейс користувача, а тільки кадри, що належать певній мережі VLAN. Цей режим роботи VPWS можна назвати комутацією віртуальних локальних мереж, або VLAN-комутацією. У термінології MEF це послуга EVPL.

Для того, щоб узагальнити поняття інтерфейсу з користувачем, форум IETF

ввів термін **канал приєднання** (Attachment Circuit, AC). AC поставляє вхідний потік даних користувача для мережі провайдера, тобто те навантаження, яке потрібно комутувати. Послуга VPWS завжди з'єднує два користувацьких канали приєднання.

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. Його роль в схемі емуляції – виділення кадрів Ethernet із загальних потоків, що надходять на порти маршрутизатора, для передачі в псевдоканал. Тим самим модуль моста формує логічний інтерфейс віртуального комутатора. Наприклад, якщо це режим комутації портів, то модуль моста конфігурується так, щоб всі кадри, які прийшли на відповідний порт від користувача, прямували для подальшої обробки в псевдоканал. Якщо ж це VLAN-комутація, то модуль моста вибирає для передачі псевдоканалу тільки кадри, помічені певним значенням тегу VLAN.

Вибрані модулем моста кадри надходять в псевдоканал через два проміжних модуля – NSP і VS. Модуль NSP (Native Service Processing) забезпечує попередню обробку кадрів Ethernet. Найчастіше така обробка пов'язана зі зміною або додаванням тегу VLAN, що може знадобитися, наприклад, якщо об'єднуються користувацькі мережі, що застосовують різні значення VLAN для однієї і тієї ж віртуальної мережі. Модуль VS (Virtual Switch) комутує один з каналів приєднання з одним із псевдоканалів. Для послуги VPWS цей модуль працює «вхолосту», виконуючи постійну комутацію єдиного каналу приєднання з єдиним псевдоканалом.

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.

Процедуру інкапсуляції і формат результуючого кадру визначає специфікація RFC 4448.

У вихідного кадру відкидаються поля преамбули та контрольної суми, після чого він поміщається в кадр MPLS з двома полями міток: зовнішньою (мітка тунелю) і внутрішньою (мітка псевдоканалу).

Конфігурування псевдоканалів, тобто узгодження внутрішніх міток, що використовуються для ідентифікації та мультиплексування псевдоканалів всередині тунелю, може бути автоматизовано. Для цього застосовують протокол LDP або BGP. Прокладання псевдоканалу та прокладання тунелю – це два

незалежні процеси, тунель може бути прокладений, наприклад, за допомогою протоколу RSVP-TE, а псевдоканали в ньому – за допомогою протоколу LDP.

Протокол LDP служить також для повідомлення одним маршрутизатором PE іншого про зміну стану «працездатний-непрацездатний» псевдоканалу або каналу приєднання. Це дуже корисна властивість, так як без неї віддалений маршрутизатор PE не впізнає про відмову безпосередньо не приєднаних до нього відрізків емульованого транспортного з'єднання і буде намагатися його використати, посилаючи дані. Протокол LDP дозволяє в разі такої відмови відкликати мітку, раніше призначену псевдоканалу.

Гарантована пропускна здатність, забезпечується за допомогою техніки інжинірингу трафіку, що базується на відповідні властивості тунелів MPLS. Параметрами якості обслуговування (QoS) для віртуальних з'єднань VPWS можуть бути забезпечені за допомогою стандартних механізмів QoS, таких як, наприклад, пріоритетне обслуговування, профілювання трафіку, контроль доступу і резервування ресурсів. Детермінованість маршрутів тунелів MPLS робить контроль доступу більш визначеною процедурою, ніж в разі IP-мереж з їх розподіленим механізмом вибору маршрутів.

3.2.3. 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.

Так само як і в разі VPWS, сервіс VPLS організований на базі псевдоканалів. Відмінність полягає в тому, що для кожного VPLS використовується окремий набір псевдоканалів. При цьому кожен такий набір має повнозв'язну топологію, тобто всі прикордонні маршрутизатори PE, які беруть участь в роботі якогось екземпляра VPLS, пов'язані один з одним.

На рис. 3.6 показаний приклад мережі провайдера, що емулює два сервіси VPLS. Користувацькі мережі N1, N5 і N8 відносяться до VPLS сервісу «A», а мережі N2, N3, N4, N6 і N7 – до сервісу «B». Відповідно набір псевдоканалів PW-B1, PW-B2 і PW-B3 об'єднує прикордонні маршрутизатори, до яких під'єднані мережі сервісу «A» VPLS, а набір псевдоканалів PW-W1, PW-W2 і PW-W3 - маршрутизатори, до яких під'єднані мережі сервісу «B»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).

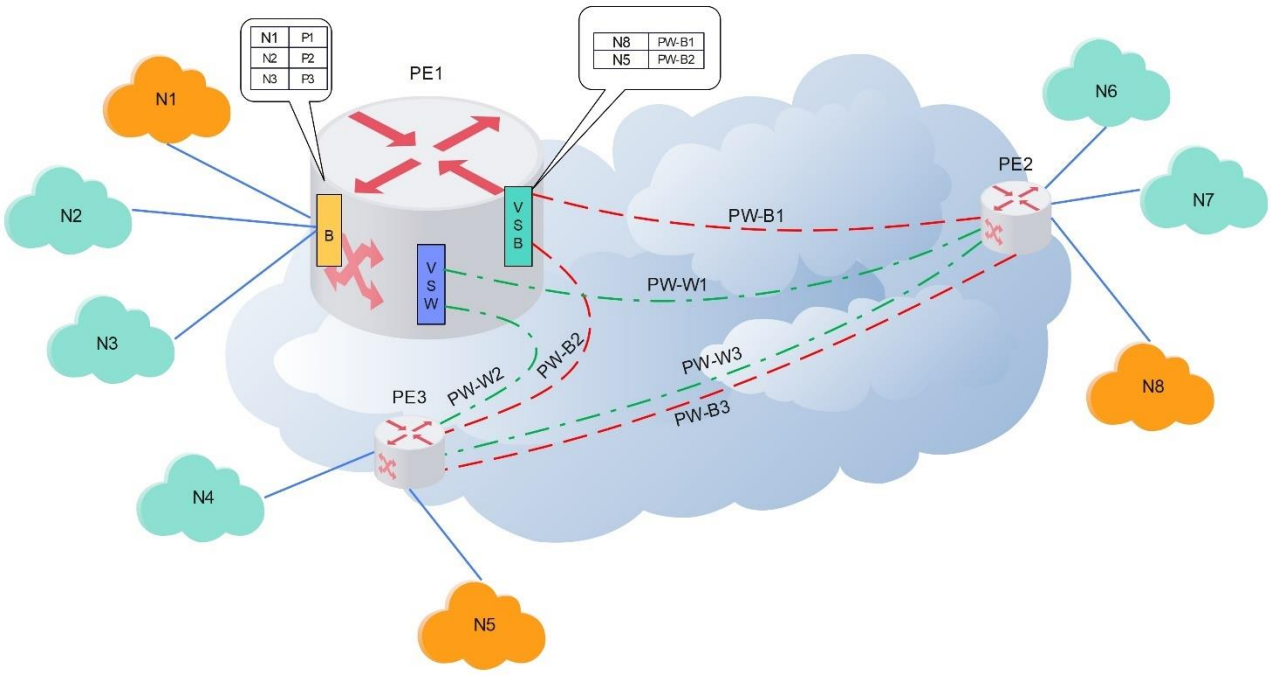


Рис. 3.6. Організація послуг VPLS

Внутрішня організація прикордонного маршрутизатора при наданні послуги VPLS показана на прикладі маршрутизатора PE1. Для підтримки кожного екземпляру сервісу VPLS прикордонному маршрутизатору потрібен окремий віртуальний комутатор, в даному випадку це модулі VSB і VSW (NSP модулі не показані, але вони входять в PE1, по одному на кожен екземпляр VPLS). Як і в разі VPWS, модуль B виконує стандартні функції моста і при цьому формує логічний інтерфейс з кожним з віртуальних комутаторів. Цей інтерфейс може також формуватися на основі комутації або користувацьких портів, коли весь трафік від певного порту (або декількох портів) передається на логічний інтерфейс, або мереж VLAN, коли вибираються кадри однієї (або декількох) користувацьких VLAN від одного або декількох портів.

Однак, якщо в разі VPWS віртуальний комутатор виконував просту роботу по передачі кадрів від логічного інтерфейсу, то для VPLS цей модуль функціонує за алгоритмом стандартного комутатора (моста). Для цього віртуальний комутатор вивчає MAC-адреси і будує свою таблицю просування, як і звичайний комутатор. На рисунку показаний спрощений вид таблиці просування PE1, що складається з двох записів: один запис пов’язує адресу M8 мережі N8 з псевдоканалом PW-B1, інший – адресу M5 мережі N5 з псевдоканалом PW-B2. Користуючись такою таблицею віртуальний комутатор, отримуючи кадри з адресами M5 або M8, спрямовує їх в псевдоканал, що веде до прикордонного комутатора, до якого під’єднана мережа з вузлом призначення. Кадри з широкотрансляційною адресою або адресою, що відсутня в таблиці просування,

надходять на всі його псевдоканали, в даному випадку – на PW-B1 і PW-W1.

Єдиною особливістю віртуального комутатора є те, що він не вивчає адреси відправлення кадрів, що приходять з логічного інтерфейсу.

Ця операція не потрібна, тому що для інтерфейсів, представлених псевдоканалами, віртуальний комутатор працює по правилу розщеплення горизонту (split horizon) – він ніколи не передає на псевдоканал кадри, отримані від будь-якого псевдоканалу. Тим самим запобігає утворенню петель між віртуальними комутаторами, а доставку кадрів за призначенням гарантує повнозв'язна топологія. Тобто будь-який кадр, що отриманий віртуальним комутатором по псевдоканалу, завжди передається на логічний інтерфейс користувача, що відповідає тому сервісу VPLS, до якого належить псевдоканал.

Модуль моста B вивчає тільки адреси, що приходять з користувацьких інтерфейсів. Вони служать йому для вибору потрібного інтерфейсу в тому випадку, коли кілька користувацьких мереж відносяться до одного сервісу VPLS.

Конфігурація PE може виявитися трудомістким заняттям, так як в разі N прикордонних маршрутизаторів потрібно створити $N\times(N-1)/2$ псевдоканалів. Крім того, додавання будь-якого нового пристрою PE вимагає переконфігурування всіх інших маршрутизаторів. Для автоматизації цих процедур використовують варіант організації VPLS, описаний в RFC 4761, так як він передбачає застосування для цієї мети протоколу BGP. Варіант VPLS, описаний в RFC 4762, розглядає розподіл міток другого рівня ієрархії за допомогою протоколу LDP, автоматизацію процедур конфігурування він не підтримує.

3.3. 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.

3.3.1. Розмежування маршрутної інформації

Кожен прикордонний маршрутизатор PE обмінюється маршрутною інформацією із з'єднаними з ним клієнтськими маршрутизаторами CE по якомусь протоколу маршрутизації класу IGP, наприклад OSPF або IS-IS (рис. 3.7). З кожним з клієнтів може використовуватися свій протокол IGP, тобто з сайтом A – протокол OSPF, а з сайтом B – IS-IS протокол. За допомогою цих протоколів маршрутизатор дізнається про те, які мережі досяжні в сайтах клієнтів. Крім того, маршрутизатор PE підтримує сеанс протоколу IGP з іншими маршрутизаторами мережі провайдера (як P, так і PE) для того, щоб знати топологію цієї мережі і маршрутизувати пакети в межах цієї мережі.

Для коректної роботи VPN потрібно, щоб інформація про маршрути через мережу провайдера не поширювалась за її межі, а відомості про маршрути в клієнтських сайтах не ставали відомими за межами певних мереж VPN.

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.

Можна уявити, що через маршрутизатор PE проходить невидима межа між зоною клієнтських сайтів і зоною ядра мережі провайдера. По один бік розташовуються інтерфейси, через які PE взаємодіє з маршрутизаторами P, а по інший – інтерфейси, до яких під'єднуються сайти клієнтів. З одного боку на PE надходять оголошення про маршрутах в мережі провайдера, з іншого – оголошення про маршрути в мережах клієнтів.

На рис. 11.7 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.

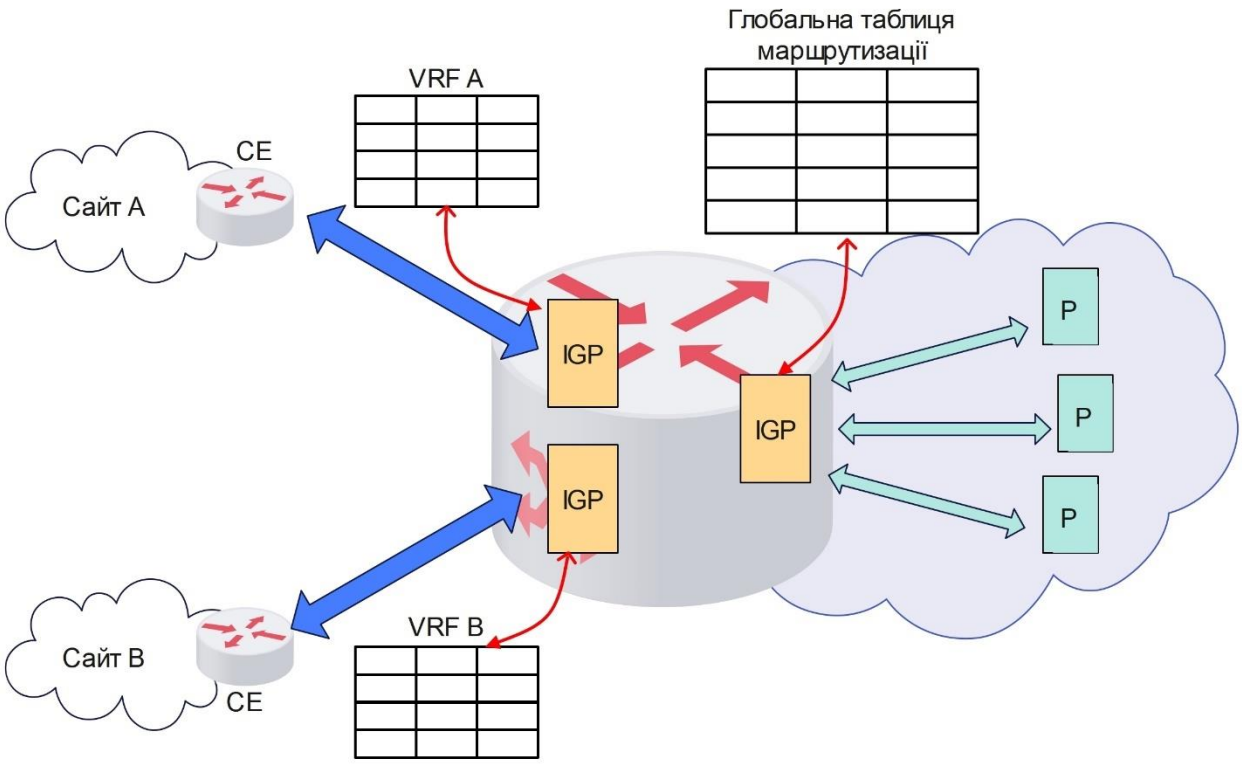


Рис. 3.7. Розмежування маршрутних оголошень в мережі MPLS VPN третього рівня

Аналогічним чином налаштовані і інші маршрутизатори PE. Таблиця маршрутизації, яка створюється на прикордонних маршрутизаторах PE на основі оголошень з магістральної мережі провайдера, має спеціальну назву: **глобальна таблиця маршрутизації**. У ній містяться маршрути в межах внутрішньої мережі провайдера, інформації про маршрути в мережах клієнтів в ній немає. Таблиці маршрутизації, які PE формує на основі оголошень, що надходять від сайтів клієнтів, отримали назву **таблиць VRF** (VPN Routing and Forwarding). У них є тільки інформація про мережах клієнтів.

Маршрутизатори P приймають і обробляють маршрутну інформацію IGP, яка поступає з усіх інтерфейсів. У створюваних ними таблицях маршрутизації є інформація тільки про мережі провайдера.

Сайти клієнтів є звичайними мережами IP, маршрутна інформація в яких може передаватися і оброблятися за допомогою будь-якого протоколу маршрутизації IGP класу. Маршрутні оголошення вільно поширюються між вузлами в межах кожного сайту до тих пір, поки не доходять до прикордонних маршрутизаторів PE, яка є перешкодою для їх подальшого поширення.

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.

Дещо спрощуючи, можна вважати, що на кожному маршрутизаторі PE створюється стільки таблиць VRF, скільки сайтів до нього під’єднано. Фактично на маршрутизаторі PE організовується кілька віртуальних маршрутизаторів, кожен з яких працює зі своєю таблицею VRF. Можливе й інше співвідношення між сайтами і таблицями VRF. Наприклад, якщо до деякого маршрутизатора PE під’єднано кілька сайтів однієї і тієї ж мережі VPN, то для них може бути створена загальна таблиця VRF. На рис. 11.7 показані дві таблиці VRF, одна з яких містить опис маршрутів до вузлів сайту A, а інша – до вузлів сайту B. До кожної такої таблиці можна отримати доступ тільки з сайтів, що належать до цієї ж мережі VPN.

3.3.2. Обмін маршрутною інформацією

Щоб зв’язати територіально розосереджені сайти замовника в єдину мережу, необхідно, по-перше, створити для них спільний простір поширення маршрутної інформації, а по-друге, прокласти у внутрішній мережі шляхи, по яких вузли, що належать різним сайтам однієї і тієї ж мережі VPN, могли б вести обмін даними захищеним чином.

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.

Особливість протоколу BGP і його розширень полягає в тому, що він отримує і передає свої маршрутні оголошення не всім безпосередньо під’єднаним до нього маршрутизаторам, як протоколи IGP, а тільки тим, які вказані в конфігураційних параметрах як сусіди. Маршрутизатори PE сконфігуровані так, що всі одержувані від клієнтських сайтів маршрутні оголошення вони за допомогою MP-BGP пересилають певним прикордонним маршрутизаторам PE. Питання про те, кому відправляти маршрутні оголошення, а кому ні, цілком залежить від топології віртуальних приватних мереж, які підтримуються даним провайдером.

Таким чином, крім маршрутів, що надходять від безпосередньо приєднаних до PE сайтів, кожна таблиця VRF доповнюється маршрутами, які отримуються

від інших сайтів даної мережі VPN за протоколом MP-BGP. Поширення маршрутів між маршрутизаторами PE забезпечується належним вибором атрибутів протоколу MP-BGP (ці атрибути описані в RFC 4360).

3.3.3. Незалежність адресних просторів сайтів

Однією з властивостей приватних мереж є незалежність їх адресних просторів. MPLS VPN третього рівня імітують цю властивість, дозволяючи використовувати один і той же адресний простір, наприклад простір приватних IP-адрес, в усіх екземплярах VPN провайдера. При цьому в межах однієї і тієї ж мережі VPN адреси не повинні повторюватися, інакше сайти не зможуть взаємодіяти один з одним.

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. Орієнтація на глобальну унікальність адрес виражається в тому, що, отримавши чергове маршрутне оголошення, протокол BGP аналізує його, не звертаючи уваги на те, до якої мережі VPN належить отриманий маршрут. Якщо на вхід протоколу BGP надходять описи маршрутів до вузлів різних мереж VPN, але із адресами IPv4, що співпадають, то протокол BGP вважає, що всі вони ведуть до одного і того ж вузла, а отже, як і потрібно в такому випадку, він поміщає в відповідну таблицю VRF тільки один найкоротший маршрут.

Проблема вирішується за рахунок застосування замість потенційно неоднозначних адрес IPv4 розширених і однозначних адрес нового типу, а саме адрес VPN-IPv4, які отримуються в результаті перетворення вихідних адрес IPv4. Перетворення полягає в тому, що до всіх адрес IPv4, що становлять адресний простір певної мережі VPN, додається префікс – **розрізнювач маршрутів** (Route Distinguisher, **RD**). RD унікально ідентифікує кожну мережу VPN. В результаті на маршрутизаторі PE всі адреси, що відносяться до різних мереж VPN, обов'язково будуть відрізнятися одна від одної, навіть якщо у них співпадають IPv4 адреси.

Розширений протокол MP-BGP має здатність переносити в маршрутних оголошеннях адреси різних типів, в тому числі IPv6, IPX, а також VPN-IPv4. Адреси VPN-IPv4 використовуються лише для маршрутів, якими маршрутизатори PE обмінюються по протоколу BGP. Перш ніж передати своєму сусіду деякий маршрут, вхідний маршрутизатор PE додає до його адреси призначення IPv4 префікс RD для даної мережі VPN, тим самим перетворюючи

його в маршрут VPN-IPv4.

На рис. 3.8 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. Тільки завдяки цим додаванням протокол BGP, що працює на віддалених маршрутизаторах PE, здатний розрізняти маршрути з співпадаючими адресами IPv4, що відносяться до різних мереж VPN.

Коли вихідний маршрутизатор PE отримує маршрут до мережі VPN-IPv4, він робить зворотне перетворення, відкидаючи префікс RD, і тільки потім поміщає маршрут в таблицю VRF і оголошує його з'єднаному з ним маршрутизатору клієнта CE з даної мережі VPN. Таким чином, всі маршрути в таблицях VRF містять адреси у форматі IPv4.

3.3.4. 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. Наприклад, в MPLS VPN третього рівня можна створити топологію «зірка», в якій периферійні сайти можуть взаємодіяти з центральним сайтом, а між собою ні, – цю топологію сервіс MPLS VPN другого рівня забезпечити не може.

Така гнучка форма створення топології VPN досягається за рахунок атрибутів експорту-імпорту маршрутів в оголошеннях MP-BGP. Атрибут **route-target (RT)** ідентифікує набір сайтів, що входять в дану мережу VPN (VRF), яким маршрутизатор PE повинен посилати маршрути.

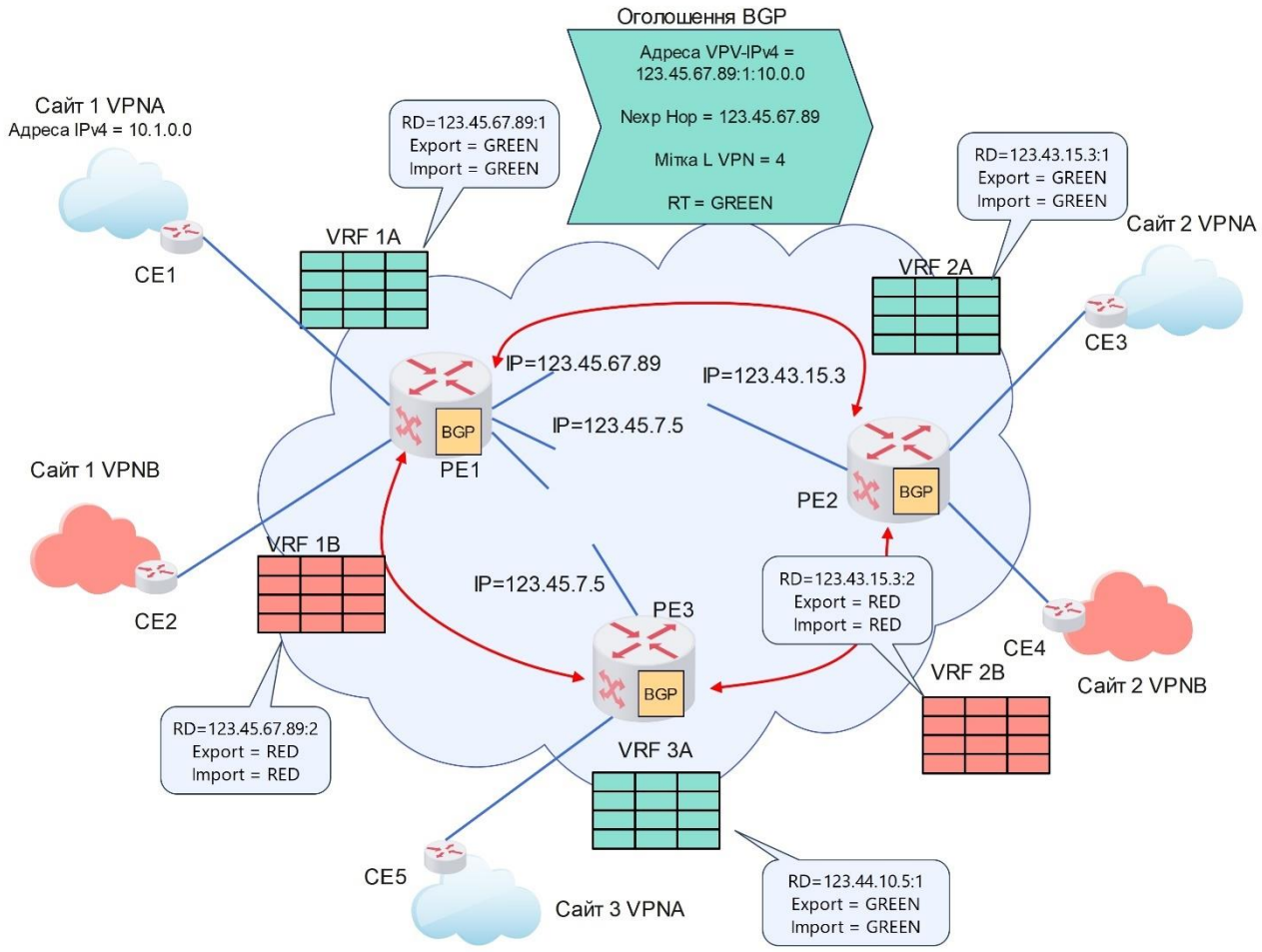


Рис. 3.8. Маршрутні оголошення MB-BGP

Значення атрибута route-target в оголошенні про маршрут визначається політикою експорту маршрутних оголошень, яка була задана при конфігуруванні таблиці VRF, що містить цей маршрут. Якщо ж маршрут не входить в число експортованих, то він не передається іншим маршрутизаторів PE, а використовується локально. Таке можливо, коли два маршрутиRT = GREENзатора CE в одній і тій же мережі VPN безпосередньо під'єднані до одного маршрутизатора PE. Формат атрибута route-target аналогічний формату розрізнювача маршрутів (RD), що забезпечує його унікальність в межах усіх мереж VPN.

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. 3.8, 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.

Приклад конфігурації зіркоподібній топології представлений на рис. 3.9. Для досягнення цього ефекту досить визначити для VRF центрального сайту політику імпорту як import = spoke, експорту – як export = hub, а для VFR периферійних сайтів вчинити навпаки, задавши import = hub і export = spoke.

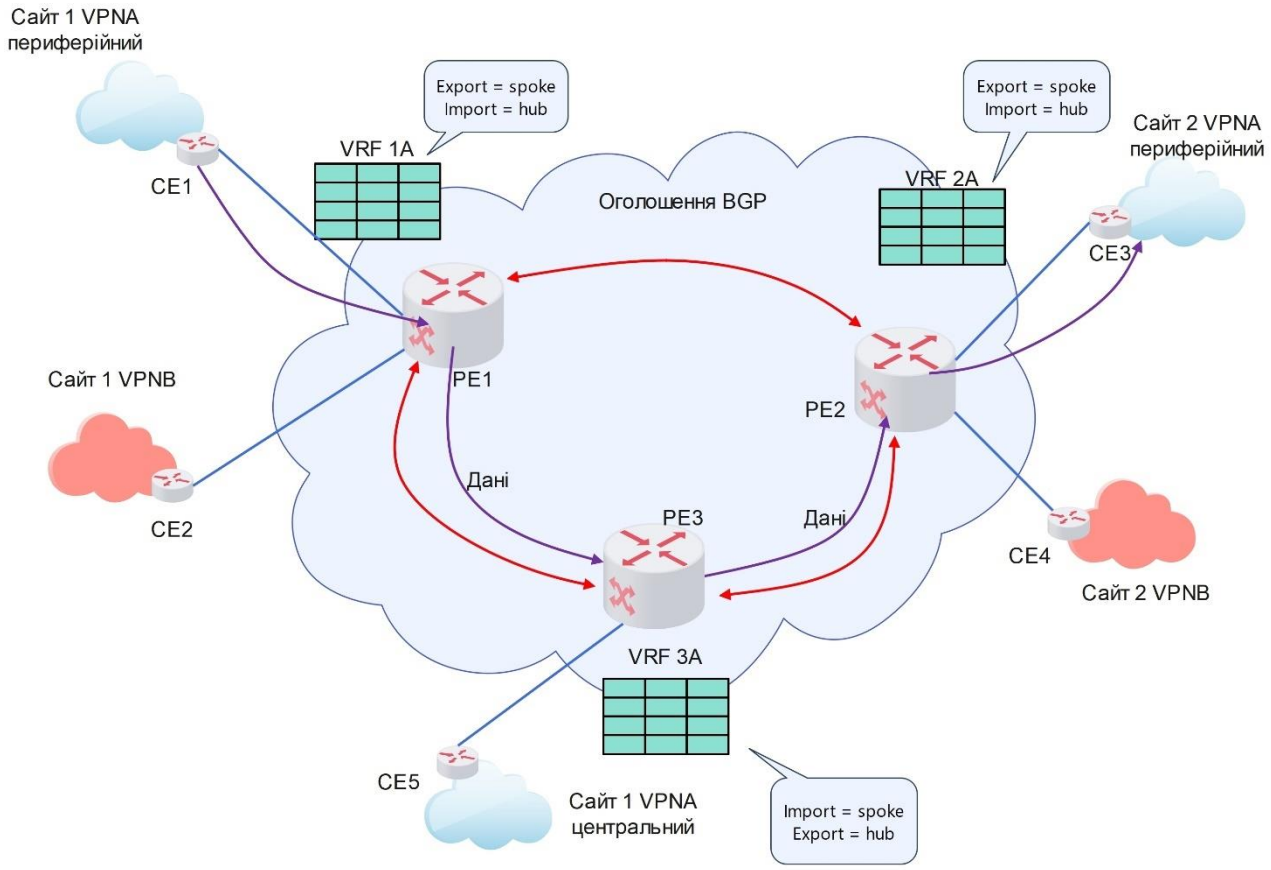


Рис. 3.9. Конфігурування топології «зірка» між сайтами VPNA

В результаті таблиці VRF периферійних сайтів не зможуть приймати маршрутні оголошення один від одного, оскільки вони передаються по мережі протоколом MP-BGP з атрибутом route-target = spoke, між тим як їх політика імпорту дозволяє отримувати оголошення з атрибутом route-target = hub. Зате оголошення таблиць VRF периферійних сайтів приймає таблиця VRF центрального сайту, для якого як раз і визначена політика імпорту spoke. Цей сайт узагальнює всі оголошення периферійних сайтів і відсилає їх назад, але вже з атрибутом route-target = hub, що збігається з політикою імпорту периферійного сайту.

Таким чином, в VRF кожного периферійного сайту з’являються записи про

мережі в інших периферійних сайтах з адресою пов’язаного з центральним сайтом інтерфейсу PE в якості наступного транзитного вузла – оскільки оголошення прийшло від нього. Тому пакети між периферійними сайтами будуть проходити транзитом через прикордонний маршрутизатор PE3, що під’єднаний до центрального сайту.

3.4. 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).

Віртуальна приватна мережа на основі шифрування – це сукупність захищених каналів, створених організацією у відкритій публічній мережі для об’єднання своїх власних мереж.

Основною публічної мережею сьогодні є Інтернет і більшість типів захищених каналів, що працюють в Інтернеті, використовують стандартний протокол IP. Захищений канал може бути утворений клієнтом Інтернету, і від провайдерів обох закінчень каналу потрібно лише надання стандартного доступу в Інтернет. У цьому полягає основна перевага VPN на основі шифрування перед VPN на основі розмежування трафіку: перші працюють в межах всього Інтернету, в той час як другі – в межах мережі одного провайдера, підтримуючого MPLS.

Мережі VPN на основі шифрування можуть бути організовані як клієнтами, так і провайдерами, але останній варіант поширений мало.

Мережа VPN на основі шифрування є свого роду «мережа в мережі», тобто сервіс, який створює у користувачів ілюзію існування їх приватної мережі всередині публічної мережі. Однією з головних властивостей такої «приватної мережі» є захищеність трафіку від атак користувачів публічної мережі. Мережам VPN доступна не лише здатність імітації приватної мережі; вони дають користувачу можливість мати власний адресний простір (наприклад, приватні IP-адреси) і забезпечувати якість обслуговування, близьке до якості виділеного каналу.

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.

Для підвищення рівня захищеності віртуальних приватних мереж технології VPN на основі шифрування можна застосовувати спільно з технологіями VPN на основі розмежування трафіку. Технології VPN на основі поділу трафіку іноді критикують за недостатній рівень безпеки, вважаючи, що без шифрування трафіку персонал постачальника послуг може отримати несанкціонований доступ до даних. Дійсно, така ймовірність існує, тому клієнт послуг VPN на основі розмежування трафіку, наприклад MPLS VPN, може самостійно підвищити захищеність свого трафіку, вдавшись до шифрування переданих даних.

Зараз найбільш широко використовуються мережі VPN на основі протоколів IPSec і SSL. Стандарти IPSec забезпечують високу ступінь гнучкості, дозволяючи вибрати потрібний режим захисту (з шифруванням або тільки із забезпеченням автентичності та цілісності даних), а також використовувати різні алгоритми автентифікації і шифрування. Режим інкапсуляції IPSec дозволяє ізолювати адресні простори клієнта або оператора зв'язку за рахунок застосування двох IP-адрес – зовнішньої і внутрішньої.

Мережі VPN на основі протоколу IPSec, як правило, будуються за типом CPVPN, тобто як віртуальні приватні мережі, в яких клієнт самостійно створює тунелі IPSec через IP-мережу постачальника послуг. Конфігурація мереж VPN на основі IPSec досить трудомістка, оскільки тунелі IPSec двоточкові, тобто при повнозв'язній топології їх кількість пропорційна $N \times (N-1)$, де N - число з'єднань. Необхідно врахувати ще й непросту задачу підтримки інфраструктури ключів. Крім того, протокол IPSec може застосовуватися для створення віртуальних приватних мереж, підтримуваних провайдером (PPVPN), – тунелі в них також будуються на базі пристроїв клієнта (CE-based), але ці пристрої віддалено конфігуруються і адмініструються постачальником послуг.

На рис. 3.10 показаний приклад організації віртуальної приватної мережі на основі шифрування, що використовується працівниками підприємства, які працюють віддалено. У корпоративній мережі встановлений VPN-шлюз, який об'єднаний з корпоративним файерволом (таке об'єднання функцій не є обов'язковим, хоча часто зустрічається). На комп'ютерах віддалених користувачів встановлена програма – PN-клієнт. PN-клієнт звертається до шлюзу і встановлює з ним захищений канал. Шлюз VPN повинен володіти високою

продуктивністю для того, щоб одночасно підтримувати достатню кількість сеансів з віддаленими користувачами. Програмне забезпечення шлюзу має також дозволяти адміністратору VPN управляти обліковими записами віддалених користувачів, а також ключами, що застосовуються для автентифікації і шифрування.

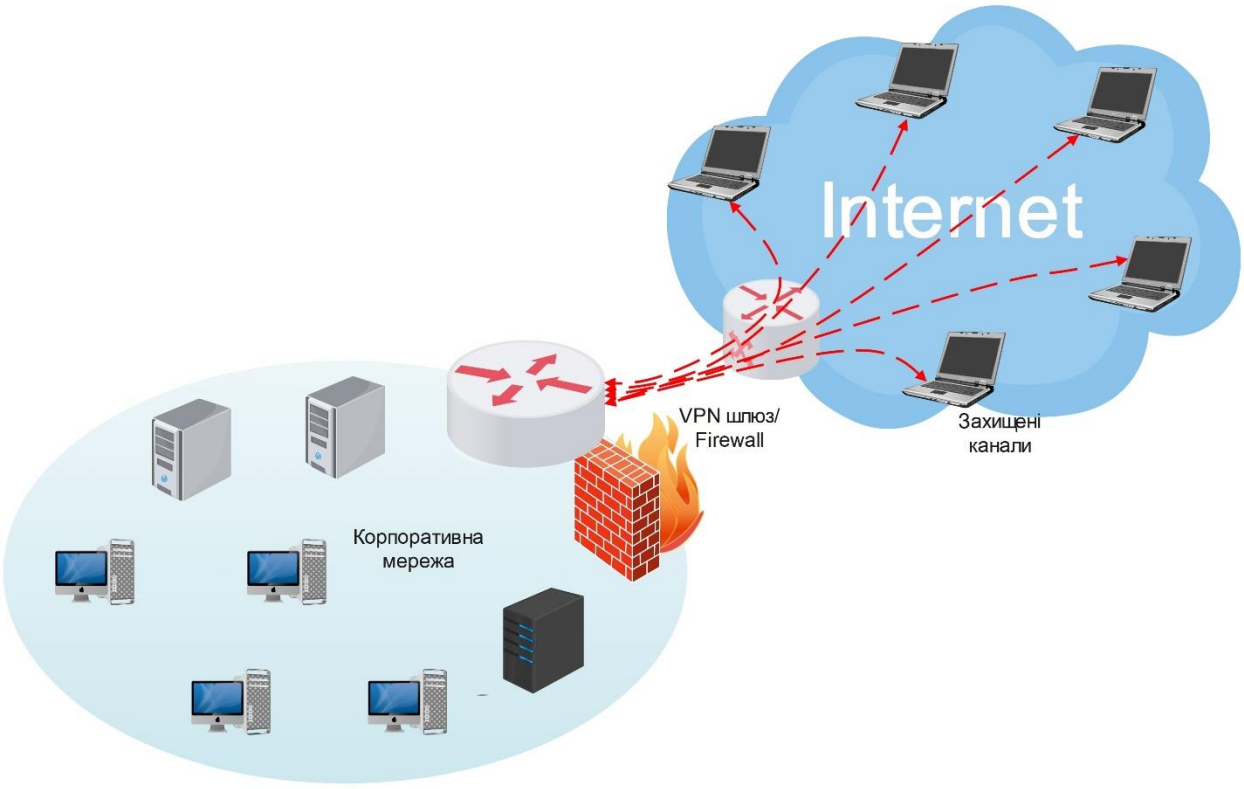


Рис. 3.10. VPN доступу на основі шифрування

В VPN на основі шифрування можливо також використання захищеного каналу на основі протоколу SSL. Цей протокол працює на рівні відображення, безпосередньо під прикладним рівнем, так що додатки, щоб створити захищений канал для свого трафіку, повинні викликати його явно. Найбільш популярним додатком, що використовує захищені канали SSL, є веб-браузер. Захищені канали SSL утворюються у веб-браузері на основі протоколу HTTP, який в цьому режимі роботи називають протоколом HTTPS. Браузер вдається до даного режиму у всіх випадках, коли необхідно забезпечити конфіденційність інформації, що передається: при покупках в інтернет-магазинах, при інтернет-банкінгу і т. п.

Служба VPN на основі SSL функціонує на базі веб-порталу, що розгорнутий в локальній мережі організації. Користувачі захищеної служби VPN отримують віддалений доступ до ресурсів цієї локальної мережі, звертаючись до веб-порталу за допомогою звичайного браузера через порт 443 (TCP-порт протоколу

HTTPS). Відсутність спеціального клієнтського програмного забезпечення, що вимагає настройки, є значною перевагою VPN на основі SSL.

4. Технології автентифікації, авторизації і управління доступом

4.1. Технології автентифікації

Автентифікація стосовно до обчислювальної системи – це доказ достовірності різних елементів цієї системи при їх взаємодії. Користувач при вході в систему повинен пред'явити системі докази, що він саме той користувач, ідентифікатор якого він вводить. Таким доказом може служити пароль. Документ, отриманий користувачем по електронній пошті, повинен супроводжуватися додатковою інформацією, яка переконує користувача, що документ не був змінений при передачі і що автором цього документа є саме та людина, від імені якого цей лист було надіслано. Тут доказом може служити електронний підпис. Пристрої, що взаємодіють по мережі, мають довести один одному, що жоден з них не підмінений зловмисником з метою відгалуження або прослуховування трафіку. Для цього в протоколі взаємодії цих пристроїв повинна бути передбачена процедура взаємної автентифікації. Взаємна автентифікація потрібно і для організації безпечного сеансу користувача і серверного додатка. Автентифікація може проводитися по відношенню не тільки до окремого користувача, але і до групи користувачів. Методи автентифікації розрізняються залежно від того, що служить автентифікатором, а також від того, яким чином організовано обмін автентифікаційними даними між елементами системи.

4.1.1. Фактори автентифікації людини

Абсолютно надійна автентифікація людини являє собою теоретично нездійсненне завдання. Немає такого автентифікатора, який зі стовідсотковою надійністю доводив би автентичність людини. Пароль можна перехопити, електронний ключ вкрасти, відбиток пальця підробити, райдужну оболонку ока підмінити якісним зображенням. Більш того, не існує наукового доказу неможливості збігу у різних людей відбитків пальців або райдужних оболонок ока. Навіть збіг результатів аналізу ДНК при сучасному рівні розвитку техніки не може служити абсолютним доказом автентичності людини.

Однак, на практиці при автентифікації користувачів в обчислювальних системах обмежуються деяким не стовідсотковим, хоча і досить високим рівнем достовірності доказу автентичності 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.

Клас автентифікаторів називають **фактором**. Якщо в процедурі автентифікації передбачається пред'явлення автентифікованим декількох автентифікаторів, що відносяться до різних класів, то таку автентифікацію називають **багатофакторної**. Найбільшого поширення в даний час отримала **двофакторна автентифікація**, при якій користувач пред'являє багаторазовий пароль («щось, що знаю») і апаратний ключ («щось, що маю»). Слід зауважити, що в деяких випадках термін «багатофакторна автентифікація» служить для позначення процедур **багатоступінчастої автентифікації**, побудованих на використанні декількох автентифікаторів, що відносяться до одного і того ж класу. Прикладом такої процедури є автентифікація власника банківського рахунку при його дзвінку в банк: спочатку його просять назвати кілька букв з його пароля, а потім задають кілька запитань з попередньо узгодженими і зафіксованими в базі даних автентифікуючої організації відповідями, наприклад, дівоче прізвище матері і т. п.

4.1.2. Автентифікація на основі паролів

Пароль – це послідовність символів, обраних або користувачем, або згенерованих програмним або апаратним засобом, або призначених адміністратором, що зберігається в секреті. Паролі відносяться до автентифікаторів класу «щось, що знаю».

Паролі бувають одноразовими і багаторазовими. **Багаторазові паролі** можуть використовуватися як доказ автентичності багаторазово. У процедурах автентифікації, що базуються на **одноразових паролях**, автентифікований повинен кожен раз пред'являти нове значення пароля. Зазвичай, для генерації одноразових паролів застосовуються спеціальні програми або апаратні пристрої.

Механізми автентифікації на основі багаторазових паролів, володіючи простотою і логічною ясністю, традиційно є найпопулярнішим засобом автентифікації. Однак вони володіють відомими недоліками. Це, по-перше, можливість розкриття і розгадування паролів, по-друге, можливість «підслуховування» пароля при його передачі по мережі шляхом аналізу мережевого трафіку. По-третє, власники паролів можуть стати жертвами

соціального інжинірингу (наприклад, екс-співробітник Агентства національної безпеки США Едвард Сноуден, який використовував логіни і паролі більше 20 своїх товаришів по службі, щоб отримати доступ до секретних файлів).

Для зниження рівня загрози розкриття паролів адміністратори мережі, як правило, застосовують вбудовані програмні засоби, що служать для формування політики призначення і використання паролів: завдання максимального і мінімального термінів дії пароля, зберігання списку вже використаних паролів, управління поведінкою системи після декількох невдалих спроб логічного входу і т. п.

У списку найбільш популярних паролів, що застосовуються користувачами Інтернету при доступі до веб-серверів, опублікованому в серпні 2015 року компанією Google, місця в першій десятці займають імена і дати народження членів сім'ї і близьких друзів, назви місць народження, дати весілля, клички домашніх тварин, що-небудь, пов'язане з улюбленою футбольною командою, і слово «password». Як видно з наведеного списку, для зацікавленої людини не складе великих труднощів підібрати ці паролі. Але навіть при виборі менш передбачуваного пароля все ж таки є ризик, що він буде розгаданий простим перебором всіх можливих символів, - такий метод часто називають **брутфорс-атакою** (brute-force – вирішувати щось «в лоб», методом грубої сили). Час підбору прямо залежить від різноманітності набору символів, з якого формується пароль, і довжини пароля. У табл. 4.1 наведені дані, що характеризують стійкість паролів, що складаються з 6 і 8 знаків, сформованих з різних наборів символів.

Серйозною проблемою використання багаторазових паролів є їх ручна синхронізація. У звичайному житті нам потрібно не один, а кілька паролів: для входу в комп'ютерну мережу підприємства, в якому ми працюємо, щоб отримати доступ до «особистого кабінету» провайдера мобільного зв'язку, для доступу до банківського рахунку і ще для доступу до самих різних інтернет-сайтах. Часто трапляється, що у всіх цих випадках застосовується один і той же пароль (можливо, з невеликими варіаціями), тому що у нас немає часу придумувати і, головне, запам'ятовувати новий пароль для доступу до нового ресурсу. Таке явище називають **ручною синхронізацією паролів**.

Поряд з паролями існує інший варіант використання автентифікаторів з класу «щось, що знаю». Адміністратор, заздалегідь безпечним чином, повідомляє користувачу деяке правило, наприклад правило перетворення послідовності чисел в інші символи. Під час процедури автентифікації система виводить на екран випадкову послідовність чисел. Користувач, згідно до відомого лише йому і системі правилу, перетворює їх в іншу послідовність символів, яку вводить в якості пароля. Оскільки система також «знає» правило

перетворення, вона може перевірити правильність введеного пароля. Тобто, спочатку в даному випадку в якості поділюваного секрету виступає правило перетворення.

Таблиця 4.1. 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)

4.1.3. Протоколи автентифікації віддалених користувачів

Контроль доступу користувачів до ресурсів корпоративної мережі повинен здійснюватися відповідно до політики безпеки організації, якій належить ця мережа. Ефективне розмежування доступу до мережевих ресурсів може бути забезпечене тільки при надійній автентифікації користувачів. Вимоги до надійності автентифікації віддалених користувачів мають бути особливо високими, оскільки при взаємодії з фізично віддаленими користувачами значно складніше забезпечити доступ до мережевих ресурсів. На відміну від локальних користувачів віддалені користувачі не проходять процедуру фізичного контролю при допуску на територію організації.

При віддаленій взаємодії важлива автентифікація не лише користувачів, але і обладнання, оскільки підміна користувача або маршрутизатора призводить до одних і тих же наслідків – дані з корпоративної мережі передаються не тим особам, яким вони призначені.

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**).

В процесі встановлення віддаленого з'єднання кожна з взаємодіючих сторін може запропонувати для застосування один із стандартних протоколів автентифікації – PAP або CHAP. Іноді компанії створюють власні протоколи автентифікації віддаленого доступу, що працюють разом з протоколом PPP. Ці фірмові протоколи, зазвичай, є модифікаціями протоколів PAP і CHAP.

Широке застосування для автентифікації по одноразових паролях отримав протокол S/Key. У програмних продуктах, що забезпечують зв'язок по протоколу PPP, протоколи PAP і CHAP, як правило, підтримуються в першу чергу.

Протокол PAP

Протокол PAP є простим методом перевірки достовірності віддаленого пристрою. Для ініціалізації процесу автентифікації на базі протоколу PAP сервер віддаленого доступу після встановлення сеансу зв'язку висилає віддаленому комп'ютеру пакет LCP (Link Control Protocol – протокол управління каналом), що вказує на необхідність застосування протоколу PAP. Далі здійснюється обмін

пакетами PAP. Віддалений комп'ютер передає по каналу зв'язку перевіряючій стороні ідентифікатор і пароль, введені віддаленим користувачем. Сервер віддаленого доступу по отриманому ідентифікатору користувача вибирає еталонний пароль з БД системи захисту і порівнює його з отриманим паролем. Якщо вони співпадають, то автентифікація вважається успішною, про що повідомляється віддаленому користувачеві.

Слід особливо відмітити, що протокол автентифікації PAP, згідно з яким ідентифікатори і паролі передаються по лінії зв'язку в незашифрованому виді, доцільно застосовувати тільки спільно з протоколом, орієнтованим на автентифікацію по одноразових паролях, наприклад спільно з протоколом S/Key. Інакше пароль, що передається по каналу зв'язку, може бути перехоплений зловмисником і використаний повторно в цілях маскування під санкціонованого віддаленого користувача.

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. Така технологія забезпечує не лише захист пароля від викрадення, але і захист від повторного використання зловмисником перехоплених пакетів із зашифрованим паролем. Протокол CHAP застосовується в сучасних мережах

набагато частіше, ніж PAP, оскільки він використовує передачу паролю по мережі в захищеній формі, і, отже, набагато безпечніший.

Шифрування паролю відповідно до протоколу CHAP виконується за допомогою криптографічного алгоритму хешування і тому є безповоротним. У стандарті RFC 1334 для протоколу CHAP в якості хеш-функції визначений алгоритм MD5. Специфікація CHAP не виключає використання інших алгоритмів обчислення хеш-функцій.

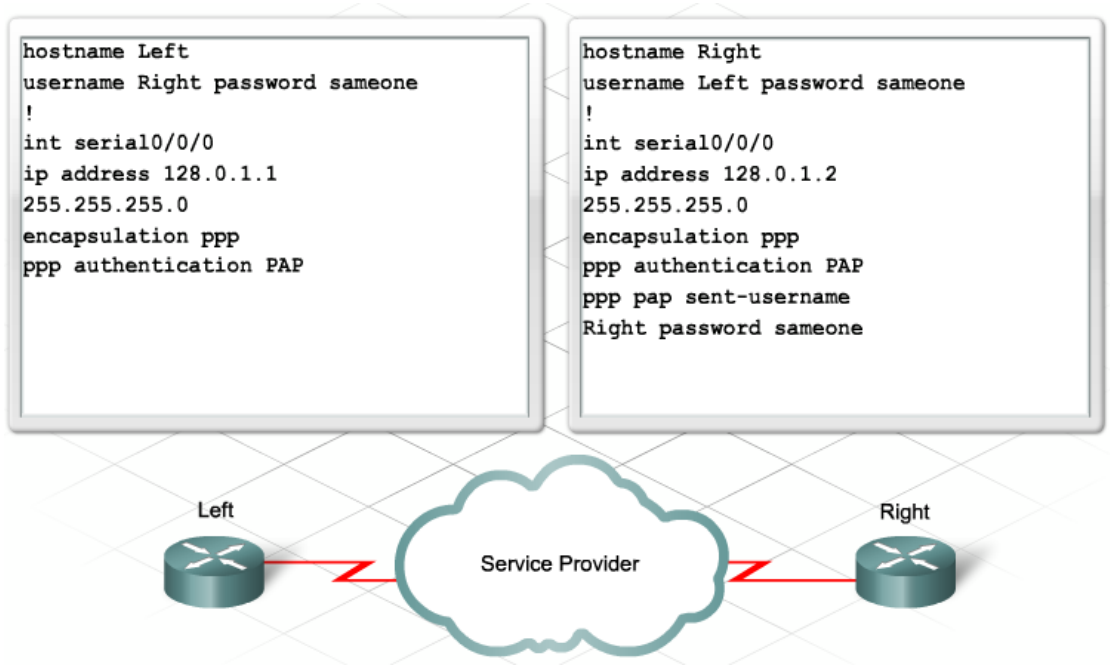


Рис. 4.1. Налаштування PAP

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 CHAP використовує для автентифікації віддаленого користувача результат шифрування довільного слова-виклику за допомогою унікального секрету. Цей секрет є як у перевіряючої сторони, так і у сторони, що перевіряється.

Процедура автентифікації починається з відправки сервером віддаленого доступу пакету *Виклик*. Віддалений комп'ютер, отримавши пакет *Виклик*, зашифровує його за допомогою односторонньої функції і відомого йому секрету, отримуючи в результаті дайджест. Дайджест повертається перевіряючій стороні у вигляді пакету *Відгук*.

Оскільки використовується одностороння хеш-функція, то по перехоплених пакетах *Виклик* і *Відгук* обчислити пароль віддаленого користувача практично неможливо.

Отримавши пакет *Відгук*, сервер віддаленого доступу порівнює вміст результату отриманого пакету *Відгук* з результатом, обчисленим самостійно. Якщо ці результати співпадають, то автентифікація вважається успішною і сервер висилає віддаленому комп'ютеру пакет *Підтвердження*. В іншому випадку сервер віддаленого доступу висилає пакет *Відмова* і розриває сеанс зв'язку.

Пакет *Виклик* має бути відправлений сервером повторно, якщо у відповідь на нього не був отриманий пакет *Відгук*. Крім того, пакет *Виклик* може відправлятися періодично протягом сеансу віддаленого зв'язку для проведення динамічної автентифікації, щоб переконатися, що протилежна сторона не була підмінена. Відповідно пакет *Відгук* повинен відправлятися стороною, що перевіряється, у відповідь на кожен прийнятий пакет *Виклик*.

Налаштування автентифікації по протоколу CHAP виконується аналогічно як і для PAP.

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.

Проте слід зазначити, що протокол S/Key не виключає необхідність задання секретного паролю для кожного користувача. Цей секретний пароль використовується тільки для генерації одноразових паролів. Для того, щоб зловмисник не зміг по перехопленому одноразовому паролю обчислити секретний початковий пароль, генерація одноразових паролів виконується за допомогою односторонньої функції. В якості односторонньої функції в специфікації протоколу S/Key визначений алгоритм хешування MD4. Деякі реалізації протоколу S/Key використовують алгоритм хешування MD5.

Іноді бажано, щоб користувач мав можливість сам призначати секретний постійний пароль. Для здійснення такої можливості специфікація S/Key передбачає режим обчислення одноразових паролів не лише на основі секретного пароля, але і на основі генерованого перевіряючою стороною випадкового числа. Таким чином, відповідно до протоколу S/Key за кожним користувачем закріплюється ідентифікатор і секретний постійний пароль.

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

4.1.4. Автентифікація на основі апаратних автентифікаторів

Види апаратних автентифікаторів

Апаратні автентифікатори, звані також **апаратними ключами**, або **токенами**, відносяться до розряду «щось, що маю». Перелічимо найбільш популярні з них (рис 4.2.):

- **Ідентифікатори IButton** мають ПЗП, що містить 64-розрядний код, однопровідний порт і схему, яка реалізує логіку управління. При зіткненні зі зчитувачем ідентифікатор IButton передає йому унікальний номер, зчитувач перевіряє його і ініціює сеанс обміну даними з ідентифікатором по визначеному для цих двох пристроїв протоколу.
- **USB-ключі**, або **USB-токени**, підключаються безпосередньо до USB-порту комп’ютера, виключаючи необхідність використання дорогих зчитувальних пристроїв. Конструктивно USB-ключі виконуються подібно переносним пристроям пам’яті Memory Stick. Кожен USB-ключ має унікальний номер, привласнений виробником.

- **Смарт-карти** (Smart Card – інтелектуальна карта) можуть бути як контактними, так і безконтактними. Контактні смарт-карти мають на одній зі сторін контактні площадки, через які при зіткненні з контактами зчитувача відбувається передача електроживлення і автентифікаційної інформації. Зчитувачі мають найрізноманітніше конструктивне виконання: наприклад, вони можуть бути вбудовані в клавіатуру або в корпус комп'ютера. В безконтактних смарт-картах передбачається радіочастотний блок з вбудованою антеною, прокладеною по периметру карти. Смарт-карта містить процесор, ПЗП, в якому зберігається криптографічна програма, ОЗП, який використовується як робоча пам'ять, а також пристрій EEPROM (програмований ПЗП, що електрично стирається), що містить змінні дані власника карти. Автентифікація власника карти здійснюється за унікальним серійним номером карти, який присвоюється їй на підприємстві-виробнику, а також по персональних даних власника, що зберігаються в пам'яті в зашифрованому вигляді.

- Рис. 4.2. Електронні пристрої-ідентифікатори

- **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. Всередині пластикового корпусу знаходиться інтегральна схема, яка

зберігає і обробляє інформацію, а також мініатюрна антена, призначена для передачі і прийому радіосигналів. Система радіочастотної автентифікації крім власне RFID-ідентифікатора включає зчитувач радіочастотних сигналів, який вбудовується в електронні замки, обчислювальні пристрої та ін. Власник RFID-ідентифікатора використовує його як пропуск в приміщення підприємства, підносячи його до зчитувача на стіні перед дверима з електронним замком. Зчитувач постійно випромінює радіочастотний сигнал, який при піднесенні ідентифікатора на певну відстань (залежне від типу пристрою) приймається його антеною і передається у вигляді живлення інтегральній схемі. Цей же ідентифікатор може служити для доступу до принтера і інших пристроїв обчислювальної системи. Крім того, RFID-ідентифікатор дозволяє службі безпеки відслідковувати переміщення його власника по всіх приміщеннях, що обладнані відповідними давачами.

Загальним недоліком всіх апаратних автентифікаторів є те, що вони можуть бути втрачені або, що значно гірше, навмисно викрадені. Будь-яка людина, що заволоділа автентифікатором, теоретично отримує в своє розпорядження всі повноваження законного власника.

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** (рис. 4.3).

Рис. 4.3. Апаратні ключі, які генерують одноразові паролі

Незалежно від того, яку реалізацію системи автентифікації на основі одноразових паролів вибирає користувач, він, як і в системах автентифікації з

застосуванням багаторазових паролів, повідомляє системі свій ідентифікатор, однак замість того, щоб вводити кожен раз один і той же пароль, він вказує послідовність цифр, яка надається йому апаратним або програмним ключем. Через певний, невеликий період часу, ключ генерує іншу послідовність – новий пароль. Сервер автентифікації перевіряє введену послідовність і дозволяє користувачу здійснити логічний вхід. Сервер автентифікації може являти собою окремий пристрій, виділений комп'ютер або програму, що виконується на звичайному сервері.

Як правило, системи автентифікації на основі одноразових паролів розраховані на перевірку віддалених, а не локальних користувачів.

Розглянемо схему використання апаратного генератора одноразових паролів, в основі якої лежить **синхронізація за часом**. Ідея методу полягає в тому, що апаратний ключ і автентифікуючий сервер по одному і тому ж алгоритму обчислюють деяке значення – **одноразовий пароль**. Алгоритм має два параметри:

- поділюваний секретний ключ, який являє собою 64-розрядне число, що унікально призначається кожному користувачеві і зберігається як в апаратному ключі, так і в базі даних сервера автентифікації;
- значення поточного часу.

Якщо обчислені значення збігаються, то автентифікація вважається успішною. Отже, нехай віддалений користувач намагається зробити логічний вхід в систему з персонального комп'ютера (рис. 4.4).

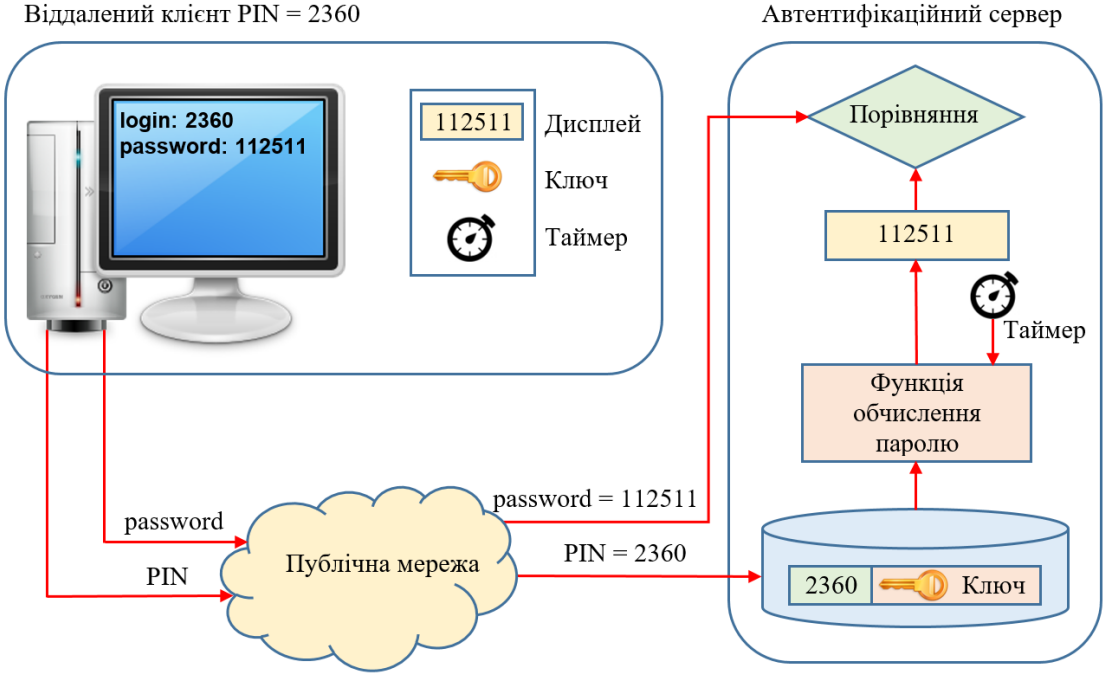


Рис. 4.4. Автентифікація на основі часової синхронізації

Автентифікуюча програма пропонує користувачу ввести його особистий персональний номер (PIN-код), що складається з чотирьох десяткових цифр (на малюнку – 2360), а також одноразовий пароль – шість цифр випадкового числа, які відображаються в той момент на дисплеї апаратного ключа (на рисунку – 112511). На основі PIN-коду сервер витягує з бази даних інформацію про користувача, а саме його секретний ключ. Потім сервер виконує обчислення за тим же алгоритмом, який закладений в апаратному ключі, використовуючи в якості параметрів секретний ключ і значення поточного часу, перевіряючи, чи збігається згенероване число з числом, яке ввів користувач. Якщо вони збігаються, то користувачу дозволяється логічний вхід.

Потенційною проблемою цієї схеми є часова синхронізація сервера і апаратного ключа. Цю проблему вирішують двома способами. По-перше, при виробництві апаратного ключа вимірюється відхилення частоти його таймера від номіналу. Далі ця величина враховується в вигляді параметру алгоритму сервера. По-друге, сервер відстежує коди, що генеруються конкретним апаратним ключем, і якщо таймер даного ключа постійно поспішає або відстає, то сервер динамічно підлаштовується під нього.

Існує ще одна проблема, що пов’язана зі схемою часової синхронізації. Одноразовий пароль, що генерується апаратним ключем, дійсний протягом деякого інтервалу часу (від декількох десятків секунд до декількох десятків хвилин), тобто протягом цього часу одноразовий пароль, по суті, є багаторазовим. Тому теоретично можливо, що дуже швидкий хакер зможе перехопити PIN-код і одноразовий пароль з тим, щоб також отримати доступ в мережу протягом цього інтервалу.

Схема часової синхронізації не вимагає наявності комп’ютера на стороні автентифікованого, для цих цілей можна обмежитися простим терміналом або факсом. Користувачі можуть навіть вводити свій пароль з телефонної клавіатури, коли дзвонять в мережу для отримання голосової пошти.

4.1.5. Автентифікація інформації. Цифровий підпис

Автентифікація даних включає:

- 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.

Всі ці завдання в тій чи іншій мірі можуть бути вирішені за допомогою цифрового підпису. Відповідно до термінології, затвердженої Міжнародною організацією зі стандартизації (ISO), під терміном **цифровий (електронний) підпис** розуміються методи, що дозволяють встановлювати справжність автора повідомлення (документа) при виникненні спору щодо авторства. Основна область застосування цифрового підпису – фінансові документи, які супроводжують електронні угоди, документи, що фіксують міжнародні домовленості, і т. п.

Цифровий підпис не ставить завдання забезпечення конфіденційності повідомлень.

Хоча для отримання підпису можуть використовуватися симетричні алгоритми, більш поширеними є алгоритми на основі відкритого і закритого ключів. На рис. 4.5 показана схема формування цифрового підпису по алгоритму RSA. Кожен користувач мережі має власний закритий ключ (D, n), який необхідний для формування підпису, а відповідний цьому секретному ключу відкритий ключ (E, n), що призначений для перевірки підпису, відомий всім іншим користувачам мережі. Підписана угода складається з двох частин: незашифрованої частини, в якій міститься вихідний текст T, і зашифрованої частини, що являє собою цифровий підпис S. 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:

$$T=S^E \bmod n$$

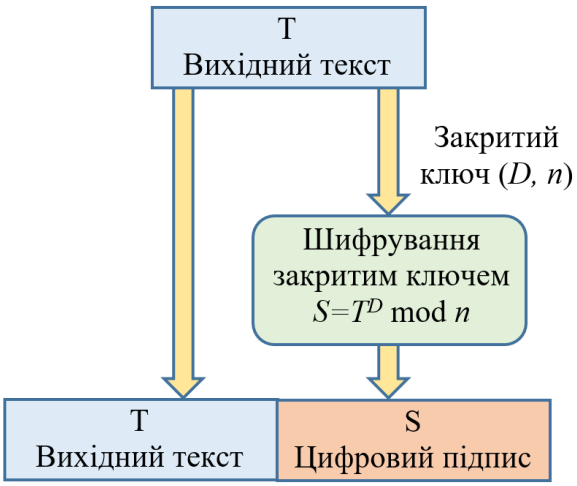


Рис. 4.5. Схема формування цифрового підпису по алгоритму RSA

Якщо результат розшифровки цифрового підпису збігається з відкритою частиною повідомлення, вважається, що документ справжній, не зазнав ніяких змін в процесі передачі, а автором його є саме та людина, яка передала свій відкритий ключ одержувачу.

До недоліків даного алгоритму можна віднести те, що довжина підпису в цьому випадку дорівнює довжині повідомлення, що не завжди зручно. Для зменшення «довжини» цифрового підпису замість $S=T^D \bmod n$ використовується формула:

$$S=(H(T))^D \bmod n$$

Тут $H(T)$ – хеш-функція, яка перетворює вихідне повідомлення в короткий дайджест. У цьому випадку одержувач повідомлення (T, S) повинен спочатку застосувати до відкритого тексту T хеш-функцію H і отримати дайджест $H(T)$, а потім приступити до розшифровки підпису S відкритим ключем. Якщо розшифрований підпис збігається з дайджестом, то авторство повідомлення доведено. Використання хеш-функцій дає виграш не тільки в обсязі повідомлення, але і в часі отримання електронного підпису.

Якщо крім перевірки автентичності документа, що забезпечується цифровим підписом, потрібно забезпечити його конфіденційність, то після застосування до тексту цифрового підпису, перед передачею його по каналу зв’язку виконують спільне шифрування вихідного тексту і цифрового підпису будь-яким спільно обраним способом шифрування.

Цифровий підпис робить юридично чинним документом не друкований документ, а сам комп’ютерний файл.

В Україні всі взаємовідносини електронних документів та підписів визначаються Законами України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис».

4.1.6. Автентифікація на основі цифрових сертифікатів

Автентифікація з застосуванням цифрових сертифікатів є альтернативою застосуванню паролів і видається природним рішенням в умовах, коли число користувачів мережі (нехай і потенційних) вимірюється мільйонами. В таких обставинах процедура попередньої реєстрації користувачів, пов’язана з призначенням і зберіганням їх паролів, стає вкрай обтяжливою, небезпечною, а іноді і просто нездійсненною. При наявності сертифікатів мережа, яка дає користувачеві доступ до своїх ресурсів, не зберігає ніякої інформації про своїх користувачів – вони її надають самі в своїх запитах у вигляді сертифікатів, що засвідчують особу користувачів. Сертифікати видаються спеціальними

уповноваженими сертифікуючими організаціями (СО) – **центрами сертифікації** (Certificate Authority, **СА**). Тому завдання зберігання секретної інформації (закритих ключів) покладається на самих користувачів, що робить це рішення більш масштабованим, ніж варіант з централізованою базою паролів.

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.

Використання сертифікатів базується на припущенні, що сертифікуючих організацій не багато і їх відкриті ключі широко доступні, наприклад, з публікацій у журналах.

Сертифікати можуть бути представлені в трьох формах (рис 4.6.):

- 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.

Коли користувач хоче підтвердити свою особистість, він пред'являє свій сертифікат в двох формах: відкритій (тобто такий, в якій він отримав його в сертифікуючій організації) і зашифрованій із застосуванням свого закритого ключа. Сторона, яка проводить автентифікацію, бере з незашифрованого сертифікату відкритий ключ користувача і розшифровує з його допомогою зашифрований сертифікат. Збіг результату з відкритим сертифікатом підтверджує, що пред'явник дійсно є власником закритого ключа, який відповідає вказаному відкритому.

Потім за допомогою відомого відкритого ключа зазначеної в сертифікаті організації проводиться розшифровка підпису цієї організації в сертифікаті. Якщо в результаті виходить той же сертифікат з тим же ім'ям користувача і його відкритим ключем, значить, він дійсно пройшов реєстрацію в сертифікаційному

центрі, є тим, за кого себе видає, і вказаний в сертифікаті відкритий ключ дійсно належить йому.

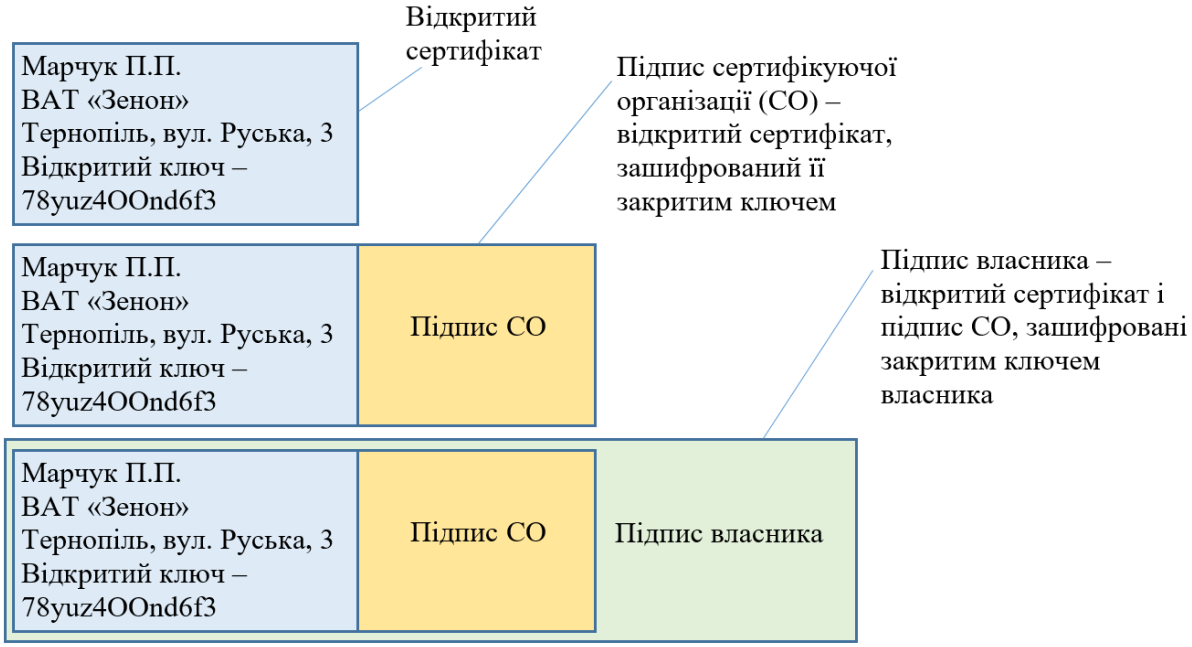


Рис. 4.6. Форми представлення цифрового сертифікату

Сертифікати можна застосовувати не тільки для автентифікації, але і для надання прав доступу до ресурсів. Для цього в сертифікат можуть вводитися додаткові поля, в яких вказується приналежність його власників до тієї чи іншої категорії користувачів. Ця категорія призначається центром сертифікації в залежності від умов, на яких видається сертифікат.

Сертифікат є посвідченням не тільки особистості, але і приналежності відкритого ключа. Цифровий сертифікат встановлює і гарантує відповідність між відкритим ключем і його власником.

Це запобігає загрозі підміни відкритого ключа. Якщо деякий абонент А отримує по мережі сертифікат від абонента Б, то він може бути впевнений, що відкритий ключ, який міститься в сертифікаті, гарантовано належить абоненту Б, адреса та інші відомості про якого містяться в цьому сертифікаті. Це означає, що абонент А може без побоювань використовувати відкритий ключ абонента Б для секретних повідомлень на його адресу.

При наявності сертифікатів відпадає потреба зберігати на серверах організацій списки користувачів з їх паролями, замість цього достатньо мати на сервері список імен і відкритих ключів центрів сертифікації. Може також знадобитись деякий механізм для встановлення відповідності категорій власників сертифікатів традиційним групам користувачів, щоб можна було в

незмінному вигляді задіяти механізми управління вибірковим доступом більшості операційних систем або додатків.

Сертифікат є засобом автентифікації користувача при його зверненні до мережевих ресурсів, роль автентифікуючої сторони виконують при цьому інформаційні сервери корпоративної мережі або Інтернету. У той же час і сама процедура отримання сертифіката також включає етап автентифікації, коли автентифікатором виступає центр сертифікації. Для отримання сертифіката клієнт повинен повідомити центру сертифікації свій відкритий ключ і певні відомості, що засвідчують його особу. Всі ці дані клієнт може відправити електронною поштою або принести на знімному носії особисто. Перелік необхідних даних залежить від типу одержуваного сертифіката. Сертифікуюча організація перевіряє докази достовірності, поміщає свій цифровий підпис в файл, який містить відкритий ключ, і посилає сертифікат назад, підтверджуючи факт приналежності даного конкретного ключа конкретній особі. Після цього сертифікат може бути вбудований в будь-який запит на використання інформаційних ресурсів мережі.

Важливим є питання про те, хто має право виконувати функції сертифікуючої організації. По-перше, завдання забезпечення своїх співробітників сертифікатами може взяти на себе саме підприємство. У цьому випадку спрощується процедура первинної автентифікації при видачі сертифіката. Підприємства достатньо обізнані про своїх співробітників, щоб брати на себе завдання підтвердження їх особи. Для автоматизації процесу генерації, видачі та обслуговування сертифікатів підприємства можуть використовувати готові програмні продукти: наприклад, компанія Netscape Communications випустила сервер сертифікатів, який організації можуть у себе встановлювати для випуску своїх сертифікатів. По-друге, ці функції можуть виконувати незалежні центри з видачі сертифікатів, що працюють на комерційній основі, наприклад сертифікуючий центр компанії Verisign. Сертифікати компанії Verisign виконані відповідно до міжнародного стандарту X.509 і використовуються в багатьох продуктах, орієнтованих на захист даних, в тому числі в популярному протоколі захищеного каналу SSL. Будь-який бажаючий може звернутися із запитом на отримання сертифіката на веб-сервер цієї компанії.

Механізм отримання користувачем сертифіката добре автоматизується в мережі в моделі «клієнт-сервер», коли браузер виконує роль клієнта, а в сертифікуючій організації встановлено спеціальний сервер видачі сертифікатів. Браузер генерує для користувача пару ключів, залишає закритий ключ у себе і передає частково заповнену форму сертифіката серверу. Для того, щоб не підписаний ще сертифікат не можна було підмінити при передачі по мережі,

браузер ставить свій електронний підпис, зашифровуючи сертифікат створеним закритим ключем. Сервер сертифікатів підписує отриманий сертифікат, фіксує його в своїй базі даних і повертає його будь-яким методом власнику. Після отримання сертифіката браузер зберігає його разом з закритим ключем і використовує при автентифікації на тих серверах, які підтримують такий процес. В даний час існує велика кількість протоколів і продуктів, які застосовують сертифікати. Зокрема, практично всі браузери і операційні системи реалізують підтримку сертифікатів.

Незважаючи на активне використання технології цифрових сертифікатів в багатьох системах безпеки, ця технологія ще не вирішила цілий ряд серйозних проблем. Це, перш за все, підтримка бази даних про видані сертифікати. Сертифікат видається не назавжди, а на певний визначений термін. Після закінчення терміну придатності сертифікат повинен або оновлюватися, або анулюватися. Крім того, необхідно передбачити можливість дострокового припинення повноважень сертифіката. Всі зацікавлені учасники інформаційного процесу повинні бути вчасно сповіщені про те, що деякий сертифікат вже недійсний. Для цього сертифікуюча організація повинна оперативно підтримувати список відкликаних сертифікатів.

Є також ряд проблем, пов’язаних з тим, що сертифікуючі організації існують не в однині. Всі вони випускають сертифікати, але навіть якщо ці сертифікати відповідають єдиному стандарту (зараз це, як правило, стандарт X.509), все одно залишаються невирішеними багато питань. Яким чином можна перевірити повноваження того чи іншого сертифікуючого центру? Чи можна створити ієрархію сертифікуючих центрів, при якій сертифікуючий центр, що стоїть вище, міг би сертифікувати центри, які розміщені нижче в ієрархії? Як організувати спільне використання сертифікатів, випущених різними сертифікуючими організаціями?

Для вирішення цих та багатьох інших проблем, що виникають в системах, які використовують технології шифрування з відкритими ключами, виявляється необхідним комплекс програмних засобів і методик, званий **інфраструктурою з відкритими ключами** (Public Key Infrastructure, **PKI**).

Дана схема автентифікації включає три основних елементи: це користувачі, цифрові сертифікати і центри сертифікації. Для того щоб дана схема працювала надійно і ефективно, в неї повинні бути включені додаткові елементи, які в сукупності з основними і утворюють PKI.

У число додаткових елементів може входити, наприклад, реєстраційний центр (Registration Authority), який служить посередником між користувачем, що запросив сертифікат, і центром сертифікації. Користувач, зазвичай, звертається до реєстраційного центру за допомогою веб-інтерфейсу і повідомляє дані про

себе. Реєстраційний центр перевіряє цю інформацію і в разі її достовірності передає дані про користувача, підписані власним закритим ключем, центру сертифікації. Реєстраційний центр може обслуговувати кілька центрів сертифікації. При відсутності реєстраційного центру його функції виконує центр сертифікації.

Іншим типом додаткових елементів PKI є різноманітні сховища сертифікатів, що містять інформацію про діючі, відкликані і сертифікати, у яких закінчився термін дії.

4.1.7. 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.

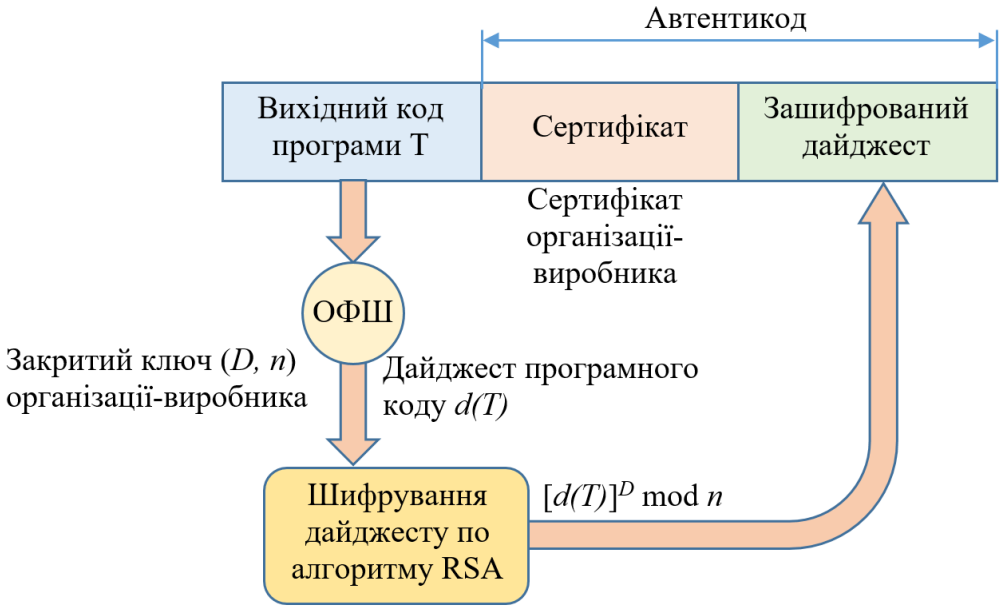


Рис. 4.7. Схема отримання автентикоду

Компанія-розробник може зажадати від користувача програми доказ легальності її придбання. Для цього компанія може запросити реєстраційний номер програми (Product ID або Serial Number), званий також **ліцензійним ключем активації**.

Іншим способом доказу легальності придбання і законності використання програмних продуктів є мініатюрні електронні пристрої – **електронні замки**, подібні до розглянутих апаратних автентифікаторів. Ці пристрої поставляються разом з захищеними від нелегального використання програмами. Перед запуском програми електронний замок повинен бути під'єднаний до комп'ютера, наприклад через USB-порт. Ініціюючий блок програми звертається до даного пристрою із запитом і, отримавши «правильну» відповідь, починає працювати, якщо ж очікувана відповідь не надходить, то виконання програми блокується.

Таким чином, електронний замок діє як специфічний автентифікатор користувача, який доводить те, що користувач є законним власником програми.

4.1.8. Біометрична 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.

Біометричні системи автентифікації є дуже зручними для користувачів. На відміну від паролів і носіїв інформації, які можуть бути втрачені, вкрадені, скопійовані, біометричні системи автентифікації засновані на людських параметрах, які завжди знаходяться разом з користувачем, і проблеми їх збереження не виникає.

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 методи

Автентифікація по відбитку пальця

Ідентифікація за відбитками пальців – найпоширеніша біометрична технологія автентифікації користувачів. Метод використовує унікальність малюнка папілярних візерунків на пальцях людей. Відбиток, отриманий за допомогою сканера, перетворюється в цифровий код, а потім порівнюється з раніше введеними наборами еталонів. Переваги використання автентифікації за відбитками пальців – легкість у використанні, зручність і надійність. Універсальність цієї технології дозволяє застосовувати її в будь-яких сферах для вирішення різноманітних завдань, де необхідна достовірна і досить точна ідентифікація користувачів.

Для отримання відомостей про відбитки пальців застосовуються спеціальні сканери. Зазвичай, застосовуються три основні типи сканерів відбитків пальців: ємнісні, прокатні, оптичні. Найпоширеніші оптичні сканери.

Автентифікація по сітківці ока

Метод автентифікації по сітківці ока отримав практичне застосування приблизно в середині 50-х років минулого століття. Саме тоді була встановлена унікальність малюнка кровоносних судин очного дна (навіть у близнюків дані малюнки не збігаються). Для сканування сітківки використовується інфрачервоне випромінювання низької інтенсивності, спрямоване через зіницю до кровоносних судин на задній стінці ока. З отриманого сигналу виділяється кілька сотень особливих точок, інформація про які зберігається в шаблоні.

До недоліків таких систем слід в першу чергу віднести психологічний фактор: не всякій людині приємно дивитися в незрозумілий темний отвір, де щось світить в око. До того ж, подібні системи вимагають чіткого зображення і, як правило, чутливі до неправильної орієнтації сітківки. Тому потрібно дивитися дуже акуратно, а наявність деяких захворювань (наприклад, катаракти) може перешкоджати використанню даного методу. Сканери для сітківки ока набули великого поширення для доступу до надсекретних об’єктів, оскільки забезпечують одну з найнижчих ймовірностей помилки першого роду (відмова в доступі для зареєстрованого користувача) і майже нульовий відсоток помилок другого роду.

Автентифікація по райдужній оболонці ока

Дана технологія біометричної автентифікації використовує унікальність ознак і особливостей райдужної оболонки ока. Райдужна оболонка – тонка рухома діафрагма ока, що розташована за рогівкою, між передньою і задньою камерами ока, перед кришталиком. Райдужна оболонка утворюється ще до

народження людини, і не змінюється протягом усього життя. Райдужна оболонка за текстурою нагадує мережу з великою кількістю оточуючих кіл і малюнків, які можуть бути виміряні комп'ютером. Малюнок райдужної оболонки дуже складний, це дозволяє відібрати близько 200 точок, за допомогою яких забезпечується висока ступінь надійності автентифікації. Для порівняння, кращі системи ідентифікації за відбитками пальців використовують 60-70 точок.

Технологія розпізнавання райдужної оболонки ока була розроблена для того, щоб звести нанівець нав'язливість сканування сітківки ока, при якому використовуються інфрачервоні промені або яскраве світло. Вчені також провели ряд досліджень, які показали, що сітківка ока людини може змінюватися з часом, в той час як райдужна оболонка ока залишається незмінною. І найголовніше, що неможливо знайти два абсолютно ідентичних малюнка райдужної оболонки ока, навіть у близнюків. Для отримання індивідуального запису про райдужну оболонку ока чорно-біла камера робить 30 записів в секунду. Ледве помітне світло висвітлює райдужну оболонку, і це дозволяє відеокамері сфокусуватися на райдужці. Потім запис оцифровується і зберігається в базі даних зареєстрованих користувачів. Вся процедура займає кілька секунд, і вона може бути повністю комп'ютеризована за допомогою голосових вказівок і автофокусування. Камера може бути встановлена на відстані від 10 см до 1 метра, в залежності від скануючого обладнання. Потім отримане зображення райдужної оболонки перетворюється в спрощену форму, записується і зберігається для подальшого порівняння. Окуляри та контактні лінзи, навіть кольорові, не діють на якість автентифікації.

Вартість даної системи завжди була стримуючим фактором перед впровадженням технології, але зараз системи ідентифікації по райдужній оболонці стають доступнішими для різних компаній. Прихильники технології заявляють про те, що розпізнавання райдужної оболонки ока дуже скоро стане загальноприйнятою технологією ідентифікації в різних областях.

Автентифікація по геометрії руки

У цьому біометричний методі для автентифікації особистості використовується форма кисті руки. Через те, що окремі параметри форми руки не є чимось унікальним, доводиться використовувати кілька характеристик. Скануються такі параметри руки, як вигини пальців, їх довжина і товщина, ширина і товщина тильного боку руки, відстань між суглобами і структура кістки. Також геометрія руки включає в себе дрібні деталі (наприклад, зморшки на шкірі). Хоча структура суглобів і кісток є відносно сталими ознаками, але розпухання тканин або удари руки можуть спотворити вихідну структуру.

Проблема технології: навіть без урахування можливості ампутації, захворювання під назвою «артрит» може сильно перешкодити застосуванню сканерів.

За допомогою сканера, який складається з камери і підсвічуючих діодів (при скануванні кисті руки, діоди включаються по черзі, це дозволяє отримати різні проекції руки), будується тривимірний образ кисті руки. Надійність автентифікації по геометрії руки співрозмірна з автентифікацією за відбитком пальця.

Системи автентифікації по геометрії руки широко поширені, що є доказом їх зручності для користувачів. Процедура отримання зразка досить проста і не висуває високих вимог до зображення. Розмір отриманого шаблону дуже малий, кілька байт. На процес автентифікації не впливають ні температура, ні вологість, ні забрудненість.

Системи автентифікації, засновані на геометрії руки, почали використовуватися в світі на початку 70-х років

Автентифікація по геометрії обличчя

Біометрична автентифікація людини по геометрії обличчя досить поширений спосіб ідентифікації. Технічна реалізація являє собою складну математичну задачу. Широке застосування мультимедійних технологій, за допомогою яких можна побачити достатню кількість відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах і інших місцях скупчення людей, стало вирішальним у розвитку цього напрямку. Для побудови тривимірної моделі людського обличчя, виділяють контури очей, брів, губ, носа, і інших різних елементів особи, потім обчислюють відстань між ними, і за допомогою нього будують тривимірну модель.

Для побудови унікального шаблону, що відповідає певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту особи, нахилу, зміни освітленості, зміни виразу. Діапазон таких варіантів варіюється в залежності від цілей застосування даного способу (для ідентифікації, автентифікації, віддаленого пошуку на великих територіях і т. д.). Деякі алгоритми дозволяють компенсувати наявність у людини окулярів, капелюхів, вусів і бороди.

Автентифікація по термограмі обличчя

Спосіб заснований на дослідженнях, які показали, що термограма обличчя унікальна для кожної людини. Термограму отримують за допомогою камер інфрачервоного діапазону. На відміну від автентифікації по геометрії обличчя, даний метод розрізняє близнюків. Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, температура тіла,

охолодження шкіри обличчя в морозну погоду не впливають на точність термограми. Через невисоку якість автентифікації, метод на даний момент не має широкого поширення.

Динамічні методи

Автентифікація по голосу

Біометричний метод автентифікації по голосу, характеризується простотою в застосуванні. Даному методу не потрібно дорога апаратура, досить мікрофона і звукової плати. В даний час дана технологія швидко розвивається, так як цей метод автентифікації широко використовується в сучасних бізнес-центрах. Існує досить багато способів побудови шаблону по голосу. Зазвичай, це різні комбінації частотних і статистичних характеристик голосу. Можуть розглядатися такі параметри, як модуляція, інтонація, висота тону, і т. п.

Основним і визначальним недоліком методу автентифікації по голосу – низька точність методу. Наприклад, людину з застудою система може не впізнати. Важливу проблему становить різноманіття проявів голосу однієї людини: голос здатний змінюватися в залежності від стану здоров'я, віку, настрою і т. д. Це представляє серйозні труднощі при виділенні характерних властивостей голосу людини. Крім того, облік шумової компоненти є ще однією важливою і невирішеною проблемою в практичному використанні автентифікації по голосу. Так як ймовірність помилок другого роду при використанні даного методу велика (порядку одного відсотка), автентифікація по голосу застосовується для управління доступом в приміщеннях середнього рівня безпеки, такі як комп'ютерні класи, лабораторії виробничих компаній і т.д.

Автентифікація по рукописному почерку

Метод біометричної автентифікації по рукописному почерку ґрунтується на специфічному русі людської руки під час підписання документів. Для збереження підпису використовують спеціальні ручки або сприйнятливі до тиску поверхні. Цей вид автентифікації людини використовує його підпис. Шаблон створюється в залежності від необхідного рівня захисту. Зазвичай виділяють два способи обробки даних про підписи:

- Аналіз самого підпису, тобто використовується просто ступінь збігу двох картинок.
- Аналіз динамічних характеристик написання, тобто для автентифікації будується згортка, в яку входить інформація по підпису, часові і статистичні характеристики її написання.

4.2. Технології управління доступом і авторизації

Після того як користувач, пройшовши автентифікацію, довів свою легальність, йому надається певний набір прав по відношенню до захищених системою ресурсів.

Наділення легальних користувачів правами доступу до ресурсів називається **авторизацією**. Процедура приведення авторизації в дію називається **управлінням доступом** (Access Control).

Якщо, наприклад, суб'єкт намагається використовувати ресурс із забороненим для нього типом доступу, то механізм управління доступом повинен відхилити цю спробу і, можливо, повідомити систему про цей інцидент з метою генерації сигналу тривоги.

4.2.1. Форми подання обмежень доступу

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. Застосування цього принципу обмежує ті можливі втрати, які можуть бути понесені в результаті ненавмисних помилок або неавторизованих дій.

Рішення про наділення користувачів правами (або, що одне і те ж, про обмеження їх прав на доступ до ресурсів) ґрунтується на політиці безпеки підприємства і може бути сформульовано в різних формах.

Обмеження доступу може задаватись у формі **правил**. На підставі правила система управління доступом в будь-який момент часу динамічно вирішує питання про надання або ненадання доступу. Правило може будуватися з урахуванням різних факторів, в тому числі тривалості сеансу зв'язку (обмеження доступу за часом використання ресурсу), віку людини (обмеження для дітей на доступ до деяких сайтів), часу доби (дозвіл на використання ресурсів і сервісів Інтернету тільки в робочі години). Популярною мірою обмеження доступу в Інтернет є **CAPTCHA** («**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part» – повністю автоматизований публічний тест Тюринга для розрізнення комп'ютерів і людей), в цьому випадку суб'єкту, який звернувся із запитом до ресурсу, пропонується ввести символи, виведені на екран в такому спотвореному вигляді, в якому їх зможе розпізнати лише людина – таким чином виключається доступ до ресурсів штучних суб'єктів (програмних систем). Іншим поширеним правилом є правило, яке носить спеціальну назву – необхідно знати (need to know). Відповідно до цього правила кожен співробітник має право

доступу тільки до тих інформаційних ресурсів, які йому необхідні для виконання його службових обов'язків.

Для обмеження доступу використовуються також контентно- і контекстно-залежні правила. Наприклад, в компанії може бути прийнято правило, що деяким категоріям користувачів забороняється доступ до документів, що містять певні ключові слова або фрази, такі як «для обмеженого використання», «секретно» або кодову назву проекту. Обмеження можуть бути накладені на доступ до ресурсів, що містять текст іноземною мовою. Це були приклади **контентно-залежних правил**. У **контекстно-залежних правилах** беруться до уваги деякі фактори, що характеризують поточний стан середовища і/або передісторію (контекст) запиту. Найпростішим правилом такого роду є відмова в доступі користувачу, який зробив підряд три безуспішних спроби автентифікації. Або доступ до деякого мережевого ресурсу підприємства може бути заборонений, якщо до моменту поточного звернення користувач виконав кілька звернень до зовнішнього сайту, вміст якого не пов'язаний безпосередньо з його професійними інтересами.

Ефективним засобом обмеження доступу є **конфігурація користувацького інтерфейсу**. Таким чином користувач може бути позбавлений не лише можливості звертатися до тих чи інших каталогів і файлів, але і можливості бачити на своєму екрані частину структури файлової системи, доступ до якої йому заборонений. Адміністратор може налаштувати систему меню користувацького інтерфейсу так, що деякі пункти цих меню не будуть виводитися на екран, що виключить принципову можливість запуску користувачем частини функцій.

Матриця прав доступу є універсальною формою подання політики контролю доступу, вона прямо («в лоб») описує для кожного користувача набір конкретних операцій, які йому дозволяється виконувати по відношенню до кожного об'єкту (рис. 4.8).

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

Рис. 4.8. Матриця прав доступу

Матричний спосіб опису прав доступу теоретично дає можливість відобразити все різноманіття відносин суб'єктів і об'єктів системи для всіх можливих поєднань {суб'єкт, об'єкт, призначені права}. Однак цей універсальний спосіб представлення, як правило, дуже складно реалізувати на практиці через громіздкість матриці, з огляду на величезну кількість елементів – як суб'єктів, так і об'єктів – в обчислювальній системі.

Особливістю матриці прав доступу є не тільки її велика розмірність, але і наявність великого числа нульових елементів. Такий вид матриць в математиці називають розрідженими. Нульове значення тут говорить про те, що для даного поєднання {суб'єкт, об'єкт} права доступу не визначені, а саме такі поєднання складають більшість в реальних системах. Властивість розрідженості матриці може бути використано для більш компактного представлення правил доступу.

З кожним об'єктом можна зв'язати **список управління доступом** (Access Control List, ACL), в якому вказані тільки ті суб'єкти (користувачі), які мають дозвіл на доступ до даного об'єкту (ресурсу). Зрозуміло, що кількість суб'єктів в даному списку буде значно менше загального числа суб'єктів системи. Такі списки повинні бути створені для всіх ресурсів. Спосіб опису прав доступу набором списків настільки ж універсальний і гнучкий, як матриця, але разом з тим має більш компактний вигляд, так як він не включає порожні елементи матриці. Список ACL складається з **елементів управління доступом** (Access Control Element, **ACE**), кожен з яких описує права доступу певного користувача до даного ресурсу. На рис. 4.9 список ACL складається з трьох елементів ACE.

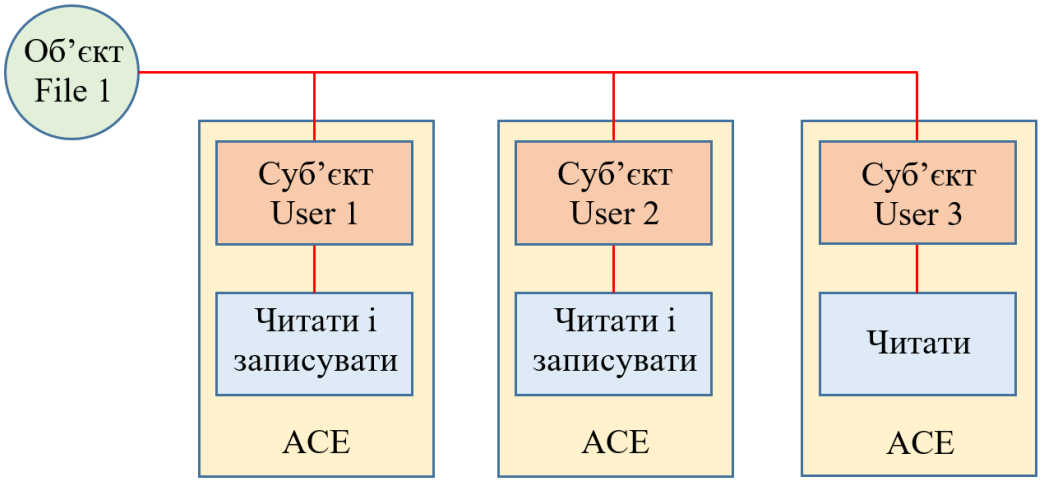


Рис. 4.9. Список управління доступом до об'єкту

Права доступу можуть бути визначені як по відношенню до ресурсів, так і по відношенню до користувачів. В останньому випадку його називають списком

дозволів (Capability). На рис. 4.10 показаний список дозволів, які має користувач User 1 по відношенню до ресурсів File 1, File 2 і File 3.

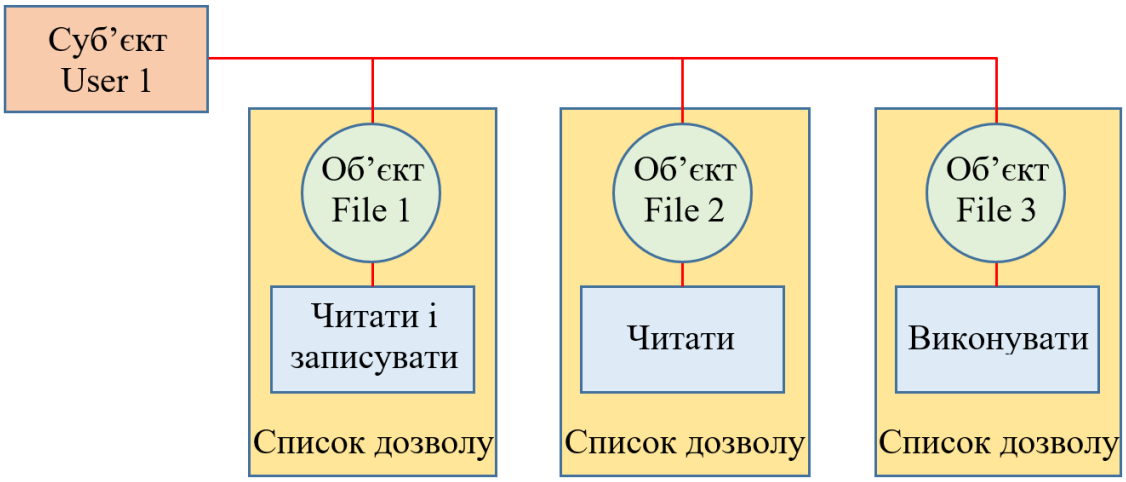


Рис. 4.10. Список дозволів користувача User 1

Очевидно, що сукупність списків управління доступом до всіх ресурсів системи несе ту ж саму інформацію, що і сукупність списків дозволів для всіх користувачів так як і ті й інші є різними проекціями однієї і тієї ж матриці. В одних реалізаціях контролю доступу (наприклад, в більшості операційних систем) застосовуються обмеження, що задані для об'єкта (ACL), а в інших (наприклад, в деяких розширеннях системи Kerberos, що включають авторизацію) – обмеження для суб'єкта (списки дозволів).

Іншим способом «стиснення» матриці є визначення прав доступу для груп суб'єктів по відношенню до груп об'єктів. Таке представлення можливе, коли багато елементів матриці мають однакове значення, що відповідає ситуації в реальній системі, коли деяка група користувачів має однакові права. Це дає можливість компактно описати права доступу за допомогою матриці меншої розмірності.

У деяких випадках, якщо існує просте правило визначення прав доступу, зберігання матриці взагалі не потрібне, значення елементів матриці можуть обчислюватися системою управління доступом динамічно. Наприклад, нехай всі об'єкти і суб'єкти системи спочатку забезпечені мітками з однієї і тієї ж множини. Крім того, припустимо для простоти викладу, що для всіх об'єктів визначено тільки один вид операції доступу. І нехай існує правило: доступ до об'єкта дозволений, якщо мітки суб'єкта та об'єкта збігаються, і не дозволений, якщо не збігаються. Маючи таке правило, немає сенсу заздалегідь створювати і

зберігати матрицю – простіше обчислювати відповідний елемент при кожній спробі доступу.

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.

4.2.2. 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. Управління доступом в методі DAC є дискреційним, або довільним, в тому сенсі, що суб’єкт, що володіє деякими дозволами на доступ до об’єктів, може на свій розсуд передати частину своїх повноважень (іноді прямо, а іноді – опосередковано) іншим суб’єктам.

Звідси випливають дві 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.

Таким чином, процедура авторизації є розподіленою між великою кількістю користувачів-власників. Власниками вважаються користувачі, які створили об’єкт, або користувачі, які були призначені власниками іншими, уповноваженими на те користувачами або системними процесами. Власник має повний контроль над створеним ним об’єктом і несе всю повноту відповідальності за управління доступом до нього. Разом з тим він може призначати права доступу до своїх об’єктів, керуючись деяким правилом, прийнятим на підприємстві.

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. Однак ця перевага має свій зворотний бік. Як і будь-яка розподілена система, система управління доступом за методом DAC страждає від неможливості гарантовано проводити загальну політику, здійснювати надійний контроль дій користувачів. Будь-яка політика безпеки, прийнята на підприємстві, може бути порушена в результаті помилкових або шкідливих дій користувачів.

Інший недолік дискреційного методу пов’язаний з тим, що тут права на доступ визначаються по відношенню до об’єкта, а не до його вмісту. Це означає, що будь-який користувач (точніше, його процес), який має доступ до файлу відповідно до деякого списку ACL1, може скопіювати його вміст в інший файл, що характеризується іншим списком ACL2. Це вказує, що системи з контролем доступу за методом DAC не можуть застосовуватися там, де потрібно дуже високий рівень захисту інформації.

4.2.3. 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.

Простота правил досягається тим, що як суб'єкти, так і об'єкти розбиваються на невелике число груп. Кожній групі об'єктів присвоюється **рівень (гриф) секретності**, а групам суб'єктів – **рівні допуску** до об'єктів того чи іншого рівня секретності. У різних системах можуть бути прийняті різні правила, але всі вони базуються на порівнянні рівня секретності об'єкта і рівня допуску суб'єкта. Наприклад, правило може бути наступним: суб'єкту дозволяється доступ до об'єкта, якщо рівень його допуску дорівнює рівню або вище рівня секретності об'єкта. На рис. 4.11 це правило представлено у вигляді матриці.

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

Рис. 4.11. Правило мандатного доступу, представлене у вигляді матриці

Користувачі позбавлені можливості керувати доступом до своїх ресурсів або передавати свої права іншим користувачам. На відміну від систем DAC, мандатний доступ має централізований характер і дозволяє жорстко проводити прийняту політику безпеки.

Елементи, що описують рівні секретності об'єктів або рівні допуску суб'єктів, називають **мітками безпеки** (Security Labels). Мандатний метод управління доступом передбачає призначення міток безпеки всім без винятку суб'єктам і об'єктам системи, щоб в подальшому вони використовувалися системою для прийняття рішення про допуск.

У більшості випадків для адекватного відображення політики безпеки неможливо сформулювати правило, що базується на обліку тільки рівнів секретності і допусків. До одного і того ж рівня секретності можуть бути віднесені різні матеріали, а відповідно до принципу мінімальних привілеїв користувач повинен отримувати доступ тільки до тієї інформації, яку йому необхідно знати.

Для того, щоб зробити можливим більш специфічне задання прав доступу, в мітки безпеки об’єкта і суб’єкта додається інформація про конкретний вид даних, до якого належить даний об’єкт або до якого дозволений доступ даному суб’єкту відповідно.

Таким чином, кожна мітка безпеки складається з двох частин:

- частина, яка відображає рівень секретності/допуску, називається **класифікацією**;
- частина, що характеризує специфіку інформації, називається **категорією**.

Категорія відносить дані до певного виду інформації. Наприклад, різні категорії можуть бути присвоєні матеріалами, які належать до різних проектів, різних адміністративних підрозділів, різних професійних груп. Одному і тому ж об’єкту/суб’єкту може бути присвоєно кілька категорій. Так, звіт про завершення етапу деякої антитерористичної операції може бути віднесений не тільки до категорії матеріалів, що стосуються даної операції, а й додатково до категорії матеріалів підрозділу, що займається цією роботою. Об’єкти однієї категорії можуть бути класифіковані по-різному: наприклад, одна частина віднесена до більш високого рівня секретності, а інша частина – до нижчого.

Рівні секретності/допуску, яких зазвичай не багато, утворюють ієрархію від найвищого до найнижчого рівня. Суб’єкт, який має допуск до деякого рівня, отримує його і по відношенню до всіх нижчих рівнів.

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.

Рисунок 5.12 ілюструє співвідношення між класифікацією і категорією. Тут різний колір кругів служить для позначення різних категорій об’єктів. На рисунку показано три рівня класифікації: «цілком таємно», «таємно» і «для службового користування». Об’єкти однієї категорії можуть належати різним рівням класифікації. У мітці безпеки суб’єкта вказана класифікація «таємно» та перераховані дві категорії, до яких йому дозволено доступ. Стрілками показані три спроби доступу. Спроба звернення до рівня «цілком таємно» була заблокована системою через недостатньо високий рівень допуску суб’єкта.

Звернення до об’єкту рівня «таємно» було дозволене, так як класифікація суб’єкта рівна класифікації об’єкта, а категорія об’єкта співпала з однією з категорій, зазначених в мітці безпеки суб’єкта. Спроба доступу до об’єкта рівня «для службового користування» була відхилена, хоча суб’єкт і має більш

високий рівень допуску («секретно»). В даному випадку обмеженням служить категорія об’єкта, яка не збігається з жодною з категорій суб’єкта.

Мандатний доступ, як уже зазначалося, є більш безпечним, ніж дискреційний, але для його ефективної реалізації потрібен великий обсяг підготовчої роботи, а після запуску системи необхідно підтримувати в актуальному стані мітки безпеки існуючих об’єктів, а також призначати мітки новим ресурсам і користувачам.

4.2.4. Рольовий метод управління доступом

Метод управління доступом RBAC, базується на ролях, в порівнянні з методами DAC і MAC більш наближений до реального життя. Як видно з назви, основною його властивістю є використання «ролей». Поняття «роль» в даному контексті найближче до поняття «посада» або «коло посадових обов’язків». Оскільки одну і ту ж посаду можуть займати кілька людей, то і одна і та ж роль може бути приписана різним користувачам.

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. Система RBAC найкраще працює в організаціях, в яких існує чіткий розподіл посадових обов’язків.

Дозволи приписуються ролям, а не окремим користувачам або групам користувачів. А вже потім ті чи інші ролі приписуються користувачеві. Наприклад, в системі управління доступом, розгорнутої в банку, всім юристам приписана роль «юрист», трейдерам – роль «трейдер», менеджерам – роль «менеджер» і т. Д. Процес визначення ролей повинен включати ретельний аналіз того, як функціонує організація, який набір функцій повинен виконувати працівник, який має ту чи іншу посаду. Кожній з ролей призначаються права доступу, необхідні і достатні користувачам для виконання службових обов’язків, обумовлених приписуванням до даної ролі.

Кожному користувачу може бути призначено кілька ролей (з деякими обмеженнями). Під час сеансу роботи користувача всі ролі, які йому призначені, стають активними і він отримує права доступу, які є результатом об’єднання прав доступу всіх цих груп.

Всі користувачі, які відіграють одну і ту ж роль, мають ідентичні права. Зміна виробничої ситуації – розширення бізнесу, впровадження нових технологій, просування співробітника по службові або переведення в інший підрозділ і ін. – все це може викликати анулювання однієї ролі користувача і приписування йому іншої ролі. Такий підхід спрощує адміністрування прав

доступу: замість необхідного в методах DAC і MAC відстеження і поновлення прав кожного окремого користувача в методі RBAC досить замінити одну роль іншою.

Таким чином, в системі RBAC є зручні механізми для дотримання принципу мінімальних привілеїв. І хоча, теоретично метод DAC дозволяє проводити ще більш тонке налаштування прав користувача, практично неможливо проконтролювати цей процес так, щоб домогтися реалізації цього принципу. В системі, де механізм призначення прав розподілений між усіма користувачами, дуже складно відстежити ситуацію, коли набір прав користувача стає неадекватним по відношенню до вирішуваних ним завдань.

Згідно природі виробничих відносин, посадові обов'язки співробітників, що займають різні позиції, можуть частково перекриватися. Деякі найзагальніші функції, такі, наприклад, як ознайомлення з інструкціями щодо дотримання режиму роботи підприємства, резервування відпусток, фіксування на внутрішньому сайті компанії індивідуального робочого графіка і ін., Можуть бути обов'язковими для всіх співробітників. Стосовно до ролей це означає, що адміністратор повинен виконувати багато рутинної роботи по приписування одних і тих же прав доступу різним ролям, в тому числі при створенні нових. Вирішенням цієї проблеми є ієрархічна організація ролей, коли одна роль може включати іншу роль, тим самим розширюючи свій набір прав за рахунок додавання прав, асоційованих з інкапсульованою роллю.

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 (рис. 27.18). Таким чином, встановлення відносин спадкування є ще одним способом наділення користувача правами поряд з явним призначенням користувачеві деякої ролі.

Важливим становищем безпеки є принцип поділу обов'язків, відповідно до якого певні посадові функції не повинні доручатися одній і тій же людині. Наприклад, працівник, якому призначена роль «інженер», побувавши у відрядженні, повинен після повернення скласти фінансовий звіт про свої витрати. Потім цей звіт повинен бути перевірений і поданий до оплати, ці дії покладаються на співробітника, віднесеного до ролі «співробітник фінансового відділу». Зрозуміло, що таке поєднання функцій, тобто одночасна приналежність одного користувача до ролей «інженер» і «співробітник фінансового відділу», є небажаним. Щоб уникнути подібних ситуацій, в методі RBAC передбачений спеціальний механізм, який накладає обмеження на приписування ролей користувачам. Цей механізм діє таким чином. Сукупність ролей, щодо суміщення яких потрібно встановлювати обмеження, об'єднується в стійку

групу, і до неї приписується число-обмежувач. У даному випадку це група ролей {«інженер», «співробітник фінансового відділу»}, якій повинен бути приписаний обмежувач 1. Якщо тепер адміністратором буде зроблена спроба приписати користувачеві обидві ці ролі, то система заблокує його дії.

Отже, 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. В DAC права призначаються користувачеві «дрібними порціями», що дозволяє йому виконувати ту чи іншу конкретну операцію над окремим об’єктом (запис в певний файл, читання іншого файлу, запуск деякої програми). Такий спосіб допомагає дуже точно створювати і індивідуально налаштовувати комплекс прав доступу користувача, однак він є дуже трудомістким, внаслідок чого зростає можливість помилок. У RBAC права доступу надаються у вигляді інтегрованого набору дозволів, розрахованих на можливість виконання деяких складних операцій: заповнення кредитного документа, генерація звітів і ін.
- RBAC є централізованим методом управління доступом – так само, як і в мандатному методі, користувач позбавлений можливості керувати призначенням прав. Призначення користувачу ролі можна вважати деяким аналогом приписування рівня допуску користувачу мандатної системи. Однак RBAC є більш гнучким способом, ніж MAC, за можливостями налаштування прав доступу він знаходиться ближче до DAC.

Метод RBAC не можна віднести до добре масштабованого. Він ефективно працює в межах єдиної системи або додатку, таких, наприклад, як FreeBSD, Solaris, СУБД Oracle, MS Active Directory, але на великих підприємствах, що мають тисячі співробітників, підтримка множини ролей з їх відносинами спадкування стає складним завданням. Займаючи проміжне становище між мандатним і дискреційним методами, рольове управління доступом поступається їм обом в масштабованості. У мандатному методі централізований характер прийняття рішень (який не сприяє масштабованості) компенсується простотою виконуваного алгоритму призначення прав. У дискреційному ж методі, навпаки, складність механізму наділення правами компенсується розподіленим характером процедури прийняття рішень.

4.3. Системи автентифікації і управління доступом операційних систем

4.3.1. 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). Зрозуміло, що при віддаленому логічному вході ризики безпеки вищі, так як автентифікаційні дані передаються через мережу (корпоративну або Інтернет) і їх легше перехопити. Перехоплення даних автентифікації є загрозою навіть у випадку суворої автентифікації, коли пароль не передається у відкритому вигляді по мережі або ж не передається зовсім: при наявності великого масиву автентифікаційних даних, тобто даних перехватів великої кількості процедур входу одного і того ж користувача, пароль може бути обчислений за наявними результатами його введення.

Хоча локальні системи автентифікації ОС підтримують всі поширені методи автентифікації – на основі багаторазових і одноразових паролів (апаратних і програмних), біометричних даних і цифрових сертифікатів, – основним методом автентифікації користувачів є метод на базі багаторазового паролю. Практично всі універсальні ОС, такі як MS Windows, Unix/Linux і Mac OS X пропонують цей метод за замовчуванням.

Одноразові паролі, що забезпечують більш надійну автентифікацію, ніж багаторазові, частіше застосовуються при віддаленому логічному вході через з'єднання VPN з шифруванням інформації, де передача автентифікаційної інформації йде через Інтернет та, отже, ризик її перехоплення і злому особливо великий. Одноразові паролі можуть поєднуватися з багаторазовими при двофакторній автентифікації.

Автентифікація на основі сертифікатів застосовується найчастіше для віддалено працюючих користувачів, які пред'являють сертифікати, видані сервером сертифікації організації, до якої належить користувач.

Автентифікація на основі біометричних даних штатними засобами універсальних ОС, зазвичай, не підтримується, так як їх підвищена надійність потрібна тільки в особливо захищених системах і, крім того, для підтримки біометричної автентифікації потрібно придбати і встановити відповідне спеціальне програмне забезпечення і спеціальні пристрої.

Необхідно відрізняти процедуру автентифікації користувача операційної системи від процедури автентифікації користувача серверної частини деякого додатка. Багато серверних додатків мають власну систему автентифікації користувачів, що ніяк не пов'язана з системою автентифікації ОС, під управлінням якої вони працюють. Наприклад, так працюють багато реалізації FTP-сервера, сервера баз даних. Незалежність системи автентифікації сервера додатків має як свої позитивні, так і негативні сторони. Перевагою тут є розмежування за замовчуванням користувачів ОС, яким потенційно може знадобитися доступ до будь-якого ресурсу комп'ютера, і користувачів деякого сервісу, яким потрібен доступ тільки до ресурсів, що належать до даного сервісу, наприклад тільки до файлів, що зберігаються в кореневому каталозі FTP-сервера. До недоліків можна віднести низьку захищеність протоколу автентифікації деяких додатків, а також необхідність запам'ятовування двох різних імен і паролів для одного і того ж користувача, помилки адміністраторів ОС і сервісів через дублювання облікових записів і т. п.

4.3.2. 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.

Як приклад розглянемо деякі властивості системи управління доступом в ОС сімейства Windows. Ця система, побудована на основі дискреційного алгоритму, відрізняється високим ступенем гнучкості, яка досягається за рахунок великої кількості типів суб'єктів і об'єктів доступу, а також деталізації операцій доступу.

Для поділюваних ресурсів в ОС Windows застосовується загальна модель об'єкта, яка містить такі характеристики безпеки, як набір допустимих операцій, ідентифікатор власника, список управління доступом. Об'єкти створюються для будь-яких ресурсів в тому випадку, коли вони є або стають поділюваними: файлів, каталогів, пристроїв, секцій пам'яті, процесів.

Для системи безпеки ОС Windows характерна наявність великої кількості різних вбудованих суб'єктів доступу – як окремих користувачів, так і груп. Так, в системі завжди є користувачі Administrator, System і Guest, а також групи Users, Administrators, Account Operators, Server Operators, Everyone і ін. Зміст цих вбудованих користувачів і груп полягає в тому, що вони початково наділені деякими правами, полегшуючи адміністратору роботу по створенню ефективної системи розмежування доступу. При додаванні нового користувача адміністратору залишається тільки вирішити, до якої групи або груп віднести цього користувача. Звичайно, адміністратор може створювати нові групи, а також додавати права до вбудованих груп для реалізації власної політики безпеки, але в багатьох випадках вбудованих груп виявляється цілком достатньо.

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. За рахунок зменшення набору можливостей (доступних користувачу за замовчуванням) адміністратор може «змусити» користувача

працювати з тим операційним середовищем, яке найкраще відповідає політиці безпеки.

В основному саме права, а не дозволи відрізняють одну вбудовану групу користувачів від іншої. Права у вбудованих груп можуть бути вбудованими або змінними. **Вбудовані права** є невід'ємними атрибутами вбудованих груп, адміністратор не може їх редагувати. **Змінні права** можна видаляти або додавати до прав вбудованої групи із загального списку змінюваних прав. Наприклад, вбудована група Users не має ніяких змінних або вбудованих прав, в той час як група Administrators наділена широким набором як вбудованих (створення і управління користувацькою обліковою інформацією, управління аудитом, форматування жорсткого диска сервера і ін.), так і змінних прав (інтерактивний і віддалений логічний вхід, встановлення прав власності на файли, управління аудитом подій, пов'язаних з безпекою, зміна системного часу, зупинка системи і ін.).

Для ОС Windows характерна висока ступінь деталізації операцій доступу. Так, для доступу до файлів і каталогів передбачено два типи дозволів:

- **індивідуальні дозволи** – відносяться до елементарних операцій;
- **стандартні дозволу** – об'єднанням індивідуальних дозволів.

У таблиці 4.2 наведено перелік індивідуальних дозволів на доступ до файлів.

Таблиця 4.2. Індивідуальні дозволи на доступ до файлів

Дозвіл	Для файлу
Read (R)	Читання даних, атрибутів, імені власника і дозволів файлу
Write (W)	Читання імені власника і дозволів файлу, зміна атрибутів файлу, зміна і додавання даних файлу.
Execute (X)	Читання атрибутів файлу, імені власника і дозволів. Виконання файлу, якщо він зберігає код програми.
Delete (D)	Видалення файлу.
Change Permission (P)	Зміна дозволів файлу.
Take Ownership (O)	Вступ у володіння файлом.

Для файлів визначено чотири стандартних дозволи: No Access, Read, Change і Full Control, відповідність яких групам індивідуальних дозволів показано в табл. 4.3.

Таблиця 4.3. Стандартні та індивідуальні дозволи для файлів

Стандартні дозволи	**Індивідуальні дозволи**
No Access	Ні одного
Read	RX
Change	RWXD
Full Control	Усі

Результатом успішної автентифікації користувача в ОС Windows є створення для нього системою так званого **токена доступу** (Access Token). Токен доступу прив'язується до всіх процесів, які даний користувач створює протягом сеансу роботи. Токен доступу включає ідентифікатор користувача і ідентифікатори всіх груп, в які він входить, список прав користувача на виконання системних операцій і ін.

Доступ до об'єкту описується списком ACL. Власник об'єкта – зазвичай користувач, який його створив, – має право керувати доступом до об'єкту і може змінювати ACL об'єкта, щоб дозволити або не дозволити іншим здійснювати певний вид доступу до об'єкта.

Перевірка прав доступу до об'єктів будь-якого типу виконується централізовано за допомогою модуля ОС – **монітору безпеки** (Security Reference Monitor). Монітор безпеки порівнює ідентифікатори користувача і груп користувачів з токена доступу процесу з відповідними ідентифікаторами, що зберігаються в елементах ACL об'єкта. Система безпеки могла б здійснювати перевірку дозволів кожен раз, коли процес використовує об'єкт. Але список ACL складається з багатьох елементів, процес протягом свого існування може мати доступ до багатьох об'єктів, і кількість активних процесів в кожен момент часу також велика. Тому, для зниження витрат перевірка виконується тільки при першому зверненні процесу до об'єкта, а не при кожному використанні об'єкта.

Гнучкість системи безпеки ОС сімейства Windows багато в чому визначається різноманітністю прав на виконання системних дій, високим ступенем деталізації операцій доступу до об'єктів, а також існуванням вбудованих груп, що дозволяють адміністратору ефективно реалізовувати політику безпеки даної інформаційної системи.

4.4. Централізовані системи автентифікації та авторизації

4.4.1. Концепція єдиного логічного входу

Традиційний спосіб автентифікації за допомогою багаторазових паролів відмінно підходить для випадку, коли користувач весь час працює з єдиним комп'ютером, звертаючись тільки до його ресурсів та ресурсів Інтернету, що не вимагає автентифікації. Такому користувачу потрібно запам'ятовувати і періодично міняти тільки один пароль. На жаль, така ситуація рідко зустрічається в житті. Більш типовим є випадок, коли користувачу доводиться працювати на різних, географічно розосереджених комп'ютерах і при цьому отримувати доступ до різних серверів, наприклад серверу свого підприємства, серверів підприємства- партнера, до захищених веб-сайтів Інтернету.

У тому випадку, коли кожен комп'ютер і кожен сервер вимагають окремої автентифікації за допомогою багаторазового пароля, користувачу доводиться пам'ятати і оновлювати доволі багато паролів, і з цією задачею багато користувачів справляються не досить успішно. Тому не дивно, що великі зусилля витрачаються на розробку процедур **єдиного логічного входу** (Single Sign On, **SSO**).

Метою єдиного логічного входу 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.

В даний час не існує системи автентифікації, що реалізує концепцію єдиного логічного входу, яка б працювала з усіма типами операційних систем, додатків і при цьому враховувала б різноманітні відносини між організаціями, до яких належать користувачі та інформаційні ресурси. Однак є системи, що дозволяють організувати єдиний логічний вхід для однорідної інформаційної системи, наприклад для мережі, що використовує тільки одну певну ОС або один певний протокол автентифікації, або для групи організацій, які довіряють один одному при автентифікації своїх користувачів. Так, наприклад, властивість однорідності операційних систем є умовою застосування системи єдиного входу на основі довідкової служби Microsoft Active Directory.

Узагальнена схема, що ілюструє ідею систем єдиного логічного входу, представлена на рис. 4.12.

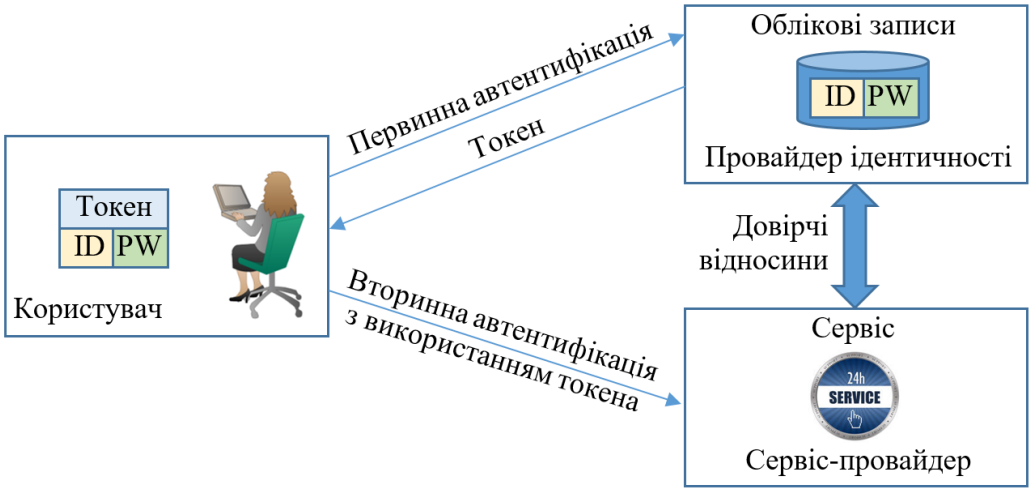


Рис. 4.12. Схема єдиного логічного входу

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.

Особливістю цієї схеми є те, що провайдер сервісів не підтримує базу облікових даних користувачів. База облікових даних є тільки у провайдера ідентичності, а провайдер сервісів довіряє результатам автентифікації користувачів, виконаної провайдером ідентичності. Кажуть, що в такому випадку існують довірчі відносини (Trust Relationships) між провайдером ідентичності і провайдером сервісів.

Користувач виконує логічний вхід в мережу, звертаючись до провайдера ідентичності. Якщо користувач зміг підтвердити свою автентичність, то провайдер ідентичності надає користувачу деяку інформаційну структуру –

токен доступу, який користувач зберігає у своїй базі даних. При необхідності отримання доступу до деякого сервісу користувач пред'являє токен доступу ресурсному серверу. Токен доступу захищений криптографічно таким чином, що ресурсний сервер має можливість перевірити той факт, що токен був виданий користувачу сервером автентифікації, якому ресурсний сервер довіряє автентифікувати користувачів. Кажуть, що в цьому випадку відбувається вторинна автентифікація користувача, але для самого користувача вона прозора, так як пред'явленням токена доступу займається програмне забезпечення його комп'ютера.

Токен доступу, зазвичай, має обмежений час дії, наприклад добу, тому користувач повинен його відновлювати, повторюючи процедуру з сервером автентифікації.

4.4.2. 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.

Система централізованої автентифікації тісно пов'язана з системою централізованого керування доступом, так як остання повинна базуватись на результатах автентифікації кожен раз, коли обчислювальний процес, який представляє користувача, намагається отримати доступ до ресурсу комп'ютера, що входить в деякий домен.

Система Kerberos може працювати в середовищі багатьох популярних ОС, наприклад в ОС Windows система Kerberos вбудована як основний компонент безпеки. Існують реалізації Kerberos для сімейства Unix, включаючи Red Hat Linux, Fedora, CentOS, і для Mac OS X. Поточною версією є версія 5, яка стандартизована IETF в RFC 4120.

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).

Мережева служба Kerberos побудована в архітектурі клієнт-сервер, що дозволяє їй працювати в найскладніших мережах. Kerberos-клієнт встановлюється на всіх комп'ютерах мережі, які можуть звернутися до будь-якої мережевої служби. У таких випадках Kerberos-клієнт від імені користувача передає запит на Kerberos-сервер і підтримує з ним діалог, необхідний для виконання функції системи Kerberos.

Отже, в системі Kerberos є наступні учасники: Kerberos-сервер, Kerberos-клієнти, ресурсні сервери (рис. 4.13). Kerberos-клієнти намагаються отримати доступ до мережевих ресурсів – файлів, додатків, принтеру і т. д., які знаходяться на ресурсних серверах. Цей доступ може бути наданий, по-перше, тільки легальним користувачам, а по-друге, при наявності у них достатніх повноважень, визначених службами авторизації відповідних ресурсних серверів – файловим сервером, сервером додатків, сервером друку. Однак в системі Kerberos ресурсним серверам забороняється «безпосередньо» приймати запити від клієнтів, їм дозволяється починати розгляд запиту клієнта тільки тоді, коли на це надходить дозвіл від Kerberos-сервера.

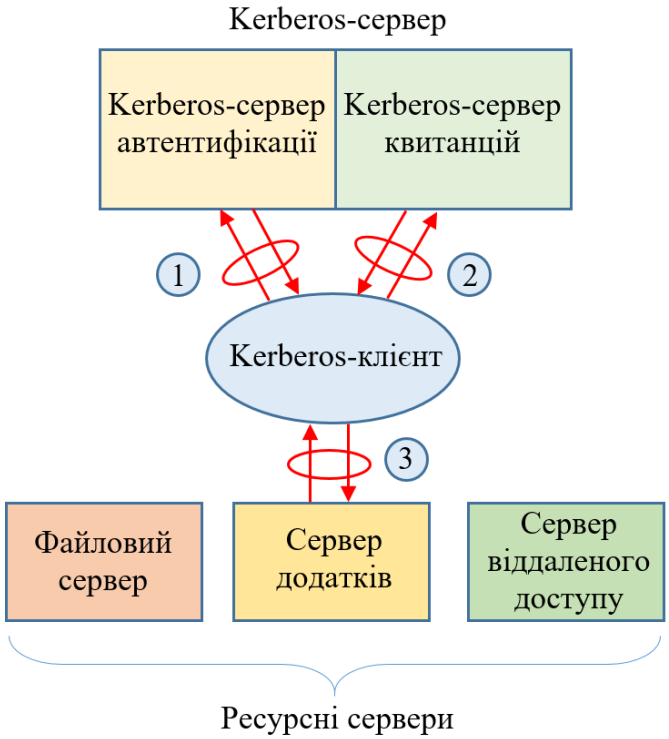


Рис. 4.13. Три етапи роботи системи Kerberos

Таким чином, 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.

Для вирішення першої і другої задач клієнт звертається до Kerberos-сервера. Кожна з цих двох задач вирішується окремим сервером, що входять до складу Kerberos-сервера. Виконання первинної автентифікації і видача дозволу на продовження процесу отримання доступу до ресурсу здійснюються так званим **Kerberos-сервером автентифікації** (Authentication Server, AS). Цей сервер зберігає в своїй базі даних інформацію про ідентифікатори і паролі користувачів. Паролі користувачів, а точніше хеш-функції від паролів, є секретними ключами користувачів.

Другу задачу, що пов’язана з отриманням дозволу на звернення до ресурсного сервера, вирішує інша частина Kerberos-сервера – **Kerberos-сервер квитанцій** (Ticket-Granting Server, TGS). Сервер квитанцій для легальних клієнтів виконує додаткову перевірку і дає клієнтові дозвіл на доступ до потрібного йому ресурсного серверу, для чого наділяє його електронною формою-квитанцією. Для виконання своїх функцій сервер квитанцій використовує копії секретних ключів всіх ресурсних серверів, які зберігаються у нього в базі даних. Крім цих ключів TGS-сервер має ще один секретний ключ, спільний з AS-сервером.

Третє завдання – отримання дозволу на доступ безпосередньо до ресурсу – вирішується на рівні ресурсного сервера власними засобами, які не відносяться безпосередньо до системи Kerberos, але здатними взаємодіяти з нею.

Секретні ключі користувачів і ресурсних серверів утворюють базу даних ключів Kerberos-сервера. Власне, володіння секретним ключем і є умовою автентифікації користувача або ресурсного сервера. Крім секретних ключів користувачів і ресурсних серверів в Kerberos також застосовуються секретні ключі сеансів автентифікації, які розподіляє Kerberos-сервер. Через ці обставини Kerberos-сервер також називається *Kerberos Key Distribution Centre*, або *Kerberos KDC*. Секретні ключі користувачів і ресурсних серверів називають ще майстер-ключами, так як вони є постійними ключами, що автентифікують суб’єкт, на відміну від ключів сеансів, які мають нетривалий термін дії.

Введення центру автентифікації істотно покращує масштабованість системи автентифікації на основі симетричного шифрування в порівнянні з децентралізованою системою. Дійсно, якщо на підприємстві є N користувачів і M ресурсних серверів, яким потрібна взаємна автентифікація, то при

децентралізованій автентифікації необхідно $N \times M$ ключів, що для підприємства з 1000 співробітників і 50 ресурсними серверами дає 50 000 ключів. При централізованій системі автентифікації необхідно мати тільки $N+M$ ключів, що становить 1050 ключів для даного прикладу, – тобто майже в 50 разів менше.

Kerberos забезпечує захищену автентифікацію сторін тільки в початковий момент сеансу обміну даними між ними. Після цього захист даних – їх конфіденційність, автентичність і цілісність – повинен забезпечуватися засобами ресурсного сервера і клієнта, якщо це необхідно.

4.4.3. Централізований контроль віддаленого доступу

Для управління віддаленими з'єднаннями невеликої локальної мережі цілком достатньо одного сервера віддаленого доступу. Проте, якщо локальна мережа об'єднує великі сегменти і число віддалених користувачів істотно зростає, то одного сервера віддаленого доступу недостатньо.

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

Розглянемо, як вирішується завдання контролю доступу до мережі віддалених користувачів відповідно до звичайної схеми, коли віддалені користувачі намагаються дістати доступ до мережевих ресурсів, які знаходяться під управлінням декількох різних ОС. Користувач з'єднується зі своїм **сервером віддаленого доступу** (Remote Access Server, **RAS**), і RAS виконує для нього процедуру автентифікації, наприклад по протоколу CHAP. Користувач логічно входить в мережу і звертається до потрібного сервера, де знову проходить автентифікацію і авторизацію, внаслідок чого отримує або не отримує дозвіл на виконання певної дії.

Неважко помітити, що така схема незручна користувачу, оскільки йому доводиться кілька разів виконувати автентифікацію – при вході в мережу на сервері віддаленого доступу, а потім ще кожного разу при зверненні до кожного ресурсного сервера мережі. Користувач вимушений запам'ятовувати декілька різних паролів. Крім того, він повинен знати порядок проходження різних процедур автентифікації в різних ОС. Виникають також труднощі з адмініструванням такої мережі. Адміністратор повинен заводити облікову інформацію про кожного користувача на кожному сервері. Ці розрізнені БД важко підтримувати в коректному стані. При звільненні співробітника складно виключити його з усіх списків. Виникають проблеми при призначенні паролів, істотно ускладнюється аудит.

Дані недоліки усуваються при установці в мережі централізованої служби автентифікації і авторизації. Для централізованого контролю доступу виділяється окремий сервер, званий сервером автентифікації. Цей сервер служить для перевірки достовірності віддалених користувачів, визначення їх повноважень, а також фіксації і накопичення реєстраційної інформації, пов'язаної з віддаленим доступом. Надійність захисту підвищується, якщо сервер віддаленого доступу запитує необхідну для автентифікації інформацію безпосередньо у сервера, на якому зберігається загальна БД системи захисту комп'ютерної мережі. Проте, в більшості випадків сервери віддаленого доступу потребують посередника для взаємодії з центральною БД системи захисту, наприклад із службою каталогів.

Більшість мережевих ОС і служб каталогів зберігають еталонні паролі користувачів з використанням одностороннього хешування, що не дозволяє серверам віддаленого доступу, які стандартно реалізовують протоколи PAP і CHAP, витягнути відкритий еталонний пароль для перевірки відповіді.

Роль посередника у взаємодії між серверами віддаленого доступу і центральної БД системи захисту може бути покладена на сервер автентифікації. Централізований контроль віддаленого доступу до комп'ютерних ресурсів за допомогою сервера автентифікації виконується на основі спеціалізованих протоколів. Ці протоколи дозволяють об'єднувати сервери віддаленого доступу і сервер автентифікації в одну підсистему, що виконує усі функції контролю віддалених з'єднань на основі взаємодії з центральною БД системи захисту. Сервер автентифікації створює єдину точку спостереження і перевірки усіх віддалених користувачів і контролює доступ до комп'ютерних ресурсів відповідно до встановлених правил.

До найбільш популярних протоколів централізованого контролю доступу до мережі віддалених користувачів відносяться протоколи TACACS (Terminal Access Controller Access Control System) і RADIUS (Remote Authentication Dial-In User Service). Вони призначені в першу чергу для організацій, в мережі яких використовується декілька серверів віддаленого доступу. У цих системах адміністратор може керувати БД ідентифікаторів і паролів користувачів, надавати їм привілеї доступу і вести облік звернень до системних ресурсів.

Протоколи TACACS і RADIUS вимагають застосування окремого сервера автентифікації, який для перевірки достовірності користувачів і визначення їх повноважень може використовувати не лише власну БД, але і взаємодіяти з сучасними службами каталогів, наприклад з NDS (Novell Directory Services) і Microsoft Active Directory. Сервери TACACS і RADIUS виступають посередниками між серверами віддаленого доступу, що отримали дзвінки від користувачів, з одного боку, і мережевими ресурсними серверами – з іншого.

Реалізації TACACS і RADIUS можуть також служити посередниками для зовнішніх систем автентифікації.

Розглянемо особливості централізованого контролю віддаленого доступу на прикладі протоколу TACACS (рис. 4.14).

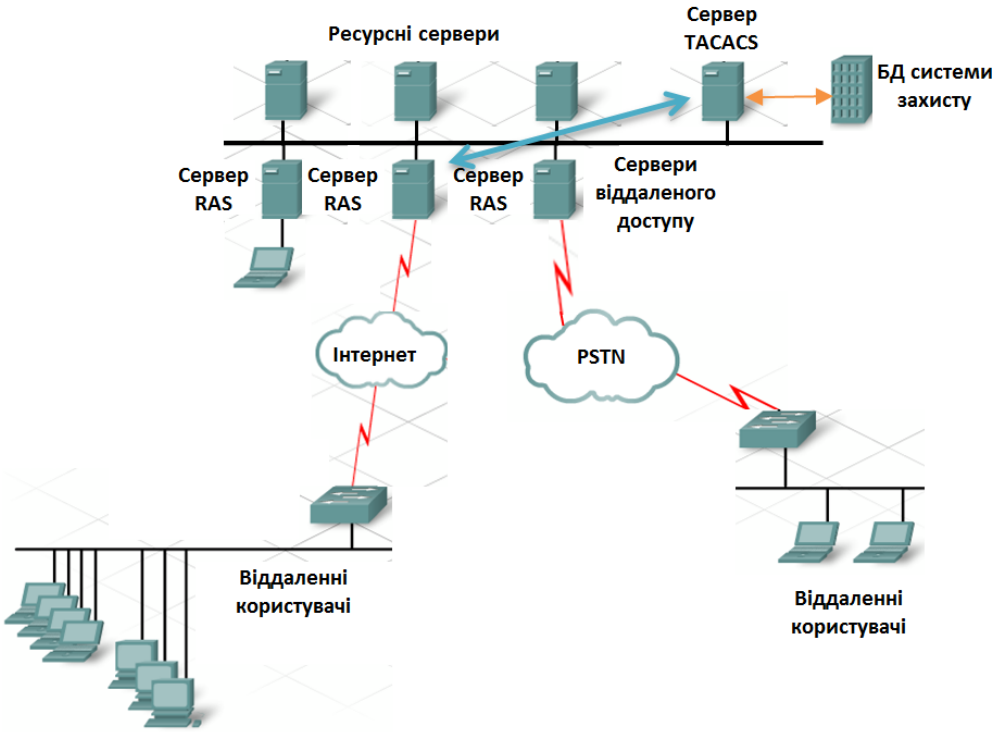


Рис. 4.14. Схема централізованого контролю віддаленого доступу з використанням протоколу TACACS

Система TACACS виконана в архітектурі «клієнт-сервер». У мережі, що містить декілька серверів віддаленого доступу, встановлюється один сервер автентифікації, який називають сервером TACACS (це програма, що працює в середовищі універсальної ОС, частіше усього UNIX).

На сервері TACACS формується центральна база облікової інформації про віддалених користувачів, що включає їх імена, паролі і повноваження. У повноваженнях кожного користувача задаються підмережі, комп'ютери і сервіси, з якими він може працювати, а також різні види обмежень, наприклад часові обмеження. На цьому сервері ведеться БД аудиту, в якій накопичується реєстраційна інформація про кожен логічний вхід, тривалість сесії, а також час використання ресурсів мережі.

Клієнтами сервера TACACS є сервери віддаленого доступу, які приймають запити на доступ до ресурсів мережі від віддалених користувачів. У кожного такого сервера вбудоване ПЗ, що реалізовує стандартний протокол, по якому

вони взаємодіють з сервером TACACS. Цей протокол також називається TACACS.

Протокол TACACS стандартизує схему взаємодії серверів віддаленого доступу з сервером TACACS на основі завдання можливих типів запитів, відповідей і з'єднань. Визначені запити, з якими клієнти можуть звертатися до сервера TACACS. Сервер на кожен запит повинен відповісти відповідним повідомленням. Протокол задає декілька типів з'єднань, кожне з яких визначається як послідовність пар запит-відповідь, орієнтована на вирішення окремої задачі.

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.

За допомогою з'єднання **AUTH** сервери віддаленого доступу перенаправляють серверу TACACS потік запитів на логічне підключення користувачів до мережі в цілому.

З'єднання **LOGIN** служить для перенаправлення запитів серверу TACACS на логічне підключення користувачів до окремих комп'ютерів локальної мережі.

При з'єднанні **AUTH** сервер віддаленого доступу посилає на сервер TACACS тільки одне повідомлення – пакет AUTH, на який сервер TACACS відповідає повідомленням REPLY.

Сервер TACACS на підставі наявних у нього даних перевіряє пароль і повертає відповідь у вигляді пакету REPLY, де повідомляє про успіх або неуспіх автентифікації. Відповідно до протоколу TACACS пароль передається між сервером віддаленого доступу і сервером автентифікації у відкритому виді. Тому протокол TACACS необхідно застосовувати спільно з протоколом автентифікації по одноразових паролях, наприклад з протоколом S/Key.

На підставі отриманих від сервера TACACS вказівок сервер віддаленого доступу виконує процедуру автентифікації і дозволяє або не дозволяє віддаленому користувачу логічно увійти в мережу.

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.

Слід зазначити, що недоліки протоколу TACACS, пов'язані з відкритою передачею пароля по мережі, усунені компанією Cisco у версії **TACACS+**. Відповідно до протоколу TACACS+ пароль для передачі по мережі шифрується за допомогою алгоритму MD5. TACACS+ передбачає роздільне зберігання БД автентифікаційної, авторизаційної і облікової інформації, у тому числі і на різних серверах. Поліпшена взаємодія з системою Kerberos.

Іншою поширеною системою централізованої автентифікації при віддаленому доступі є система RADIUS. По своїх функціональних можливостях протоколи TACACS і RADIUS практично еквівалентні і є відкритими стандартами, проте протокол RADIUS став популярніший. Це пов'язано з тим, що серверне ПЗ поширюється безкоштовно. Крім того, протокол RADIUS менш складний в реалізації.

RADIUS

Повний опис цього протоколу міститься в RFC-2138 і RFC-2139. Цей протокол був розроблений незалежною групою розробників (на даний момент протокол не модифікується) і тому набув широкого поширення у сторонніх розробників. Як правило, усі виробники програмних і апаратних клієнтів підтримують цей протокол. Коротко про протокол можна сказати наступне: 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+

Цей протокол є розробкою фірми Cisco Systems і його реалізація періодично модифікується. Цей протокол є новим витком розвитку більш ранніх версій протоколів TACACS і XTACACS: хоч в офіційних випусках і говориться, що всього лише підвищена безпека протоколу, але реально увесь протокол технічно був переписаний наново, тому не слід плутати між собою ці протоколи (старіший протокол TACACS практично ніхто зараз не використовує, тому якщо буде посилання на протокол TACACS, швидше за все мове йде про TACACS+). Протокол 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).

В таблиці 4.4 приведено порівняльні характеристики обох протоколів.

Таблиця 4.4. Порівняння характеристик протоколів RADIUS і TACACS+

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	+	-

5. Технології безпеки на основі фільтрування і моніторингу трафіка

5.1. Використання списків контролю доступу

5.1.1. Фільтрування трафіку

Під фільтрацією трафіку розуміється обробка IP-пакетів маршрутизаторами і фаєрволами, яка веде до відкидання деяких пакетів або зміни їх маршруту. Фільтрація трафіку дозволяє або запобігти атаці на мережу, заздалегідь блокуючи доступ до неї для деяких зовнішніх мереж і хостів, або, якщо джерело атаки не було попередньо заблоковане, зупинити її.

Фільтрація трафіку дозволяє адміністратору контролювати трафік в різних сегментах мережі. Фільтрація являє собою процес аналізу вмісту пакету з метою дозволу або блокування його передачі.

Фільтрація пакетів може бути простою і складною і може забороняти або дозволяти трафік за наступними критеріями (рис. 5.1):

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

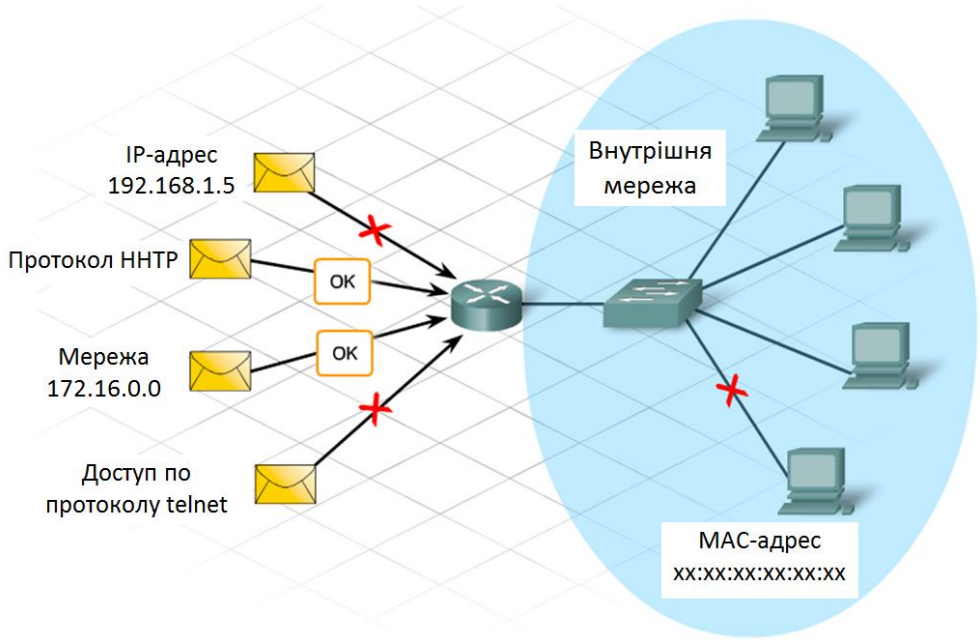


Рис. 5.1. Критерії фільтрування пакетів

Фільтрація пакетів дозволяє підвищити продуктивність мережі. Завдяки відхиленню небажаного або забороненого трафіку близько до його відправника, трафік не передається по мережі і не споживає цінні ресурси.

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

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

Деякі пристрої фільтрують лише трафік, що виникає у внутрішній мережі. Більш досконалі пристрої безпеки здатні розпізнавати і фільтрувати відомі типи атак із зовнішніх джерел.

5.1.2 Типи і використання списків контролю доступу

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. Шляхом правильного підбору списків доступу адміністратор мережі може розробити практично будь-яку потрібну йому стратегію безпеки.

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.

Списки контролю доступу являють собою фільтри для порівняння, класифікації й обробки пакетів. Їх можна застосовувати для контролю потоку вхідних або вихідних пакетів для будь-якого інтерфейсу маршрутизатора.

ACL-списки являють собою набір інструкцій, які застосовуються до одного або декількох інтерфейсів маршрутизатора і виконують фільтрування вхідних і вихідних потоків даних, в залежності від конфігурування (рис. 5.2). Списки для вихідного трафіку зазвичай більш ефективні, тому вони мають перевагу в порівнянні із списками для вхідного трафіку. Маршрутизатор, в якому сконфігурований ACL-список для вхідного трафіку, повинен перевіряти кожний пакет на його відповідність умовам списку перед тим, як відправити пакет на вихідний інтерфейс.

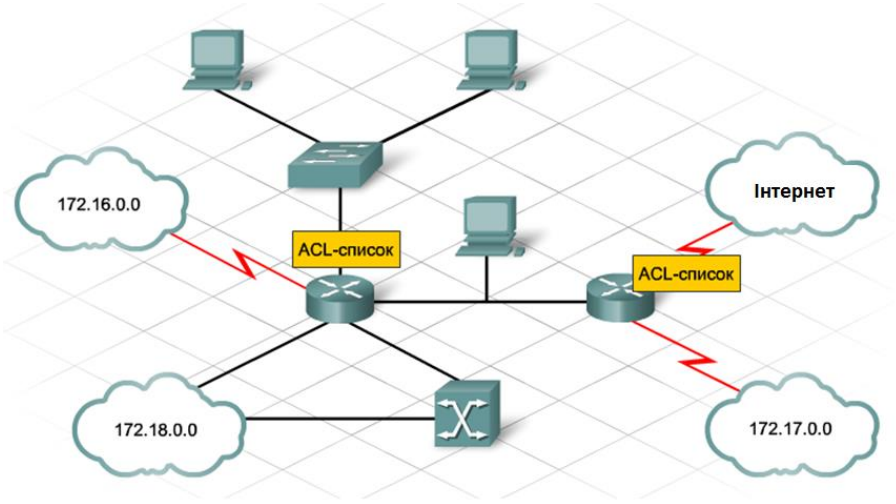


Рис. 5.2. Приклад використання ACL-списків

Застосування ACL-списків виражається в тім, що маршрутизатор аналізує кожен пакет, що проходить через даний інтерфейс у зазначеному напрямку, і виконує відповідні дії. 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.

ACL-список, що застосовується як вихідний до інтерфейсу, не діє для вхідного трафіку по тому ж інтерфейсу. Для кожного інтерфейсу маршрутизатор може мати один вхідний ACL-список і один вихідний ACL-список одночасно.

Адміністратору доступно кілька варіантів створення списків контролю доступу. Складність вимог до структури визначає тип необхідного ACL-списку. Існує три типи ACL-списків.

1. Стандартні ACL-списки
2. Розширені ACL-списки
3. Іменовані ACL-списки

Стандартний ACL-список є найпростішим з трьох типів. При створенні стандартного ACL-списку для IP-протоколу, фільтрація здійснюється на основі вихідної IP-адреси пакета. Такий тип ACL-списку корисний для дозволу доступу всіх служб певного користувача або локальної мережі (LAN) через маршрутизатор з забороною доступу з інших IP-адрес. Стандартним ACL-спискам присвоюються номери з діапазону від 1 до 99 і від 1300 до 1999.

Розширений ACL-список використовується для фільтрації не тільки по вихідній IP-адресі, але і за кінцевою IP-адресою, протоколом і номерами портів. Розширені ACL-списки використовуються частіше стандартних, оскільки вони забезпечують більш високий рівень контролю. Розширеним ACL-спискам присвоюються номери з діапазону від 100 до 199 і від 2000 до 2699.

Іменований ACL-список (NACL-список) має формат стандартного чи розширеного списку і позначається описовим іменем, а не номером. При налаштуванні іменованих ACL-списків, маршрутизатор IOS використовує режим підкоманди NACL.

Адміністратор може використовувати вхідний чи ACL-список для інтерфейсу маршрутизатора. Вхідної чи вихідної напрям завжди розглядається з точки зору маршрутизатора. Трафік, що поступає через інтерфейс, є вхідним, а відправляється через інтерфейс - виходить.

Налаштування ACL-списків складається з двох етапів:

1. Створення списку доступу.
2. Зв’язування списку доступу з інтерфейсом.

5.1.3. Використання шаблонних масок

У простих ACL-списках вказується тільки один дозволений або заборонений адрес. Для блокування кількох адрес або їх діапазонів необхідно кілька інструкцій або **шаблонна маска** (Wildcard Mask). Використання IP-адреси мережі з шаблонною маскою забезпечує більшу гнучкість. За допомогою шаблонної маски можна блокувати діапазон адрес або всю мережу всього однієї інструкцією.

Шаблонна маска являє собою 32-розрядний двійковий код, розбитий на 4 октети, який записується в десятковому форматі.

Одиниці в цій масці означають, що відповідні позиції адреси можуть містити будь-які значення (не перевіряються), а нулі вказують на конкретні значення (перевіряються).

Наприклад, запис 219.17.100.2 0.0.0.0 вказує на конкретний хост з IP-адресою 219.17.100.2, а запис 219.17.100.2 0.0.0.255 – вказує на всі хости, які належать мережі 219.17.100.0, оскільки в четвертому октеті вихідного адресу можуть знаходитись будь-які значення.

Для того, щоб вказати на усі хости, що належать підмережі 192.168.77.32/27 (255.255.255.224), необхідно використати наступну маску 0.0.0.31, згідно якої будуть перевірятись лише останні 5 біт IP-адреси.

Крім того існують спеціальні ключові слова **host** і **any,** які являють собою назви масок спеціального виду.

Запис **host 219.17.100.2** означає те ж саме, що і запис **219.17.100.2 0.0.0.0.** Таким чином, замість маски **0.0.0.0** можна використовувати ключове слово **host**.

Ключове слово **any** еквівалентно масці **0.0.0.0 255.255.255.255**. Маска, що складається з одних одиниць, тобто 255.255.255.255, означає, що жоден біт адреси не повинен аналізуватися.

5.1.4. Стандартні списки контролю доступу

Стандартні списки доступу дозволяють аналізувати вихідні IP-адреси пакетів TCP/IP і відкидати або пропускати їх на підставі результатів аналізу. Для створення стандартного ACL-списку необхідно увійти в режим глобальної конфігурації та за допомогою команди **access-list** ввести інструкції списку контролю доступу. Необхідно ввести всі інструкції з однаковим номером ACL-списку, поки список контролю доступу не буде готовий.

Синтаксис стандартного ACL-списку наступний:

access-list *номер списку доступу* {**permit | deny**} *[вихідна адреса] [шаблонна маска]*

Ключове слово **permit** чи **deny** вказує, чи варто дозволити (permit) проходження пакета, що задовольняє шаблону, або заборонити (deny) його; параметр ***вихідна адреса*** застосовується для визначення вихідної IP-адреси пакетів, що потребують обробки.

Оскільки кожен пакет порівнюється з інструкцією списку контролю доступу до знаходження збігу, то порядок розміщення інструкцій в ACL-списку може впливати на створюванні затримки. Тому слід розташовувати інструкції таким чином, щоб більш часто використовувані умови в ACL-списку передували менш частим. При цьому слід пам'ятати, що при збігу пакет більше не порівнюється з іншими інструкціями в ACL-списку. Це означає, що якщо один рядок дозволяє пакет, а наступний рядок в ACL-списку забороняє його, то пакет буде дозволений. З цієї причини слід планувати ACL-список таким чином, щоб інструкції з більш визначеними вимогами розташовувалися перед інструкціями з більш загальними вимогами. Іншими словами, слід забороняти доступ певного вузла в мережі, дозволяючи доступ іншим у всій мережі.

Для опису функції кожного розділу чи інструкції ACL-списку використовується команда **remark**:

access-list *номер списку доступу* **remark** *[текст]*

Для видалення ACL-списку використовується наступна команда:

no access-list *номер списку*

З стандартного чи розширеного ACL-списку не можна видалити один рядок. Замість цього ACL-список видаляється повністю і його необхідно замінити.

На рис. 5.3 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.

```
R2# conf t
R2(config)#access-list 3 deny host 192.168.4.12
R2(config)#access-list 3 permit 192.168.4.0 0.0.0.255
R2(config)#access-list 3 permit 192.168.1.66 0.0.0.0
```

Фільтрація по ACL-списку неможлива до його призначення інтерфейсу.

ACL-список необхідно застосовувати якомога ближче до адреси

призначення.

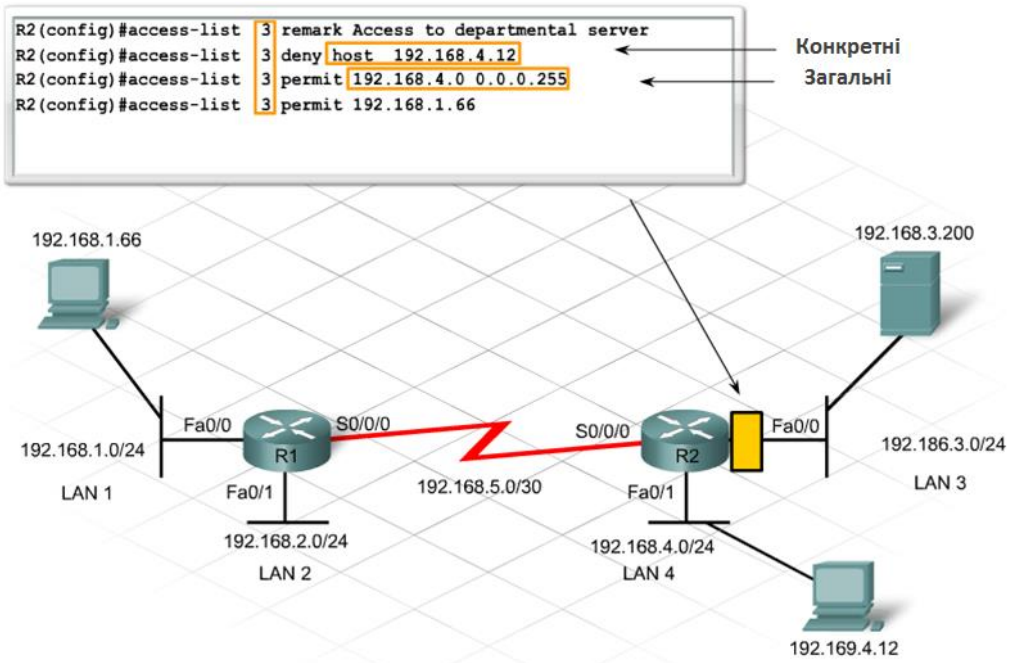


Рис. 5.3 Приклад використання стандартного ACL-списку

Для зв’язування списку контролю доступу з інтерфейсом необхідно перейти в режим конфігурування цього інтерфейсу та ввести команду:

ip access-group *номер списку доступу* [**in | out**]

Параметр **out** вказує, що список повинен використовуватися для фільтрації вихідних пакетів, а параметр **in** – для вхідних пакетів. Для маршрутизатора вихідними (out) будуть пакети, що передаються його інтерфейсом у мережу, а вхідними (in) — пакети, що надходять з мережі на його інтерфейс.

Наступні команди дозволяють помістити список контролю доступу access-list 3 для інтерфейсу FastEthernet0/0 маршрутизатора R2 з фільтрацією вхідного трафіку (рис. 5.4):

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 3 out
```

По замовчуванню, в ACL-списку до інтерфейсу застосовується out напрямок.

Щоб від’єднання ACL-списку від інтерфейсу без зміни самого ACL-списку, використовується команда

no ip access-group *номер списку доступу*.

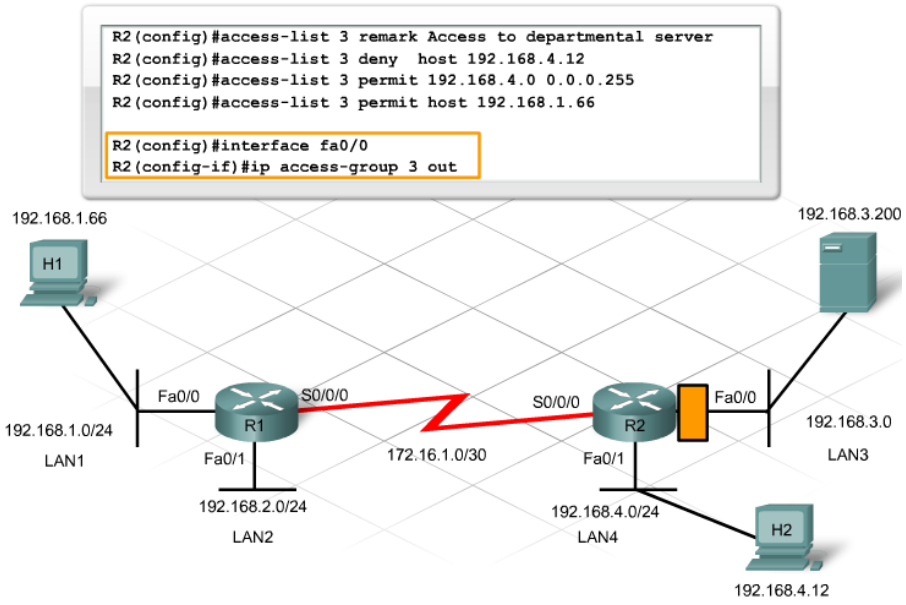


Рис. 5.4 Приклад зв'язування стандартного ACL-списку

5.1.5. 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.)

Отже, розширені ACL-списки мають більший набір можливостей, що дозволяє створювати більш докладні списки контролю доступу. Формат рядків розширеного списку доступу:

access-list *номер ACL-списку* {**permit | deny**} *[протокол] [вихідна адреса] [шаблонна маска] [адреса призначення] [шаблонна маска] [умова відповідності порта][порт]*

Перед полем вихідної адреси можна вказати протокол 3 або 4 рівня OSI моделі (IP, TCP, UDP, ICMP та інші), а після вихідної адреси – адресу призначення і порт. Усі ці поля є необов'язковими.

Приклад (рис. 5.5), у компанії є сервер з адресою 192.168.3.75.

До нього встановлені такі вимоги:

- дозволяти доступ до вузлів у локальній мережі 192.168.2.0;
- дозволяти доступ до вузла 192.168.1.66;
- блокувати доступ до вузлів у локальній мережі 192.168.4.0;
- дозволяти доступ до решти адресами в компанії.

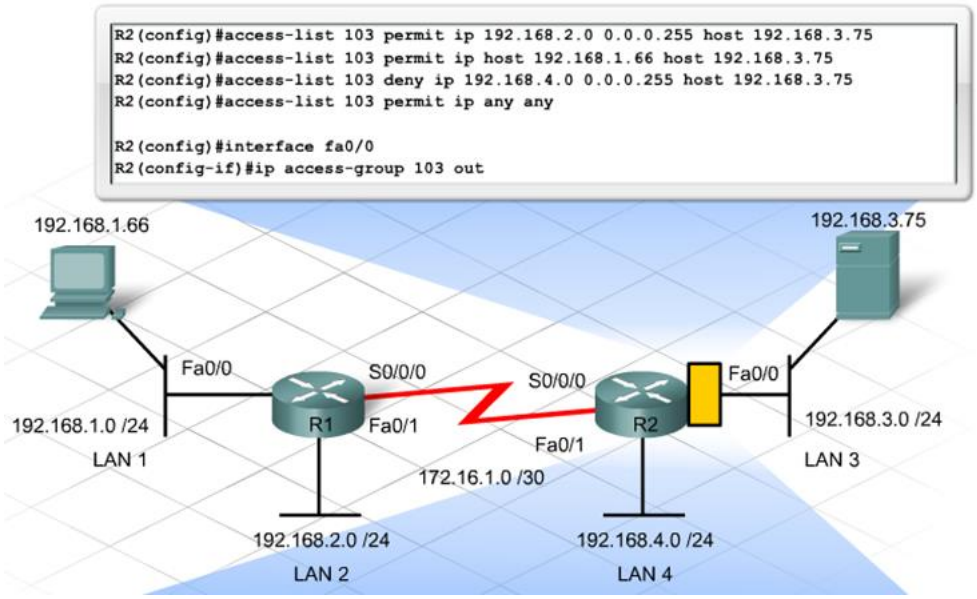


Рис. 5.5 Приклад використання розширеного ACL-списку

R2# conf t
R2(config)#access-list 103 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.75
R2(config)#access-list 103 permit ip host 192.168.1.66 host 192.168.3.75
R2(config)#access-list 103 deny ip 192.168.4.0 0.0.0.255 host 192.168.3.75
R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 103 out

Якщо в команді створення розширеного списку контролю доступу не вказати порт, то всі порти будуть доступні. Для задання порту можна використовувати *умову відповідності порту* за допомогою одного із наступних операторів:

eq – пакети з даним портом;

gt – лише пакети з більшим номером порта;

lt – лише пакети з меншим номером порта;

neq – лише пакети з іншим портом

range – лише пакети з номерами портів у зазначеному діапазоні.

Порти можна задавати за допомогою номерів або ключових слів (табл. 5.1).

Таблиця 5.1. Найбільш використовувані порти.

Ключове слово	**Номер порта**	**Опис**
domain	53	Domain Name Service
ftp	21	File Transfer Protocol
ftp-data	20	FTP data connections
pop3	110	Post Office Protocol v3
smtp	25	Simple Mail Transport Protocol
telnet	23	Telnet
http	80	World Wide Web
rip	520	Routing Information Protocol
snmp	161	Simple Network Management Protocol
tftp	69	Trivial File Transfer Protocol

Розглянемо наступний приклад:

R1(config)#access-list 122 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.89 eq 80

Ця інструкція ACL-списку дозволяє трафік з мережі 192.168.1.0 до Web-сервера 192.168.2.89 по порту 80. Якщо користувач спробує підключитися через Telnet або по FTP до вузла 192.168.2.89, то йому буде відмовлено в доступі.

5.1.6. Іменовані списки контролю доступу

Програмне забезпечення Cisco IOS версії 11.2 і вище дозволяє створювати іменовані ACL-списки (NACL-списки). У NACL-списку описову назву замінює числові діапазони, необхідні для стандартних та розширених ACL-списків. Іменовані ACL-списки володіють можливостями та перевагами стандартних та розширених ACL-списків, при їх створенні відрізняється тільки синтаксис.

Ім’я ACL-списку є унікальним. Для створення іменованого ACL-списку використовується наступна команда:

ip access-list {standard | extended} *ім’я*

Після виконання цієї команди маршрутизатор перемикається в режим підкоманд конфігурації NACL. Після задання початкової команди іменування необхідно ввести всі дозволяючи та забороняючі інструкції, по одній за раз. У

NACL-списках використовується синтаксис команд стандартного чи розширеного ACL-списку з дозволяючою (**permit**) або забороняючою (**deny**) інструкцією на початку. Наприклад:

```
R1(config)# ip access-list extended cisco
R1(config-ext-nacl)#permit ip 192.168.1.66 0.0.0.0 any
R1(config-ext-nacl)#permit ip 192.168.1.77 0.0.0.0 any
```

Іменований ACL-список прив'язується до інтерфейсу аналогічно як і стандартний чи розширений ACL-списки.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group cisco out
```

5.1.7. 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.

Стандартні ACL-списки легко створювати і впроваджувати. Однак фільтрація за стандартними ACL-списками можлива тільки на основі вихідної адреси і застосовується до всього трафіку без урахування його типу або призначення. Занадто близьке розміщення стандартного ACL-списку до джерела може ненавмисно блокувати допустимий трафік. Отже, важливо розміщувати стандартні ACL-списки якомога ближче до вузла призначення.

У випадку більш складних вимог до фільтрації слід використовувати розширений ACL-список. Розширені ACL-списки дають більший контроль, ніж стандартні. Вони допускають фільтрацію по вихідним і кінцевим адресами. Ці списки також забезпечують фільтрацію по протоколу мережевого рівня, протоколу транспортного рівня і номерах портів, якщо це необхідно.

Слід розміщувати розширений ACL-список ближче до вихідної адреси. Завдяки аналізу по вихідній і кінцевій адресі, ACL-список дозволяє блокувати пакети, що направляються у визначену кінцеву мережу перш, ніж вони покинуть вихідний маршрутизатор. Таким чином, можна підтримувати пропускну здатність.

Розглянемо приклад (рис. 5.6, 5.7). Вимоги: Необхідно заборонити трафік з мережі 192.168.1.0 в мережу 192.168.4.0. Дозволити трафіку з мережі 192.168.1.0 досягнення інших мереж.

На рис. 5.6 показана реалізація даного завдання, використовуючи стандартний ACL-список.

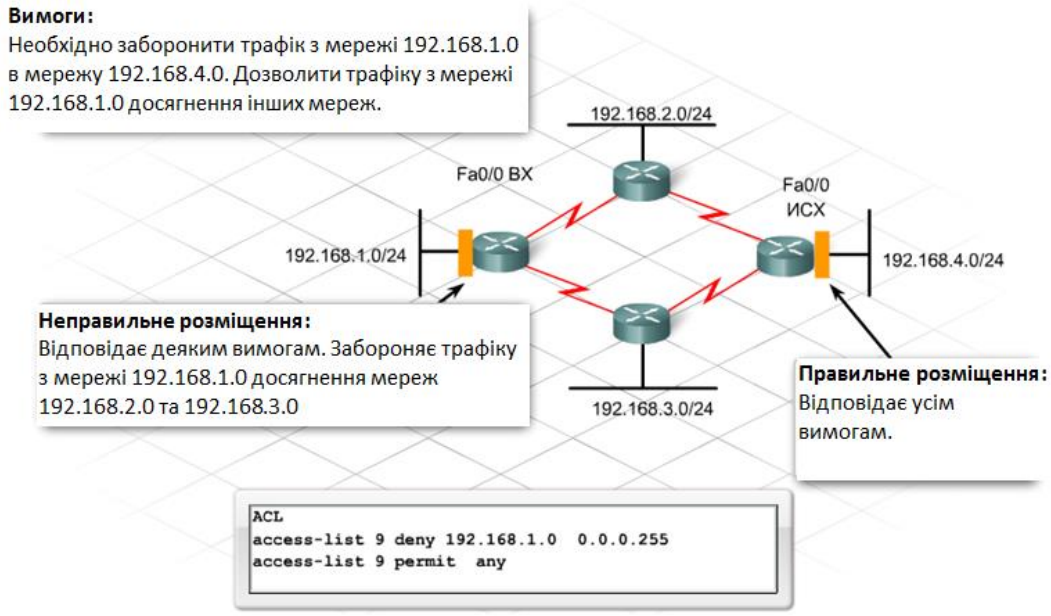


Рис. 5.6. Приклад реалізації завдання за допомогою стандартного ACL-списку

На рис. 5.7 показана реалізація даного завдання, використовуючи розширений ACL-список.

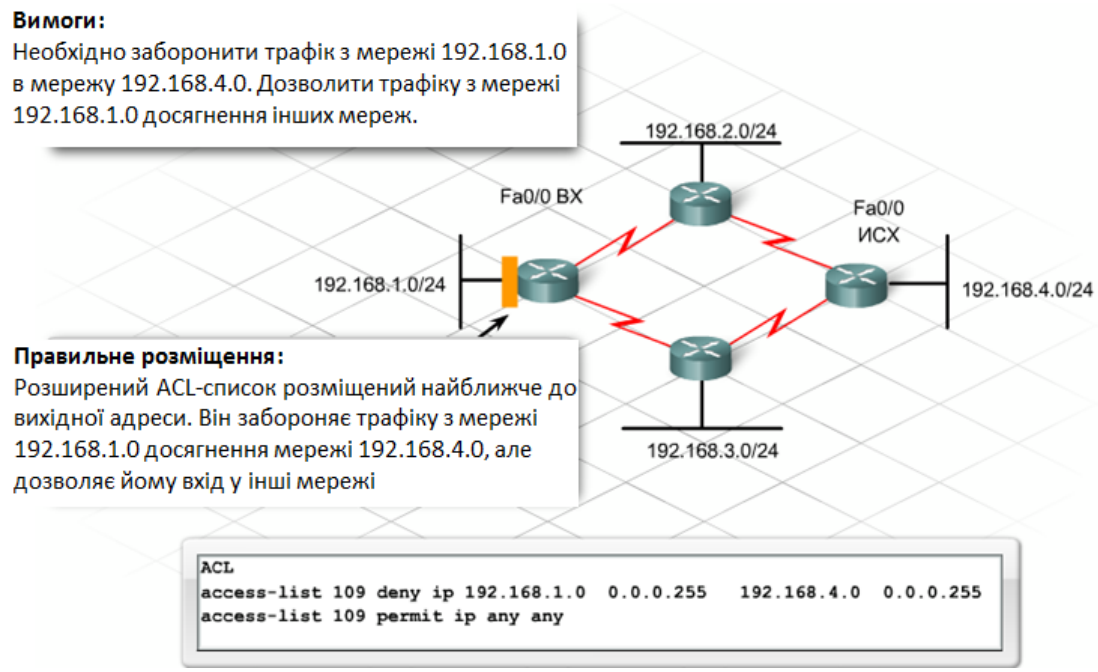


Рис. 5.7. Приклад реалізації завдання за допомогою розширеного ACL-списку

5.1.8. Перевірка списків контролю доступу

Деякі команди дозволяють оцінити правильність синтаксису, порядок інструкцій і розміщення в інтерфейсах ACL-списків.

show ip interface

Ця команда виводить відомості про IP-інтерфейс із зазначенням будь-яких привласнених ACL-списків.

```
R2#show ip interface fa0/0
FastEthernet0/0 is up, line protocol is up
 (**выходные данные опущены**)
  Internet address is 192.168.3.1 /24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Outgoing access list is 3
  Inbound  access list is not set
```

show access-lists *[номер списку доступу]*

Ця команда дозволяє вивести вміст всіх ACL-списків маршрутизатора. Вона також виводить на екран число збігів по кожній дозволяючій або забороняючій інструкції з моменту застосування ACL-списку. Щоб вивести певний список, потрібно вказати його ім’я або номер.

```
R2#show access-lists
Standard IP access list 3
 10 permit 192.168.1.66
 20 deny   192.168.1.0, wildcard bits 0.0.0.255 (8 matches)
 30 permit 192.168.2.0, wildcard bits 0.0.0.255 (12 matches)
 40 deny   192.168.4.0, wildcard bits 0.0.0.255 (6 matches)
```

show running-config

Ця команда виводить на екран всі налаштовані ACL-списки маршрутизатора, навіть якщо вони в даний момент не застосовані до інтерфейсу.

При використанні нумерованих ACL-списків інструкції, що вводяться після створення ACL-списку, додаються в кінець. Такий порядок може не дати очікуваних результатів. Щоб вирішити цю проблему, видаліть вихідний ACL-список і створіть його заново.

```
R2#show running-config
Building configuration...

Current configuration : 1935 bytes
!version 12.4
!
hostname R2
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 ip access-group 3 out
 duplex auto
 speed auto
 !
access-list 3 remark This is a standard ACL
access-list 3 permit 192.168.1.66
access-list 3 deny   192.168.1.0 0.0.0.255
access-list 3 permit 192.168.2.0 0.0.0.255
access-list 3 deny 192.168.4.0 0.0.0.255
```

Часто рекомендують створювати ACL-списки в текстовому редакторі. Це дозволить легко змінювати і вставляти ACL-перелік в конфігурацію маршрутизатора. Проте слід пам’ятати, що при копіюванні та вставці ACL-списку важливо спочатку видалити поточний ACL-список, в іншому випадку всі інструкції будуть додані в кінець.

5.2. Фаєрволи

5.2.1.Функціональне призначення фаєрволів

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.

Вихідним значенням терміну «фаєрвол» (від англ. Firewall) є елемент конструкції будинку, а саме стіна, зроблена з вогнетривкого матеріалу, що перешкоджає поширенню вогню між частинами будинку. Термін «брандмауер» (від нім. Brandmauer) багато років тому прийшов в українську мову з німецької. Спочатку він позначав перегородку в поїзді, що відокремлює область топки паровоза від пасажирського відділення.

Для того, щоб фільтрувати трафік, фаєрвол повинен мати принаймні два мережевих інтерфейси: з внутрішньою мережею і з зовнішньою мережею (рис 5.8.). Фаєрвол захищає внутрішню мережу (наприклад, локальну мережу підприємства) від загроз, що виходять із зовнішньої мережі (як правило, Інтернет). Фаєрвол може також захищати одну внутрішню мережу підприємства від іншої, якщо відповідно до принципу мінімуму повноважень користувачам цих мереж не потрібен повний взаємний доступ до ресурсів один одного.

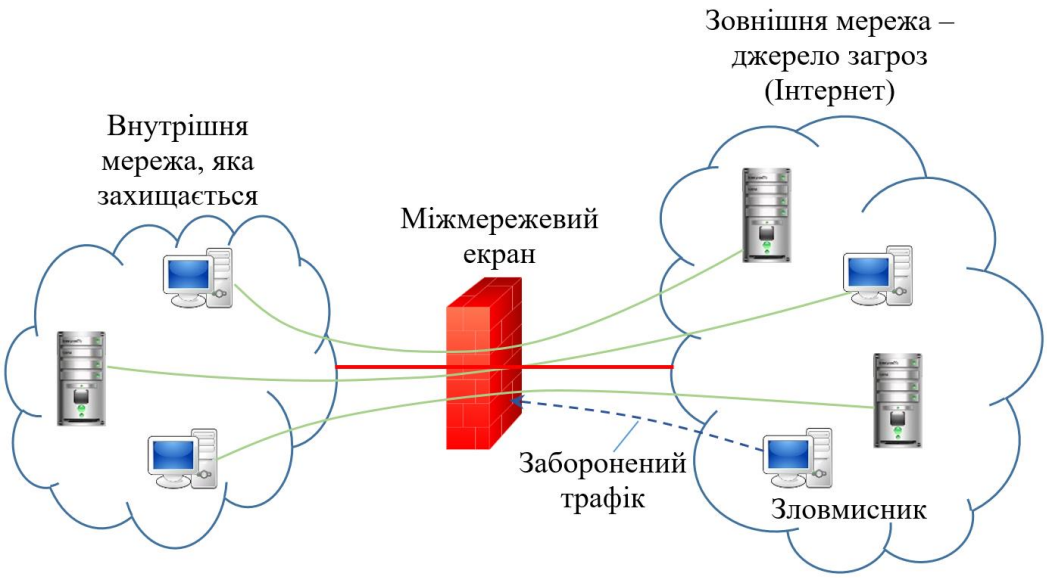


Рис. 5.8. Використання фаєрвола для захисту внутрішньої мережі від зовнішніх загроз

Для ефективного виконання фаєрволом його головної функції – аналізу і фільтрації трафіку – необхідно, щоб через нього проходив весь трафік, яким обмінюються вузли внутрішньої мережі з вузлами Інтернету. У тому випадку, коли мережа пов’язана з зовнішніми мережами декількома лініями зв’язку, кожна лінія зв’язку повинна бути захищена фаєрволом.

Фаєрвол захищає мережу не тільки від несанкціонованого доступу і атак зовнішніх зловмисників, а й від помилкових дій користувачів внутрішньої мережі, наприклад передача в зовнішню мережу конфіденційної інформації.

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).

Більшість з перерахованих функцій часто реалізуються у вигляді окремих продуктів або в складі систем захисту інших типів. Так, функції пакетної фільтрації вбудовані практично в усі маршрутизатори, завдання виявлення вірусів вирішується безліччю різноманітних програм, шифрування трафіку – невід'ємний елемент технологій захищених каналів і т. д. Проксі-сервери часто поставляються у вигляді додатків, вони самі іноді інтегрують в собі багато функцій, що властиві мережевим екранам, такі, наприклад, як фільтрація по вмісту (контенту) або трансляція мережевих адрес.

5.2.2. Типи фаєрволів

Фаєрволи можна класифікувати за різними критеріями, однак найбільш важливими технічними характеристиками фаєрволів є: способі реалізації, способі фільтрації і рівні моделі OSI.

В якості апаратної складової мережевого екрану може виступати маршрутизатор або комбінація маршрутизаторів, комп'ютер або комбінація комп'ютерів, комбінація маршрутизаторів і комп'ютерів, нарешті, це може бути спеціалізований пристрій. Такою ж різноманітністю відрізняється і програмна складова мережевого екрану, що має гнучку структуру і включає в себе різні модулі, функції яких можуть широко змінюватись.

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

(найчастіше в якості такої спеціалізованої платформи використовується універсальна ОС з набором специфічних налаштувань, що забезпечують максимальний рівень безпеки, а також сервер, що сертифікований для роботи з програмним забезпеченням 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.

Фаєрволи з запам'ятовуванням стану для кожного сеансу, який задовольняє деяким умовам, створюють динамічну структуру даних в спеціальній таблиці станів фаєрвола. Після приходу чергового пакету контрольованого сеансу стан сеансу коригується і приймається рішення про виконання заданої дії з пакетом – пропускати або відкидати. Відстеження для протоколів стану сеансів вимагає великих обсягів ресурсів, саме тому фаєрволи із запам'ятовуванням стану створюються на програмно-апаратних платформах, які мають велику оперативну пам'ять для зберігання таблиці стану сеансів і швидкодіючі процесори для обробки пакетів в реальному часі. Якщо ж ресурсів такого фаєрвола виявляється недостатньо, то він замість користі може принести шкоду, коли внутрішні сервери виявляються недоступними не через атак на них, а через затори трафіку на інтерфейсах фаєрвола.

Однією з найбільш важливих характеристик фаєрвола є рівень протоколу моделі OSI, на якому він працює. По цій ознаці розрізняють фаєрволи канального, мережевого, сеансового і прикладного рівнів. Якщо ж фаєрвол аналізує і фільтрує трафік на декількох рівнях, то його відносять до самого вищого із всіх цих рівнів.

Рівень протоколу, на якому працює фаєрвол, часто використовують в якості інтегральної характеристики, оскільки з нею корелюють інші ознаки брандмауера. Наприклад, фаєрволи, що працюють на сеансовому і прикладному рівнях, частіше відносяться до фаєрволів із запам'ятовуванням стану, а більш прості фаєрволи мережевого рівня – без запам'ятовування.

До **фаєрволів канального рівня** можуть бути умовно віднесені керовані комутатори, які володіють розширеним набором функцій, в тому числі можливістю фільтрації кадрів канального рівня на основі створених адміністратором списків контролю доступу.

Фаєрволи мережевого рівня, звані також **фаєрволами з фільтрацією пакетів** (Packet Filtering Firewall), в повній відповідності зі своєю назвою

вирішують задачу фільтрації пакетів по IP-адресах (як відправника, так і отримувача), а також за значенням поля протоколу верхнього рівня – в пакет мережевого рівня можуть бути вкладені повідомлення протоколів TCP, UDP, ICMP і ін. Незважаючи на свою назву, такі фаєрволи працюють і на більш високому, транспортному рівні, тобто на рівні портів TCP і UDP, але тільки на основі статичних правил, при яких не відслідковуються стани з'єднань, тобто в режимі без запам'ятовування стану. Тому, за допомогою брандмауера мережевого рівня можна заблокувати доступ до певного додатку, заборонивши проходження пакетів з певними номерами портів TCP або UDP, але не можна захистити мережу від спотвореного сеансу TCP або HTTP, тому що це вимагає відстеження послідовності кроків в сеансі, а значить, і запам'ятовування стану сеансу, чого фаєрволи мережевого рівня робити не вміють.

Цьому типу фаєрволів відповідають маршрутизатори, що підтримують користувацькі фільтри, а також програмні персональні фаєрволи операційних систем. Адміністратор може задати досить витончені правила фільтрації, що стосуються захисту ресурсів внутрішньої мережі, проте цей тип мережевих екранів поступається за ступенем захисту іншим типам. Перевагами фаєрволів мережевого рівня є простота, невисока вартість і мінімальний вплив на продуктивність мережі (тобто їх додаткова робота по фільтрації трафіку не уповільнює маршрутизацію пакетів між двома мережами).

Фаєрволи сеансового рівня відстежують стани сеансів протоколів, іншими словами, виконують операцію запам'ятовування стану на рівнях нижче прикладного. Для того щоб контролювати процес встановлення з'єднання, фаєрвол повинен фіксувати для себе поточний стан з'єднання, тобто запам'ятовувати, яке останнє повідомлення відправив клієнт і яке повідомлення він очікує отримати. Перш за все, мається на увазі стан сеансу протоколу TCP, його початкова трикрокова процедура встановлення з'єднання. Фаєрвол перевіряє, наскільки відповідає послідовність обміну повідомленнями контрольованому протоколу. Тобто, наприклад, якщо клієнт надсилає TCP-повідомлення *SYN*, що подає запит TCP-з'єднання, сервер повинен відповідати TCP-повідомленням *ACK SYN*, а не надсилати у відповідь, наприклад, свій TCP-запит *SYN*. Після того, як фаєрвол встановив допустимість TCP-з'єднання, він починає працювати простою передавальною ланкою між клієнтом і сервером. Таким чином, фаєрвол сеансового рівня може захистити мережу від різних типів TCP-атак, в яких порушується логіка встановлення з'єднання.

Підтримка запам'ятовування стану сеансів протоколів дозволяє цьому типу брандмауера захищати мережу не лише від атак на протокол TCP, але і від деяких інших видів атак, які можна розпізнати і зупинити, аналізуючи не окремі пакети, а їх послідовність. Наприклад, атаку Ping flood можна розпізнати по занадто

маленькому інтервалу між ехо-запитами від одного і того ж джерела, для чого встановлюється гранично допустимий мінімальний інтервал між ехо-запитами, а потім фіксується час приходу чергового запиту. Якщо він виявляється менше граничного, то пакет відкидається. Таким чином, запам'ятовування стану сеансів може узагальнюватися і на протоколи, що працюють без встановлення з'єднання (ICMP, UDP, DNS), а це означає, що на відміну від мережевих фаєрволів фаєрволи сеансового типу здатні захистити мережу від деяких видів DoS-атак, навіть якщо вони і не використовують протокол TCP.

Фаєрволи прикладного рівня здатні інтерпретувати, аналізувати і контролювати вміст повідомлень, якими обмінюються програми. Вони також працюють на основі фільтрації із запам'ятовуванням стану, але аналізують стани протоколів не тільки нижніх рівнів аж до транспортного, але і прикладного рівня, таких як протоколи SSH, HTTP, FTP, SQL, SMTP, POP3, IMAP, FTP, SSH, SQL і ін.

Особливим типом фаєрволів цього рівня є проксі-сервер, який перехоплює запити клієнтів до зовнішніх серверів, щоб потім відправити їх від свого імені. Цей тип мережевих екранів забезпечує найвищий рівень захисту, хоча і має свої недоліки, наприклад вимагає великих обчислювальних витрат. Крім того, проксі-сервери можуть приховувати адресу клієнта, що знижує ефективність інших засобів захисту.

Слід відрізняти функції з блокування додатків, реалізовані фаєрволами мережевого рівня, від захисту додатків внутрішньої мережі фаєрволами прикладного рівня. Фаєрвол мережевого рівня розуміє структуру заголовків пакетів TCP і UDP, за рахунок чого може заборонити або дозволити проходження пакетів з певним номером програмного порту TCP або UDP, а так як цей номер привласнений серверній частині деякого додатка, то блокується весь трафік ззовні до цього додатка.

Фаєрвол прикладного рівня діє більш гнучко. Він контролює сеанс деякого додатку і дозволяє або забороняє певні види взаємодії між внутрішньою і зовнішньої частинами цього додатку відповідно до заданих правил. Наприклад, при контролі веб-служби фаєрвол може дозволити використання тільки певних команд протоколу HTTP, а решта заборонити. У список заборонених команд можуть потрапити небезпечні для веб-сервера команди PUT і DELETE. Аналогічно, при контролі поштової служби фаєрвол прикладного рівня може не пропускати назовні листи, які не підписані цифровим підписом відправника, якщо в цьому полягає політика безпеки підприємства.

Фаєрвол прикладного рівня, який використовується в якості корпоративного брандмауера, найчастіше є інтегрованим продуктом з модульною структурою, яка дозволяє йому змінювати набір підтримуваних функцій фільтрації в

залежності від потреб конкретної мережі. 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.

5.3. Проксі-сервери

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.

Роль транзитного вузла дозволяє проксі-серверу логічно розірвати пряме з’єднання між клієнтом і сервером з метою контролю процесу обміну повідомленнями між ними.

Подібно до мережевого екрану, проксі-сервер може ефективно виконувати свої функції тільки за умови, що контрольований ним трафік не піде обхідним

шляхом. Проксі-сервер може бути встановлений не тільки на платформі, де працюють всі інші модулі брандмауера (рис. 5.9, а), але й на будь-якому іншому вузлі внутрішньої мережі або мережі демілітаризованої зони (рис. 5.9, б). В останньому випадку програмне забезпечення клієнта повинно бути налаштоване таким чином, щоб у нього не було можливості встановити пряме з'єднання з ресурсним сервером, минаючи проксі-сервер.

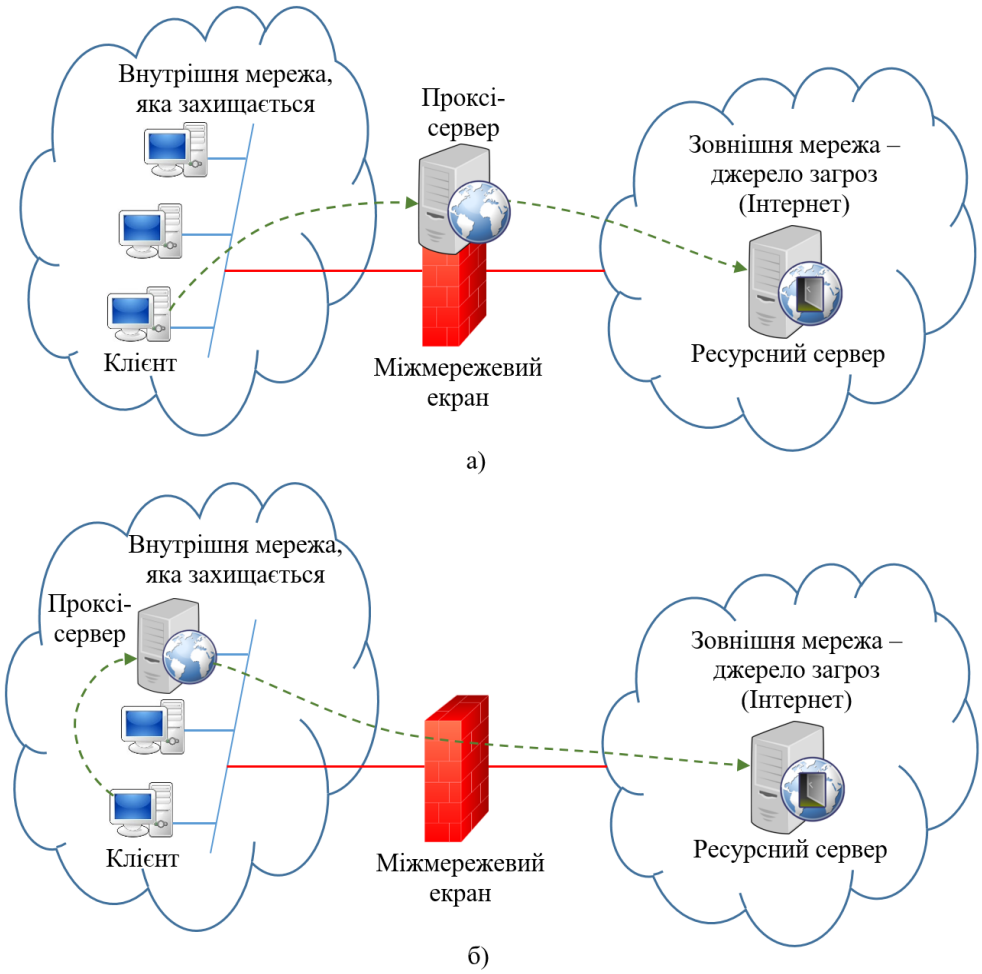


Рис. 5.9. Варіанти розміщення проксі-сервера

Коли клієнтові необхідно отримати ресурс (файл, веб-сторінку, поштове повідомлення) від будь-якого сервера, він посилає свій запит проксі-серверу. Проксі-сервер аналізує цей запит і на підставі заданих йому адміністратором правил вирішує, яким чином цей запит повинен бути оброблений (відкинутий, переданий без зміни ресурсному серверу, модифікований певним способом перед передачею).

В якості правил, якими керується проксі-сервер, можуть виступати умови пакетної фільтрації. Правила можуть бути досить складними: наприклад, в робочі години блокується доступ до певних вузлів і/або додатків, а доступ до

інших вузлів дозволяється тільки певним користувачам, причому для FTP-серверів користувачам дозволяється робити лише завантаження, а вивантаження забороняється. Проксі-сервери можуть також фільтрувати поштові повідомлення по типу файлів, що пересилаються (наприклад, заборонити отримання додатків формату MP3) і по їх контенту. До різних користувачів можуть застосовуватися різні правила фільтрації, тому часто на проксі-сервери покладається завдання автентифікації користувачів.

Якщо після оцінки запиту від програми проксі-сервер констатує, що запит задовольняє умовам проходження далі в зовнішню мережу, то він за дорученням додатку, але від свого імені виконує процедуру з'єднання з сервером, якого потребував даний додаток.

У деяких випадках проксі-сервер може змінювати запит клієнта. Наприклад, якщо в нього вбудована функція трансляції мережевих адрес, він може підміняти в пакеті запиту IP-адреси і/або номери портів TCP і UDP відправника. Таким способом проксі-сервер позбавляє зловмисника можливості сканувати внутрішню мережу для отримання інформації про адреси вузлів і структуру мережі. Єдина доступна зловмисникові адреса в такому випадку – це адреса комп'ютера, на якому виконується програма проксі-сервера. Тому багато атак, що побудовані на знанні зловмисником адрес вузлів внутрішньої мережі, не реалізовуються.

Проксі-сервер, виступаючи посередником між клієнтом і сервером, взаємодіючими за певним протоколом, не може не враховувати специфіку цього протоколу. Так, для кожного з протоколів HTTP, HTTPS, SMTP/POP, FTP, telnet існує особливий проксі-сервер, орієнтований на використання відповідними додатками: веб-браузером, програмою електронної пошти, FTP-клієнтом, клієнтом telnet. Кожен з цих посередників приймає і обробляє пакети тільки того типу додатку, для обслуговування якого він був створений. Зазвичай кілька різних проксі-серверів об'єднують в один програмний продукт.

Розрізняють проксі-сервери прикладного і сеансового рівнів.

Проксі-сервер прикладного рівня вміє «вклинюватись» в процедуру взаємодії клієнта і сервера по одному з прикладних протоколів, наприклад HTTP, HTTPS, SMTP/POP, FTP або telnet. Щоб виступати в ролі посередника на прикладному рівні, проксі-сервер повинен «розуміти» зміст команд, «знати» формати і послідовність повідомлень, якими обмінюються клієнт і сервер відповідної служби. Це дає можливість проксі-серверу проводити аналіз вмісту повідомлень і робити висновки про підозрілий характер того чи іншого сеансу.

Проксі-сервер сеансового рівня виконує свою посередницьку місію на транспортному рівні, контролюючи TCP-з'єднання. Очевидно, що, працюючи на більш низькому рівні, проксі-сервер володіє меншим «інтелектом» і має менше

можливостей для виявлення та попередження атак. Однак, він має одну дуже важливу перевагу перед проксі-сервером прикладного рівня – універсальність, тобто він може бути використаний будь-якими додатками, що працюють по протоколу TCP (а в деяких випадках і UDP).

5.4. Фаєрволи з функцією NAT

Однією з функцій фаєрвола є **трансляція мережевих адрес** (Network Address Translation, **NAT**). В цьому випадку фільтрація трафіку полягає не в пропуску або відкиданні пакетів, а в заміні зовнішньої IP-адреси пакету, яка використовувалась при маршрутизації пакету через Інтернет, на внутрішню, яка необхідна для маршрутизації у внутрішній корпоративній мережі.

Сьогодні існують дві причини звернення до технології NAT: одна з них – дефіцит адрес IPv4, інша – приховування адрес хостів для підвищення безпеки мережі. В обох випадках внутрішня мережа використовує приватні адреси, які замінюються однією або декількома публічними адресами при відправці пакетів в зовнішні мережі. Застосування NAT дозволяє приховати адреси вузлів своєї мережі, щоб не дати можливості зловмисникам скласти уявлення про структуру та масштаби корпоративної мережі, а також про структуру і інтенсивності вихідного і вхідного трафіків.

Технологія NAT стояла біля витоків зародження фаєрволів як окремого класу продуктів. На початку 90-х років, коли дефіцит адрес IPv4 ще мало відчувався, кілька фахівців заснували компанію Network Translation і розробили програмний продукт PIX, який дозволяв транслювати мережеві адреси. Пізніше цю компанію придбала компанія Cisco, а програмний продукт став знаменитим фаєрволом **Cisco PIX Firewall**, який є одним з флагманів засобів захисту цього класу.

5.4.1. 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.

Ідея технології NAT полягає в наступному. Нехай мережу підприємства утворює домен, вузлам якого присвоєні приватні адреси (рис. 5.10). На маршрутизаторі, що з'єднує мережу підприємства з зовнішньою мережею, встановлено програмне забезпечення NAT. Цей NAT-пристрій динамічно відображає набір приватних адрес {IP*} на набір глобальних адрес {IP}, отриманих підприємством від постачальника послуг і привласнених зовнішньому інтерфейсу маршрутизатора підприємства.

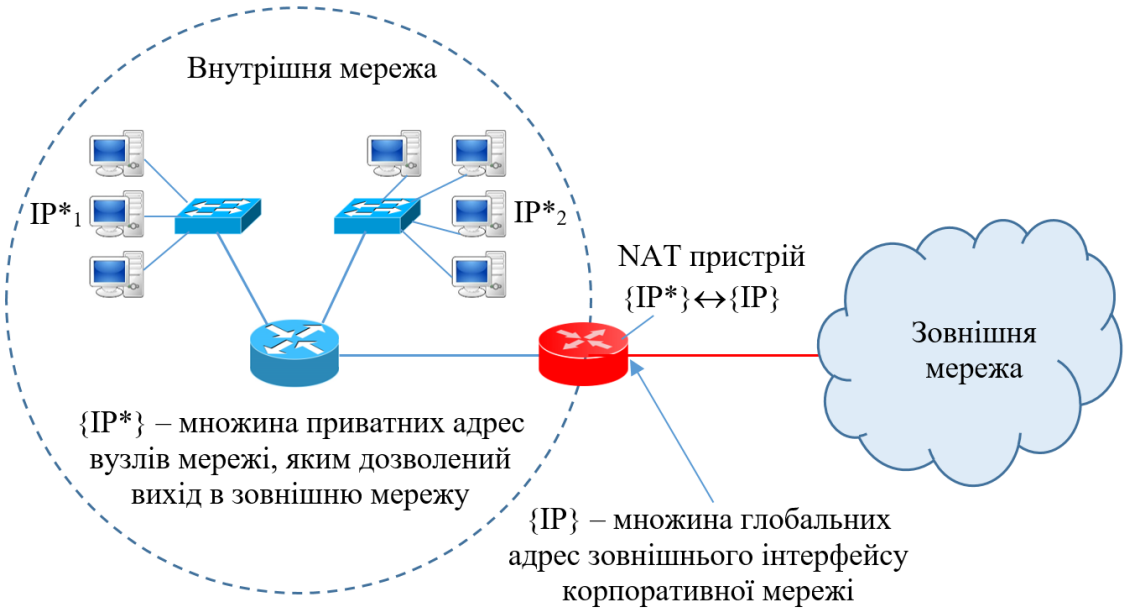


Рис. 5.10. Схема дії традиційної технології NAT

Важливим для роботи NAT-пристрою є правило поширення маршрутних оголошень через кордони приватних мереж. Оголошення протоколів маршрутизації про зовнішні мережі «пропускаються» прикордонними маршрутизаторами у внутрішні мережі і обробляються внутрішніми маршрутизаторами. Маршрутизатори зовнішніх мереж не отримують оголошень про внутрішні мережі, оголошення про них відфільтровуються при передаванні на зовнішні інтерфейси. Тому внутрішні маршрутизатори «знають» маршрути до усіх зовнішніх мереж, а зовнішнім маршрутизаторам нічого не відомо про структуру приватних мереж.

Традиційна технологія NAT поділяється на технології **базової трансляції мережевих адрес** (Basic Network Address Translation, **Basic NAT**) і **трансляції мережевих адрес і портів** (Network Address Translation Port, **NAPT**). В технології Basic NAT для відображення використовуються тільки IP-адреси, а в технології NAPT – ще й так звані транспортні ідентифікатори, в якості яких найчастіше виступають порти TCP і UDP.

5.4.2. Базова трансляція мережевих адрес

Якщо кількість локальних вузлів, яким необхідно забезпечити вихід у зовнішню мережу, менша або рівна наявній кількості глобальних адрес, то для кожної приватної адреси гарантовано однозначне відображення на глобальну адресу. У кожен момент часу кількість внутрішніх вузлів, які отримують можливість взаємодіяти із зовнішньою мережею, обмежується кількістю адрес в глобальному наборі. Зрозуміло, що в такій ситуації метою трансляції є не стільки вирішення проблеми дефіциту адрес, скільки забезпечення безпеки.

Приватні адреси деяких вузлів можуть відображатися на глобальні адреси статично. До таких вузлів можна звертатися ззовні, використовуючи закріплені за ними глобальні адреси Відповідність внутрішніх адрес зовнішнім задається таблицею, яку підтримує маршрутизатор або інший пристрій (фаєрвол), на якому встановлено програмне забезпечення NAT.

У кількох доменах можуть бути однакові приватні адреси. Наприклад, в мережах А і В на рис. 5.11 для внутрішньої адресації застосовується один і той же блок адрес 10.0.1.0/24. У той же час адреси зовнішніх інтерфейсів обох мереж (181.230.25.1/24, 181.230.25.2/24 і 181.230.25.3/24 в мережі А і 185.127.125.2/24, 185.127.125.3/24 і 185.127.125.4/24 в мережі В) унікальні глобально, тобто ніякі інші вузли в зовнішній мережі їх не використовують. В даному прикладі в кожній з мереж тільки три вузла мають можливість «виходу» за межі мережі свого підприємства. Статична відповідність приватних адрес цих вузлів глобальним адресам задано в таблицях прикордонних пристроїв обох мереж.

Коли вузол 10.0.1.5 мережі А посилає пакет хосту 10.0.1.2 мережі В, то він поміщає в заголовок пакета в якості адреси призначення глобальну адресу 185.127.125.2/24. Вузол-відправник, за замовчуванням, направляє пакет своєму маршрутизатору R1, якому відомий маршрут до мережі 185.127.125.0/24. Маршрутизатор передає пакет на прикордонний маршрутизатор R2, якому також відомий маршрут до мережі 185.127.125.0/24. Перед відправкою пакету модуль NAT, що працює на даному прикордонному маршрутизаторі R2, використовуючи таблицю відображення, замінює в полі адреси відправника приватну адресу 10.0.1.5 відповідною їй глобальною адресою 181.230.25.1/24. Коли пакет після проходження по зовнішній мережі надходить на зовнішній інтерфейс NAT-пристрою мережі В, глобальна адреса призначення 185.127.125.2/24 перетворюється на приватну адресу 10.0.1.2. Пакети, які передаються в зворотному напрямку, проходять аналогічну процедуру трансляції адрес.

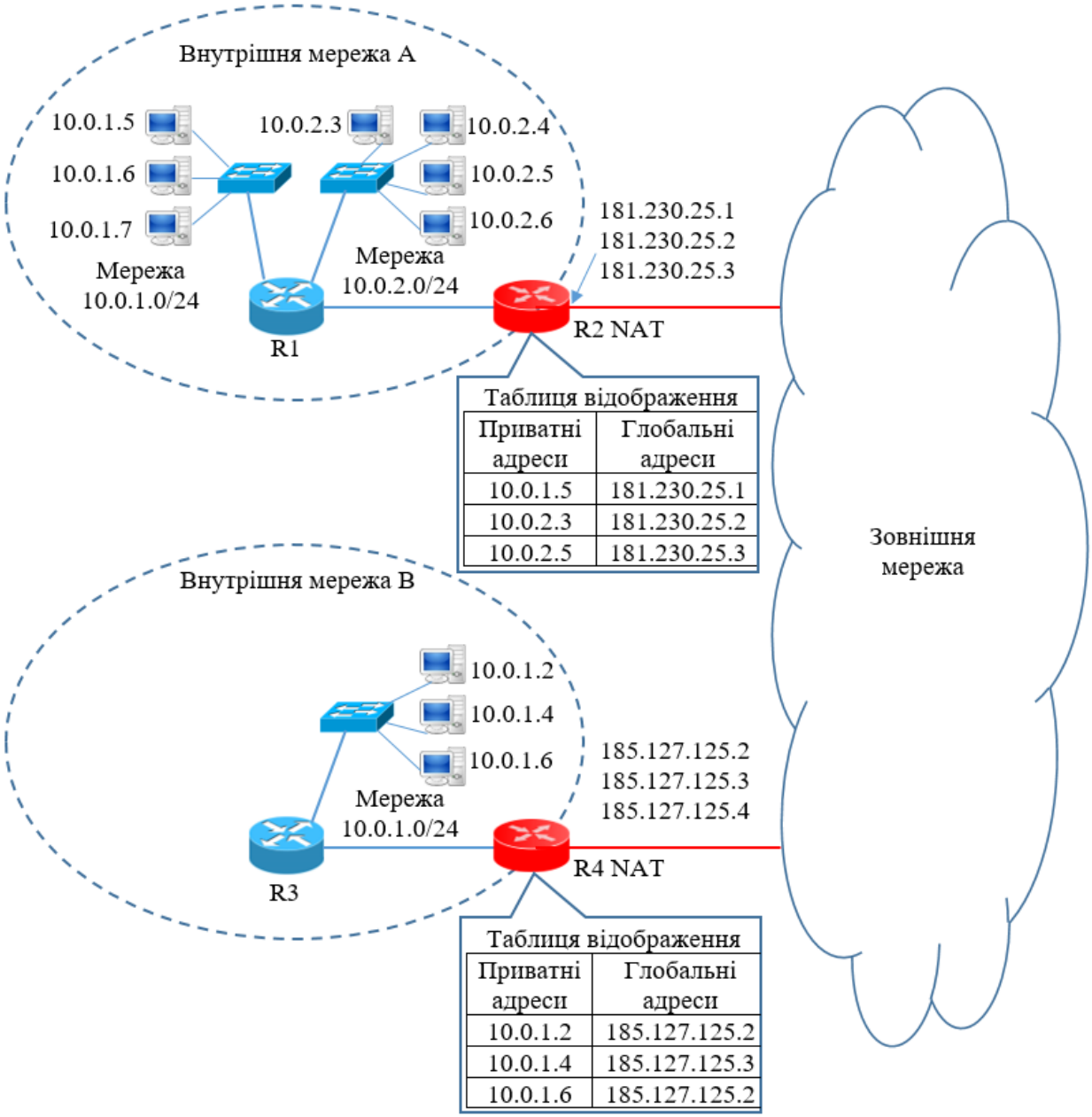


Рис. 5.11. Базова трансляція мережевих адрес

В описаній операції не потрібна участь вузлів відправника та одержувача, тобто вона прозора для користувачів.

5.4.3. Трансляція мережевих адрес і портів

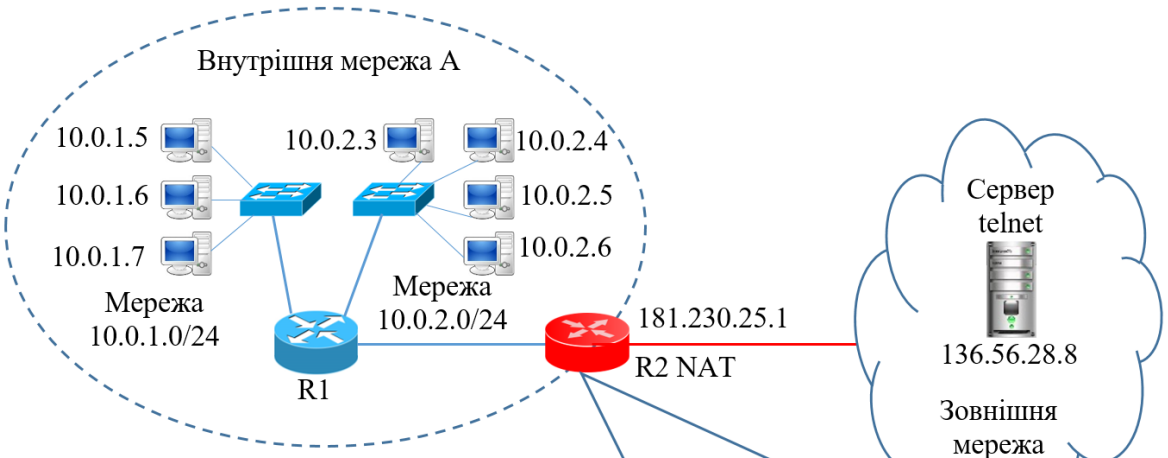
Нехай деяка організація має приватну IP-мережу і глобальний зв'язок з постачальником послуг Інтернету. Зовнішньому інтерфейсу прикордонного маршрутизатора R2 призначена глобальна адреса, а решта вузлам мережі організації призначені приватні адреси. NAPT дозволяє всім вузлам внутрішньої мережі одночасно взаємодіяти із зовнішніми мережами, використовуючи єдину

зареєстровану глобальну IP-адресу.

Оскільки, в полі адреси відправника всіх пакетів, що відправляються з будь-якого пристрою внутрішньої мережі в зовнішню мережу, поміщається одна і та ж адреса (адреса зовнішнього інтерфейсу прикордонного маршрутизатора), то для однозначної ідентифікації вузла-відправника залучається додаткова інформація. Якщо в IP-пакеті знаходяться дані протоколу UDP або TCP, то в якості такої інформації виступає номер порту UDP або TCP відповідно. Але і це не вносить повної ясності, оскільки з внутрішньої мережі може виходити кілька запитів з співпадаючими номерами портів відправника, а значить, виникає питання про однозначність відображення єдиної глобальної адреси на набір внутрішніх адрес. Рішення полягає в тому, що при проходженні пакету з внутрішньої в зовнішню мережу кожній парі {внутрішня приватна адреса; номер порту TCP або UDP відправника} ставиться у відповідність пара {глобальна IP-адреса зовнішнього інтерфейсу; призначений номер порту TCP або UDP}. Призначений номер порту вибирається довільно, однак повинна бути виконана умова його унікальності в межах всіх вузлів, які отримують вихід в зовнішню мережу. Відповідність фіксується в таблиці.

Ця модель при наявності єдиної глобальної IP-адреси, отриманої від постачальника послуг, задовольняє вимогам щодо доступу до зовнішніх мереж для більшості мереж середніх розмірів.

На рис. 5.12 наведено приклад, коли в мережі А використовуються внутрішні адреси з пулу 10.0.0.0. Зовнішньому інтерфейсу маршрутизатора цієї мережі постачальником послуг призначена адреса 181.230.25.1.



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

Рис. 5.12. Трансляція мережевих адрес і портів

Коли хост 10.0.1.5 внутрішньої мережі посилає в зовнішню мережу пакет серверу telnet, то він в якості адреси призначення використовує його глобальну адресу 136.56.28.8. Пакет надходить маршрутизатору R1, який знає, що шлях до мережі 136.56.0.0/16 йде через прикордонний маршрутизатор R2. Модуль NAPT маршрутизатора R2 транслює адресу 10.0.1.5 і порт TCP 1245 джерела в глобальну адресу 181.230.25.1 і унікально призначений TCP-порт, в наведеному прикладі – 3451. У такому вигляді пакет відправляється в зовнішню мережу і досягає сервера telnet. Коли одержувач генерує відповідь, то він в якості адреси призначення вказує єдину глобальну адресу внутрішньої мережі, що є адресою зовнішнього інтерфейсу NAPT-пристрою. В полі номера порту одержувача сервер поміщає призначений номер TCP-порту, взятий з поля порту відправника пакету. При надходженні відповідного пакета на NAPT-пристрій внутрішньої мережі саме за номером порту в таблиці трансляції вибирається потрібний рядок. По ній визначається внутрішня IP-адреса відповідного вузла і дійсний номер порту. Ця процедура трансляції повністю прозора для кінцевих вузлів.

5.5. Типові архітектури мереж, що захищаються файерволами

Вище було розглянуто функціональні можливості фаєрволів щодо захисту однієї мережі від можливих атак, що виходять від іншої мережі. У найпростішому випадку перша мережа – це єдина внутрішня мережа підприємства, а зовнішня представлена всіма мережами Інтернету, з'єднаними з внутрішньою мережею через єдину лінію зв'язку підприємства з провайдером Інтернету. В реальності ситуація виявляється складнішою – мережа підприємства може складатися з декількох мереж, при цьому сервери і хости цих мереж потребують захисту різного типу. Наприклад, якщо в одній мережі знаходиться поштовий сервер і веб-сервер підприємства, а в іншій – сервер бази даних клієнтів підприємства, то доступ до них повинен регулюватися відповідно до різних правил.

Якщо додати до цього, що багато підприємств поєднують свої мережі з Інтернетом декількома лініями зв'язку і, можливо, через кілька провайдерів, то захист мережі підприємства набуває ще один вимір – захист всього периметра мережі за допомогою декількох фаєрволів, при цьому їх правила захисту повинні бути узгодженими. Під **мережею периметра** розуміється сукупність всіх зв'язків корпоративної мережі з зовнішніми мережами – мережами провайдерів або корпоративними мережами інших підприємств.

Для надійного й ефективного захисту корпоративної мережі вона повинна бути логічно сегментована таким чином, щоб ресурси кожної підмережі по відношенню заходів захисту були подібними. 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**).

Розглянемо особливості організації захисту DMZ на прикладі мережі, показаної на рис. 5.13. 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.

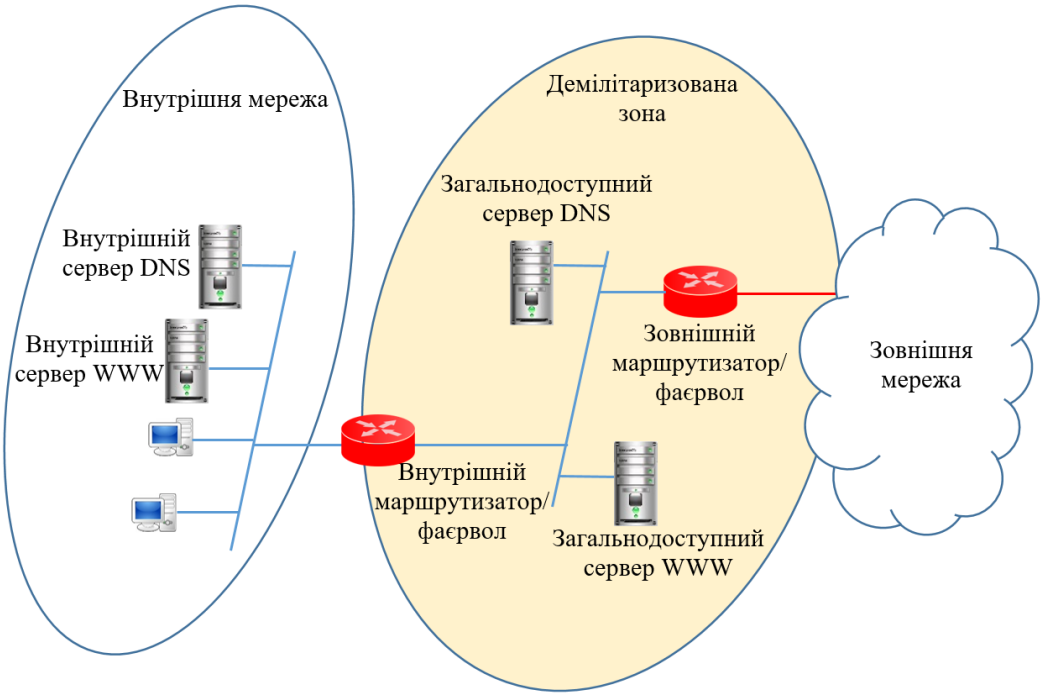


Рис. 5.13. Використання демілітаризованої зони

В мережі DMZ розташовані два загальнодоступних сервера – зовнішній DNS-сервер і зовнішній веб-сервер підприємства. У цій зоні можуть бути розміщені також проксі-сервери.

Враховуючи, що саме призначення цих комп'ютерів передбачає практично ніяк не обмежуваний доступ до них зовнішніх користувачів (а значить, і зловмисників), їх необхідно захищати особливо ретельно. Головними завданнями при захисті цих комп'ютерів (званих іноді **комп'ютерами-бастіонами**) є забезпечення цілісності та доступності розміщених на них даних для користувачів зовнішньої мережі. Цю задачу вирішують «індивідуальні» засоби захисту, що встановлюються на комп'ютерах-бастіонах, такі, наприклад,

як антивірусні програми або фільтри спаму. Крім того, кожен сервер, до якого дозволено звернення зовнішніх користувачів, повинен бути сконфігурований на підтримку тільки мінімально необхідної функціональності. Наприклад, публічний DNS-сервер підприємства не повинен бути відкритим для будь-яких запитів, так як він може стати інструментом DDoS-атаки.

Щоб пояснити, яким чином мережа периметра підсилює захист внутрішньої мережі, давайте подивимося, що станеться, якщо який-небудь зловмисник зможе «зламати» перший рубіж захисту – зовнішній маршрутизатор – і почне прослуховувати трафік підключеної до нього мережі периметра. Очевидно, що він отримає доступ тільки до трафіку загальнодоступних серверів, який не є секретним.

Зовнішній маршрутизатор покликаний фільтрувати трафік з метою захисту мережі периметра і внутрішньої мережі. Однак сувора фільтрація в цьому випадку виявляється незатребуваною. Загальнодоступні сервери за своєю суттю призначені для практично необмеженого доступу. Що стосується захисту внутрішньої мережі, правила фільтрації для доступу до її вузлів і сервісів є одними і тими ж для обох маршрутизаторів, тому зовнішній маршрутизатор може просто покластися в цій справі на внутрішній маршрутизатор.

Зазвичай, зовнішній маршрутизатор знаходиться в зоні ведення провайдера, і адміністратори корпоративної мережі обмежені в можливостях його оперативного конфігурування. Це є ще однією причиною, по якій функціональне навантаження на зовнішній маршрутизатор зазвичай невелике.

Основна робота по забезпеченню безпеки локальної мережі покладається на внутрішній маршрутизатор, який захищає її як від зовнішньої мережі, так і від мережі периметра. Правила, визначені для вузлів мережі периметра з доступу до ресурсів внутрішньої мережі, часто бувають більш суворими, ніж правила, що регламентують доступ до цих ресурсів зовнішніх користувачів.

Це робиться для того, щоб в разі злому будь-якого комп’ютера-бастіону зменшити число вузлів і сервісів, які згодом можуть бути атаковані з цього комп’ютера. Саме тому внутрішній маршрутизатор повинен відкидати всі пакети, які поступають у внутрішню мережу з мережі DMZ, виключаючи пакети кількох протоколів (наприклад, HTTP, SMTP, DNS), що необхідні користувачам внутрішньої мережі для звернення до зовнішніх серверів, встановлених в мережі DMZ або ж за межами корпоративної мережі.

Захист внутрішньої мережі можна посилити, якщо в ній є аналоги зовнішніх серверів, тобто в прикладі, це внутрішні веб-сервер і DNS-сервер. У такій конфігурації тільки цим серверам в разі потреби дозволяється взаємодіяти з серверами зони DMZ, внутрішні ж користувачі працюють безпосередньо лише з внутрішніми серверами. Наприклад, DNS-сервером за замовчуванням для

користувачів внутрішньої мережі повинен бути призначений внутрішній DNS-сервер, і тільки йому дозволено звертатися до зовнішнього DNS-сервера в тому випадку, коли він не може вирішити запит самостійно.

Захист внутрішніх серверів можна посилити за рахунок використання приватних IP-адрес у внутрішній мережі. У цьому випадку внутрішній маршрутизатор при трансляції приватних адрес повинен підтримувати режим NAPT на своєму інтерфейсі, що зв'язує його з мережею DMZ.

5.6. Моніторинг трафіку. Аналізатори протоколів

Файервол може успішно захистити внутрішню мережу від різноманітних атак за умови, що його фільтри правильно сконфігуровані. Однак навіть правильні фільтри конфігуруються статично, так що для справді ефективного захисту потрібно заздалегідь передбачити всі можливі атаки, а це в принципі неможливо. Будь-який новий тип атаки має всі шанси «пройти» через фаєрвол і досягти внутрішніх серверів мережі, що захищається. Виявити сліди атак, які змогли подолати бар'єр брандмауера, можна шляхом моніторингу мережевого трафіку.

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.

5.6.1. 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. Аналізатор протоколів підключається до мережі як звичайний вузол. Відмінність полягає в тому, що аналізатор протоколів може приймати всі пакети даних, що передаються по мережі, в той час як звичайна станція – адресовані тільки їй. Програмне забезпечення аналізатора протоколів складається з ядра, що підтримує роботу мережного адаптера і декодує одержувані дані, і додаткового програмного коду, що залежить від типу досліджуваної мережі. До складу деяких аналізаторів може входити також експертна система, яка здатна видавати користувачу рекомендації про те, які експерименти слід проводити в даній ситуації, що можуть означати ті чи інші результати вимірювань, як усунути деякі види несправностей в мережі.

Ґрунтуючись на результатах аналізу вмісту пакетів певного протоколу, можна оптимізувати продуктивність мережі, знаходити і усувати неполадки, здійснювати обґрунтовану і зважену зміну будь-яких компонентів мережі.

Можливості аналізатора багато в чому визначаються пристроєм і обсягом буфера захоплення пакетів. Буфер може розташовуватися на мережевій карті, або для нього може бути відведено місце в оперативній пам'яті одного з комп'ютерів мережі.

Якщо буфер розташований на мережевій карті, то управління ним здійснюється апаратно, і за рахунок цього швидкість введення підвищується. У разі недостатньої продуктивності процедури захоплення частина інформації буде губитися, і аналіз виявиться неможливим. При заповненні буфера або припиняється захоплення, або заповнення починається з початку буфера.

Як приклад розглянемо популярний вільно розповсюджуваний програмний аналізатор протоколів **Wireshark** (колишня назва - Ethereal). Wireshark дозволяє аналізувати захоплений трафік, використовуючи ієрархічне представлення полів пакетів (рис. 5.14).

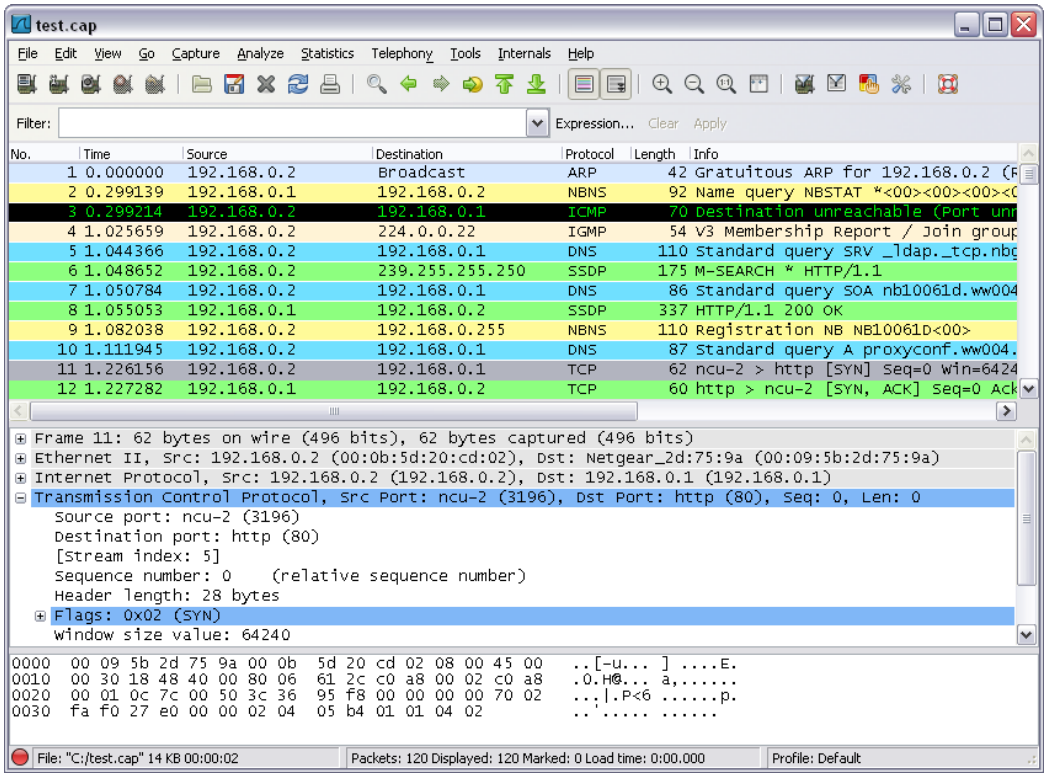


Рис. 5.14. Аналіз трафіку за допомогою Wireshark

Верхня панель вікна результатів Wireshark укрупнено показує основні параметри кожного захопленого пакета. Нижня панель дозволяє розглянути один з пакетів більш детально, при цьому ті поля, які складаються з декількох підполів, можна розкривати рекурсивно, добираючись до самого дна ієрархії ознак пакета, наприклад до ознак заголовка IP або TCP. Wireshark підтримує довгий список протоколів від канального до прикладного рівня, що дає можливість розкриття заголовків протоколів з поясненнями призначення кожного поля.

Wireshark дозволяє задавати фільтри двох типів: фільтр захоплення пакетів і фільтр відображення пакетів; умови завдання фільтрів досить гнучкі, практично будь-яке поле будь-якого протоколу може бути використано в умовах цих фільтрів. Захоплені кадри поміщаються в файл з розширенням .pcap (packet capture), стандартизований формат якого сьогодні підтримують практично всі програмні та програмно-апаратні засоби моніторингу трафіку.

Застосування аналізаторів протоколів для виявлення атак потребує значного досвіду, так як за десятками сеансів різних протоколів, що часто несуть надлишкову інформацію, не просто побачити підозрілу активність. Тому часто аналіз даних, зібраних аналізатором в файлі формату PCAP, автоматизують за допомогою програм аналізу трафіку (не слід плутати з аналізаторами протоколі).

5.6.2. 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.

Практично всі провідні виробники мережевого обладнання підтримують протокол NetFlow. Отже, для того, щоб перетворити маршрутизатор в джерело інформації про трафік, що проходить через нього, досить активізувати на ньому систему NetFlow і вказати, куди потрібно передавати статистику.

NetFlow збирає статистику не про кожен пакет, а про потік пакетів, звідси і назва протоколу (Net – мережа, Flow – потік). Під потоком розуміється послідовність пакетів, що належать одному і тому ж з'єднанню між певними додатками двох певних комп'ютерів, наприклад Skype-сеанс між двома користувачами, передача файлу з сервера на клієнтський комп'ютер, читання даних веб-сторінки з сервера браузером клієнтського комп'ютера. Аналогом потоку можна вважати дані телефонної розмови між двома абонентами, проте між двома комп'ютерами, на відміну від телефонів, може вестися відразу кілька «розмов». Тому для визначення потоку потрібно використовувати не тільки адреси, що беруть участь в сеансі комп'ютерів, але і додаткові ознаки. Зібрану статистику про проходження потоків можна використовувати для різних цілей, і одна з найважливіших – розпізнавання мережевих атак.

NetFlow визначає потік як набір декількох ознак, до числа яких найчастіше входять:

- IP-адреса відправника;
- IP-адреса отримувача;
- порт TCP/UDP відправника;
- порт TCP/UDP отримувача;
- тип протоколу, що переноситься IP-пакетом (корисно в тих випадках, коли це не TCP або UDP, наприклад це може бути ICMP або OSPF);
- індекс інтерфейсу, на який отримано пакет;
- якість обслуговування – значення байту ToS/DiffServ.

NetFlow збирає різноманітну статистику про потік, таку як час початку і закінчення потоку, обсяг даних, переданих з моменту початку потоку, середня швидкість передачі даних, ну і, зрозуміло, всі параметри, що визначають потік, тобто адреси, порти і т. д. Зібрана статистика передається в колектори (один або

кілька серверів) при закінченні потоку або ж після закінчення певного періоду часу, якщо потік ще не закінчився.

Маршрутизатор може збирати дані NetFlow в двох режимах: безперервному, коли обробляється кожен пакет, що надходить в маршрутизатор, і вибірковому, коли обробляється тільки кожен *n*-й пакет. Вибірковий режим менш надійний для розпізнавання атак, зате він створює набагато менше додаткового навантаження на маршрутизатор, а для магістрального маршрутизатора, через який проходять десятки, а іноді і сотні тисяч потоків, це суттєво.

Типова система моніторингу на базі NetFlow включає наступні функціональні компоненти (рис. 5.15):

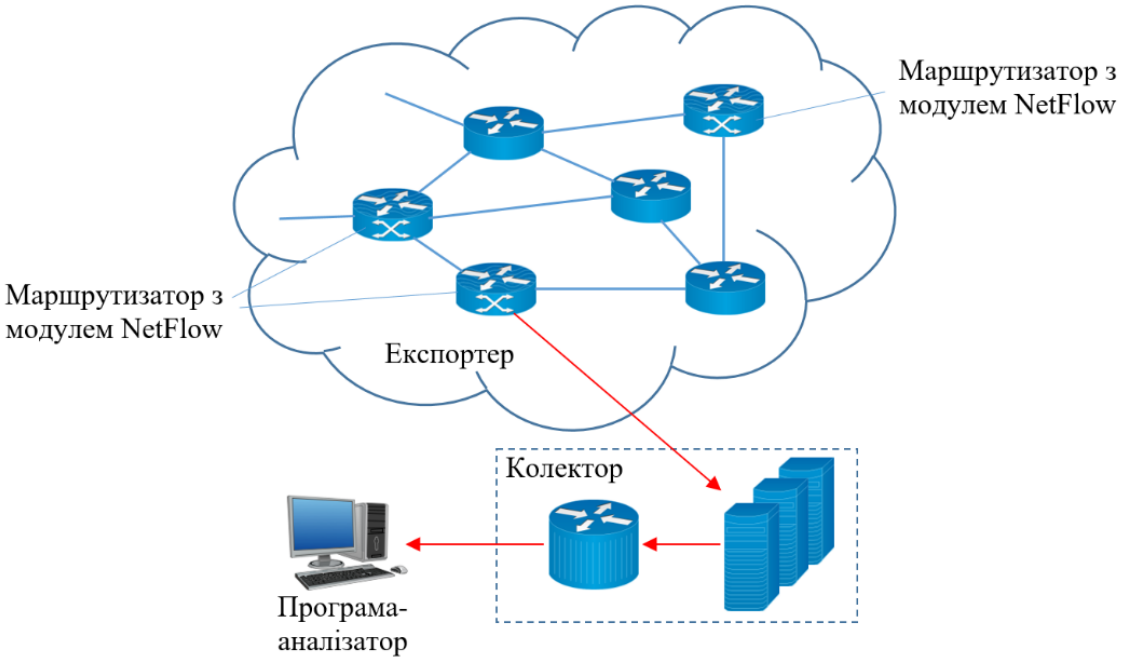


Рис. 5.15. Типова схема моніторингу на базі NetFlow

- **Експортер потоку** або **сенсор**, агрегує пакети в потоки і передає статистичні дані про ці потоки в один або кілька колекторів. Експортером найчастіше є маршрутизатор або комутатор, хоча можуть бути використані і інші пристрої, які отримують дані шляхом віддзеркалення порту комутатора.
- **Колектор** відповідає за прийом, зберігання і попередню обробку даних про потоки, отримані від експортера потоку. Реалізується одним або декількома серверами.
- **Програма-аналізатор** аналізує отримані дані про потоки з метою розпізнавання можливих атак або виникнення перевантажень мережі, встановлення складу і тенденцій зміни трафіку в мережі.

На відміну від аналізаторів трафіку і систем виявлення атак, NetFlow збирає так звані метадані про трафік, не заглядаючи в поля даних пакетів. Часто статистику NetFlow порівнюють з телефонним рахунком, який показує, з ким і скільки розмовляв даний абонент, але не розкриває, про що він говорив. Однак, знання метаданих часто буває достатньо для того, щоб розпізнати атаку. Для цього застосовується загальний принцип моніторингу мережі – порівняння її поточної поведінки з «нормальною», тобто такою, яка стійко повторювалась в минулому і при цьому атак в мережі не спостерігалося.

Стійкі значення статистичних характеристик «нормальної» поведінки мережі та її вузлів, які отримані на підставі моніторингу мережі за значний період часу (тижні, місяці), називаються **базовим рівнем** (baseline) характеристик мережі.

Існують декілька основних рекомендацій для розпізнавання атак:

- **Виявлення вузлів з незвично великим числом запитів на встановлення з'єднань** (Top N Sessions). Якщо який-небудь вузол раптом увійшов в число N вузлів, найбільш активних щодо встановлення сеансів, то це повинно викликати підозри (значення N зазвичай вибирається не дуже великим, наприклад 10). Така активність характерна для DOS/DDOS-атак, вузлів, заражених черв'яками, сканування портів і деяких інших видів зловмисної діяльності. Так, комп'ютер, заражений черв'яком, зазвичай намагається заразити таким кодом якомога більше інших комп'ютерів і тому намагається з ними з'єднатися. Спам-хост буде намагатися надіслати якомога більше листів і тому встановлювати велику кількість з'єднань в одиницю часу з портом 25 (SMTP-порт, на який відправляється пошта).
- **Виявлення вузлів з незвично інтенсивним трафіком** (Top N Data). В цьому випадку хост, який зазвичай не входив в число N найактивніших, починає посилати або одержувати незвично велику кількість даних в одиницю часу, тобто генерувати занадто інтенсивний трафік. Це також може бути DoS-атака або ж активність черв'яка, який намагається заразити інші хости.
- **Аналіз *SYN* і інших прапорів заголовка TCP**. Наявність незвично великої кількості пакетів з встановленим прапором *SYN* або іншими прапорами заголовка TCP може свідчити про DoS-атаку.
- **Аналіз ICMP-повідомлень**. Велика кількість ICMP-повідомлень «Порт/хост/мережа недоступна» може свідчити про сканування зловмисником або вірусом хостів і портів.

Іншим ефективним методом аналізу трафіку є перевірка значень деяких

полів пакетів на предмет збігу зі значеннями, що використовуються в відомих типах атак (порівняння із зразками). Найчастіше зразками атаки є значення портів TCP/UDP і IP-адрес. Наприклад, хробак SQL Slammer найчастіше використовує TCP-порт 1434, а черв'як W32/Netsky.c завжди використовує DNS-сервер з адресою зі списку конкретних IP-адрес.

Коли колектор отримує кожну секунду дані про тисячі, а іноді і десятки і навіть сотні тисяч потоків, то для обробки таких даних необхідно задіяти спеціальне програмне забезпечення. Програмні системи аналізу даних NetFlow існують. Вони автоматизують процедури виявлення аномальної активності в мережі, перевіряючи потоки на відповідність численним зразкам різноманітних атак, в першу чергу атак відмови в обслуговуванні і сканування мережі та портів. Дані, віднесені системою до підозрілої активності, виділяються в особливу групу і надаються адміністратору мережі в компактній формі. Крім того, адміністратор може створювати власні правила виявлення підозрілої активності.

В цілому підхід до аналізу даних NetFlow повинен бути адаптивним, базуватись на постійному оновленні та поповненні бази ознак атак, тобто аналітик повинен намагатися «йти в ногу» з розробниками вірусів, ботів та іншого шкідливого програмного забезпечення.

5.6.3. 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.

Існують ситуації, коли мережевий екран виявляється проникним для зловмисника: наприклад, коли атака йде через тунель VPN із зламаної мережі, коли ініціатором атаки є користувач внутрішньої мережі і т. п. І справа тут не в поганій конфігурації брандмауера, а в самому принципі його роботи. Фаєрвол, незважаючи на те що володіє пам'яттю і аналізує послідовність подій, конфігурується на блокування трафіку з заздалегідь передбачуваними ознаками, наприклад за IP-адресами або протоколами. Так що факт злому зовнішньої мережі, з якою у нього був встановлений захищений канал і яка раніше поводилася цілком коректно, в правилах екрану відобразити не можна. Так само, як і неочікувану спробу легального внутрішнього користувача скопіювати файл з паролями і підвищити рівень своїх привілеїв. Подібні підозрілі дії може

виявити тільки система, оснащена агентами, що вбудовані в багато точок мережі, причому вона повинна стежити не тільки за трафіком, а й за всіма зверненнями до критично важливих ресурсів окремих комп'ютерів, а також мати інформацію про перелік підозрілих дій (сигнатур атак) користувачів. Такою і є система виявлення вторгнень. Вона не дублює дії брандмауера, а доповнює їх, виробляючи, крім того, автоматичний аналіз всіх журналів подій, що містять мережеві пристрої і засобів захисту, щоб спробувати знайти сліди атаки, якщо її не вдалося зафіксувати в реальному часі.

Іншою важливою відмінністю IDS від фаєрволів є те, що в обов'язки IDS не входить блокування підозрілого трафіку. IDS тільки намагається виявити підозрілу активність і підняти тривогу – зазвичай, шляхом попередження адміністратора мережі електронним повідомленням. Крім підняття тривоги IDS протоколює підозрілі пакети, поміщаючи їх в журнал.

Типова система IDS включає наступні функціональні елементи (рис. 5.16):

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

Джерелами даних для мережевої системи IDS є маршрутизатори, комутатори і хости локальної мережі, тобто усі елементи мережі, які передають, генерують і приймають трафік.

Давач копіює пакети, що циркулюють в мережі, і передає їх аналізатору для виявлення підозрілої активності. Давач може являти собою окремий комп'ютер, що під'єднаний до порту комутатора/маршрутизатора, або ж це може бути програмний компонент маршрутизатора, який має доступ до пакетів, що буферизуються на його інтерфейси. Давач може здійснювати первинну фільтрацію пакетів, відбираючи тільки ті пакети, які задовольняють деяким очевидним критеріям, наприклад спрямовані до публічних веб-серверів, які атакуються найбільш часто.

Аналізатор є центральним елементом IDS, він отримує дані від давачів і перевіряє їх на наявність загроз та підозрілої активності в мережі. Аналізатор працює на основі правил, складених **адміністратором** системи безпеки підприємства відповідно до політики безпеки. При виконанні умови одного з правил аналізатор формує повідомлення тривоги і передає його **менеджеру** системи IDS – програмному компоненту, який зберігає конфігурацію IDS і підтримує зручний інтерфейс з оператором IDS. Менеджер IDS сповіщає

оператора IDS про тривогу у вигляді деякого повідомлення, що привертає увагу, наприклад у вигляді текстового рядка на екрані з мерехтливим символом, у вигляді звукового сигналу і т. п.

Оператор системи IDS на основі даних повідомлення приймає рішення про реакцію мережі на підозрілу активність – це може бути відключення мережевого інтерфейсу, через який надходить підозрілий трафік, зміна правил брандмауера для блокування певних пакетів або ж ігнорування повідомлення, якщо оператор вважає, що ймовірність вторгнення дуже мала. У будь-якому випадку, всі дані про потенційне вторгнення протоколюються в журналі менеджера і можуть бути використані згодом для повторного аналізу ситуації. Якщо ж IDS виконує також функції IPS, то менеджер може автоматично передати команди на маршрутизатор або фаєрвол для блокування підозрілого трафіку.

Поряд з системами виявлення вторгнень існують **системи попередження вторгнень** (Intrusion Prevention Systems, **IPS**), які виконують автоматичні дії по припиненню атаки в разі її виявлення. Часто такі системи передоручають цю роботу фаєрволу, передаючи йому нове правило для блокування підозрілого трафіку. В IPS для виявлення вторгнень застосовуються декількох типів правил:

Правила, що базуються на сигнатурі (підпису) атаки (Signature Rules), використовують характерну для атаки послідовність символів в даних пакета. Наприклад, правило може диктувати пошук рядка «user root» в полях FTP-пакета – як відомо, цей протокол передає паролі користувачів у відкритому вигляді і застосування його суперкористувачем root вважається грубим порушенням політики безпеки підприємства, так що система IPS повинна відстежувати такі випадки. Найчастіше сигнатури атак відносяться до прикладних протоколів, для виявлення вторгнення на транспортному рівні вони менш придатні. Для ефективної роботи система IPS повинна мати велику базу сигнатур атак, що постійно поповнюються.

Правила, що базуються на аналізі протоколів (Protocol Rules), пов’язані з перевіркою логіки роботи протоколу і фіксацією відхилень від нього. Оскільки кожен протокол має специфічну логіку, IPS зазвичай має бібліотеку програмних модулів, кожен з яких може аналізувати поведінку певного протоколу. Правила аналізу протоколів написати набагато складніше, ніж правила аналізу підпису атаки, так як для цього потрібно добре знати логіку протоколу та можливі відхилення від неї. Реалізація правил аналізу протоколів вимагає великої швидкодії IPS, в іншому випадку робота системи IPS може значно сповільнитися і вона не зможе працювати в реальному часі.

Правила, що базуються на статистичних аномаліях трафіку, перевіряють такі характеристики трафіку, як Top N Sessions, Top N Data, які були розглянуті в описі технології аналізу даних NetFlow.

6. Атаки на транспортну інфраструктуру мережі

6.1. TCP-атаки

Протокол TCP використовується зловмисниками і як інструмент для організації атак (зазвичай, це атаки відмови в обслуговуванні), і як мета нападу – порушення TCP-сеансу атакованого додатку, наприклад шляхом підробки сегменту.

6.1.1. Затоплення SYN-пакетами

Цей тип DoS-атаки активно застосовується зловмисниками протягом багатьох років, вперше він був детально описаний (з приведенням коду атаки) в 1996 році, і вже в тому ж році почалося його практичне «застосування», яке триває донині. Атакованим є кінцевий вузол, як правило, сервер, що працює з клієнтами по протоколу TCP.

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. 6.1, 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. 6.1, б). Отримавши пакет з прапором *SYN*, сервер виділяє для нового з'єднання необхідні ресурси і в повній відповідності з протоколом відповідає клієнту пакетом з прапорами *ACK* і *SYN*. Після цього, встановивши тайм-аут, він починає чекати від клієнта завершальний пакет з прапором *ACK*, який, на жаль, так і не приходить.

Аналогічним чином створюється безліч інших «недовстановлених» з'єднань. Зазвичай, операційна система сервера має ліміт на кількість одночасно підтримуваних «недовстановлених» TCP-з'єднань (глобально або для кожного програмного порту окремо), так як кожне відкрите з'єднання вимагає виділення пам'яті ядра ОС для нового **блоку керування TCP** (TCP Control Block, **TCB**). Цей блок містить дані про стан з'єднання: сокет клієнта, номер очікуваного сегмента, покажчик на положення сегмента в буфері і ін. Блок TCB має розмір від 280 до 1300 байт в залежності від типу ОС. При досягненні ліміту ОС починає відкидати всі наступні запити на встановлення TCP-з'єднань, а отже, відмовляє в обслуговуванні всім, в тому числі легальним клієнтам сервера. Після закінчення тайм-ауту ОС видаляє з пам'яті блоки TCB «недовстановлених» з'єднань і знову починає встановлювати нові з'єднання.

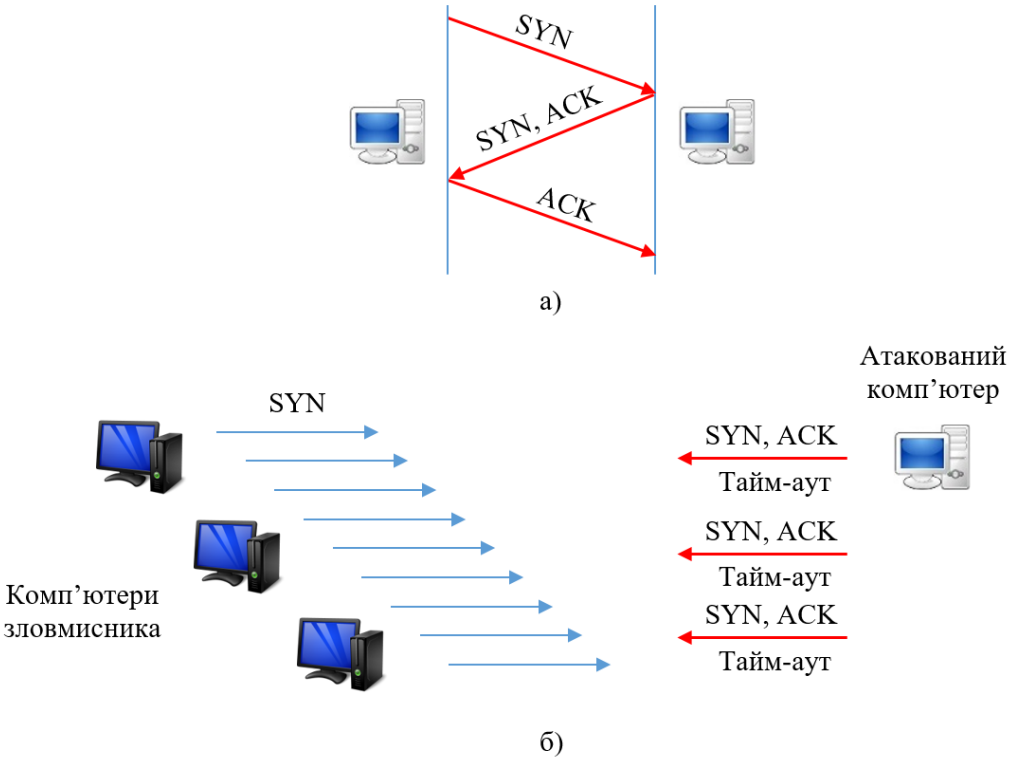


Рис. 6.1. Проведення DoS-атаки, в якій використовується особливість протоколу TCP:
а – нормальний порядок встановлення TCP-з'єднання; б – DoS-атака шляхом створення множини незакритих TCP-з'єднань

Для здійснення атаки затопленням SYN-пакетами атакуючий повинен заблокувати нормальну реакцію свого комп'ютера на отримання від атакованого сервера сегменту з прапорами *SYN/ACK*. Нормальна реакція полягає в тому, що відповідно до протоколу TCP атакуючий повинен відправити у відповідь сегмент з прапором *ACK*. Але, якщо це станеться, атакований сервер вважатиме процедуру встановлення TCP-з'єднання завершеною, видалить відповідний блок TCB зі списку «недовстановлених» з'єднань і почне приймати нові з'єднання, тобто атака не вдасться. Тому атакуючий фільтрує вхідний трафік, відсіваючи відповіді *SYN/ACK* від атакованого сервера.

Зазвичай, атака затопленням SYN-пакетами виявляється за рахунок наявності в трафіку великої кількості SYN-сегментів без відповідної кількості ACK-сегментів, що йдуть від того ж джерела. При цьому помітного сплеску мережевого трафіку може і не бути, так як ліміт «недовстановлених» з'єднань сам по собі не настільки великий. Головним засобом боротьби з атакою затопленням SYN-пакетами є **фільтрування трафіку**, що надходить від джерела атаки. Для цього потрібно визначити адресу атакуючого вузла.

У деяких випадках це зробити не просто, так як 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.

Спуфінг допомагає атакуючому не лише подолати захисний фільтр, а й позбутися від шкідливих для нього SYN/АСК-сегментів, які надсилаються у відповідь атакованим сервером. Для цього йому досить вибрати в якості «підроблених» такі адреси, які не реагуватимуть на SYN/АСК-сегменти, наприклад адреси неіснуючих вузлів.

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).

Іншим способом боротьби з атакою затопленням SYN-пакетами є **зміна параметрів протоколу TCP** – збільшення граничного числа «недовстановлених» з'єднань, зменшення тайм-ауту витіснення старих «недовстановлених» з'єднань, ускладнення логіки самої процедури встановлення з'єднання, наприклад введення спеціальних **cookie-блоків SYN**. У цьому методі при прийомі SYN-запиту сервер не запам'ятовує блок TCB у своїй оперативній пам'яті, а посилає його (в стислому вигляді) клієнту разом з *SYN/ACK* відповіддю. При нормальному ході встановлення з'єднання клієнт відповідає *ACK*-сегментом, в якому повторює стислий блок TCB, сервер, отримавши цей *ACK*-сегмент, а з ним і всі параметри встановлюваного з'єднання, створює відповідний блок TCB в пам'яті свого ядра. Оскільки в цій модифікованій процедурі на початковому етапі встановлення з'єднання ресурси на сервері не виділяються, то і атака затопленням SYN-пакетами просто не виходить.

Різновидом TCP-атаки затопленням SYN-пакетами є TCP-атака затопленням АСК-пакетами, що виконується шляхом відображення. Зловмисник посилає SYN-пакети з адресою жертви на велику кількість серверів, які відповідають на SYN-пакети пакетами з встановленим бітом АСК. АСК-пакети бомбардують атакований комп'ютер і вичерпують пропускну спроможність його вхідного інтерфейсу. Цей прийом перетворює DoS-атаку в DDoS-атаку без використання мережі ботів, так як всі комп'ютери, що відповідають на SYN-запити, не заражаються попередньо будь-яким вірусом, а працюють в повній відповідності зі стандартною версією протоколу TCP.

6.1.2. Підробка TCP-сегмента

Протокол TCP служить для підвищення надійності транспорту, для цього кожен сегмент даних супроводжується порядковим номером першого байту сегмента, причому початкові значення цих номерів для кожної з двох сторін, що обмінюються даними, вибираються випадковим чином. При прийомі чергового сегменту протокол TCP перевіряє, чи знаходиться його порядковий номер в межах вікна прийому, і тільки в разі позитивного результату такої перевірки додає прийняті дані до байтів, прийнятих раніше в ході даного TCP-сеансу. Описана перевірка призначена для захисту сегментів деякого TCP-сеансу від змішування з сегментами інших сеансів, але цей механізм захисту не є надійним, чим і користуються зловмисники.

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 IP-адреси, номера TCP-портів відправника і отримувача, а також порядкові номери з поточного діапазону вікна прийому. Приймаюча сторона не може відрізнити такі підроблені сегменти від справжніх і поміщає інформацію зловмисника в потік користувацьких даних, а отже, зловмисник може добитися бажаного ефекту: наприклад, помістити неправдиву інформацію в базу даних, заразити атакований комп'ютер вірусом і т. п.

Для того, щоб «підроблений» сегмент виглядав як справжній, атакуючий може або прослуховувати трафік, або просто перебирати всі можливі значення адрес, портів і порядкових номерів сегментів. Прослуховування трафіку є нетривіальною задачею, що пов'язана з перенаправленням трафіку (атаки такого типу розглянемо пізніше). У той же час перебір параметрів TCP-сеансу вимагає великої обчислювальної потужності комп'ютера атакуючого. В обох випадках атакувати простіше тривалі TCP-сеанси, наприклад сеанси завантаження великих відеофайлів; короткі сеанси з'єднань менш вразливі.

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. Цей прийом може застосовуватися зловмисником для різних цілей: наприклад, він може викликати таким чином порушення роботи деякого додатку, який використовує TCP як транспорт, за рахунок подання застарілої (перехопленої) інформації в якості нової.

6.1.3. Скидання TCP-з'єднання

Атака **скиданням TCP-з'єднання** використовується для розриву TCP-з'єднань легальних користувачів. При надходженні TCP-сегмента з встановленим прапором *RST* вузол повинен негайно завершити сеанс, до якого відноситься цей сегмент, і видалити всі дані, отримані в ході сеансу. Розробники протоколу TCP ввели цей прапор для обробки аварійних ситуацій. Наприклад, якщо в одному з вузлів під час TCP-сеансу відбувається збій, то після відновлення системи він може надіслати сегмент з цією ознакою, повідомити вузол-співрозмовник про неможливість продовжити розмову.

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.

6.2. ICMP-атаки

6.2.1. Перенаправлення трафіку

Перенаправлення трафіку можна здійснити в самих різних цілях, з однією з них, на-приклад, ми тільки що зіткнулися, розглядаючи атаку підробкою TCP-сегментів.

Способів перенаправлення трафіку існує кілька. Так, в межах локальної мережі це завдання можна вирішити за допомогою протоколу ICMP. 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. На рис. 6.2 маршрутизатор R1, отримавши від хоста H1 пакет, адресований хосту H2, визначає, що найкращий маршрут до хосту H2 пролягає через інший маршрутизатор даної локальної мережі, а саме через маршрутизатор R2.

Маршрутизатор R1 відкидає отриманий пакет і поміщає його заголовок в ICMP-повідомлення про перенаправлення маршруту, яке надсилає хосту H1. У повідомленні міститься IP-адреса альтернативного маршрутизатора R2, який тепер повинен використовувати хост, передаючи дані хосту H2. Хост H1 вносить зміни в свою таблицю маршрутизації і з цього моменту відправляє пакети хосту H2 по новому, скоригованому маршруту.

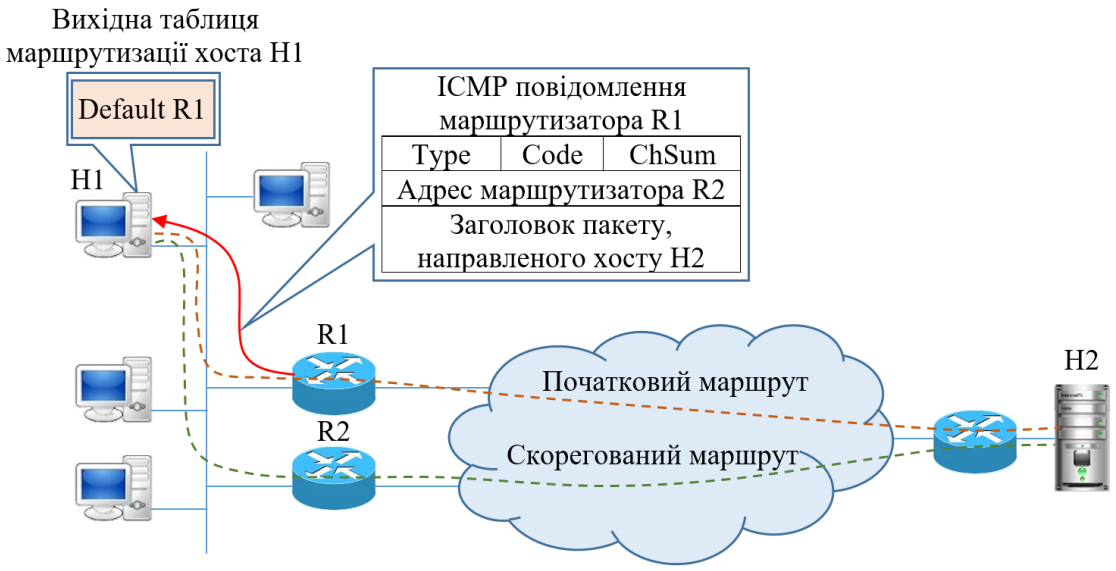


Рис. 6.2. Перенаправлення маршруту маршрутизатором по замовчуванню

Для перехоплення трафіку, що направляється хостом H1 хосту H2, зловмисник повинен сформувати і надіслати хосту H1 пакет, що маскується під ICMP-повідомлення про перенаправлення маршруту (рис. 6.3). У цьому повідомленні міститься запит про коригування таблиці маршрутизації хоста H1 так, щоб у всіх пакетах з адресою призначення IP_{H2} адресою наступного маршрутизатора була адреса IP_{HA}, що є адресою хоста-зловмисника HA.

Для того, щоб хост «повірив» цьому повідомленню, в поле IP-адреси відправника повинна бути поміщена адреса пропонованого за замовчуванням маршрутизатора R1. Коли пакети, що передаються хостом-жертвою H1, почнуть надходити на вузол зловмисника, він може або захоплювати і не передавати ці пакети далі, імітуючи для підтримки діалогу додаток, яким ці пакети призначалися, або організувати транзитну передачу даних за вказаною адресою призначення IP_{H2}. Читаючи весь трафік між вузлами H1 і H2, зловмисник отримує всю необхідну інформацію для несанкціонованого доступу до сервера H2.

Самі маршрутизатори також можуть реагувати на ICMP-повідомлення про перенаправлення маршруту, але зазвичай провайдери відключають цю опцію для запобігання атак даного типу.

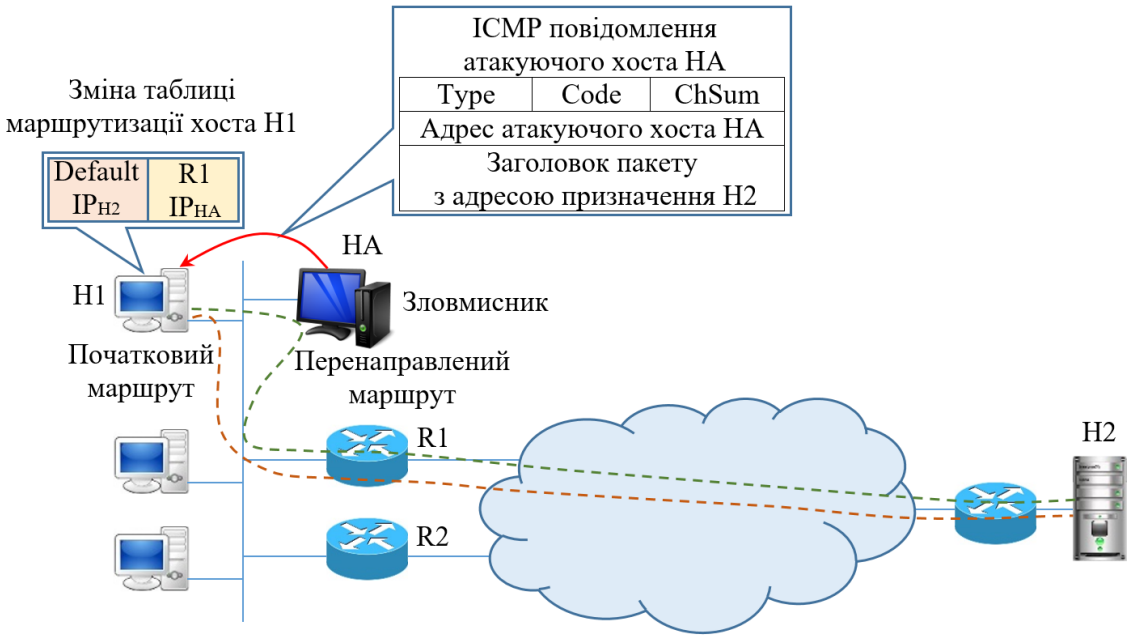


Рис. 6.3. Перенаправлення маршруту зловмисником

Простий варіант перенаправлення трафіку в локальній мережі може бути здійснений шляхом відправки в мережу неправдивої ARP-відповіді. В даному випадку схема очевидна: отримавши широкотрансляційний ARP-запит відносно деякої IP-адреси, зловмисник надсилає неправдиву ARP-відповідь, в якій повідомляється, що даній IP-адресі відповідає його власна MAC-адреса.

6.2.2. ICMP-атака Smurf

ICMP-атака **Smurf** – це DDoS-атака, яка використовує функцію exo-запиту протоколу ICMP. Назва атаки походить від назви файлу smurf.c, що містить код атаки і отримав поширення в 1998 році.

Exo-запити і exo-відповіді протоколу ICMP більш відомі по утиліті ping, за допомогою якої можна перевірити досяжність віддаленого вузла. Для перевірки досяжності утиліта ping надсилає тестованому вузлу ICMP-пакет, в якому в якості типу повідомлення зазначений код 8 (exo-запит). Отримавши його, тестований вузол відправляє в зворотному напрямку ICMP-пакет з кодом 0 (exo-відповідь).

В атаці Smurf використовується той факт, що exo-запит може бути надісланий не тільки по індивідуальній, а й по широкотрансляційній (broadcast)

адресі деякої мережі. Наприклад, якщо у мережі адреса 200.200.100.0/24, то її широкотрансляційною адресою є 200 200.100.255, і ехо-запит повинен бути доставлений всім вузлам цієї мережі. Атаку ілюструє рис. 6.4.

Комп'ютер зловмисника генерує ехо-запити з адресою отримувача 200.200.100.255 і адресою відправника 195.204.20.145. Ехо-запити передаються через Інтернет в мережу 200.200.100.0/24 і приймаються усіма вузлами цієї мережі, які відповідають на ICMP-запити ехо-відповідями. У тому випадку, коли в мережі 200.200.100.0 є досить велика кількість активних вузлів (зрозуміло, що їх не може бути більше 254), то на атакований вузол 195.204.20.145 приходить інтенсивний потік ехо-відповідей, так як саме його адреса вказана в ехо-запиті як адреса відправника. В результаті мережевий інтерфейс атакованого комп'ютера виявляється затопленим ехо-відповідями і при перевищенні інтенсивності цього потоку деякої величини його пропускна спроможність виявляється вичерпаною.

У ICMP-атаці Smurf використовується характерний прийом – посилення атаки за рахунок відображення надісланого пакета великою кількістю комп'ютерів.

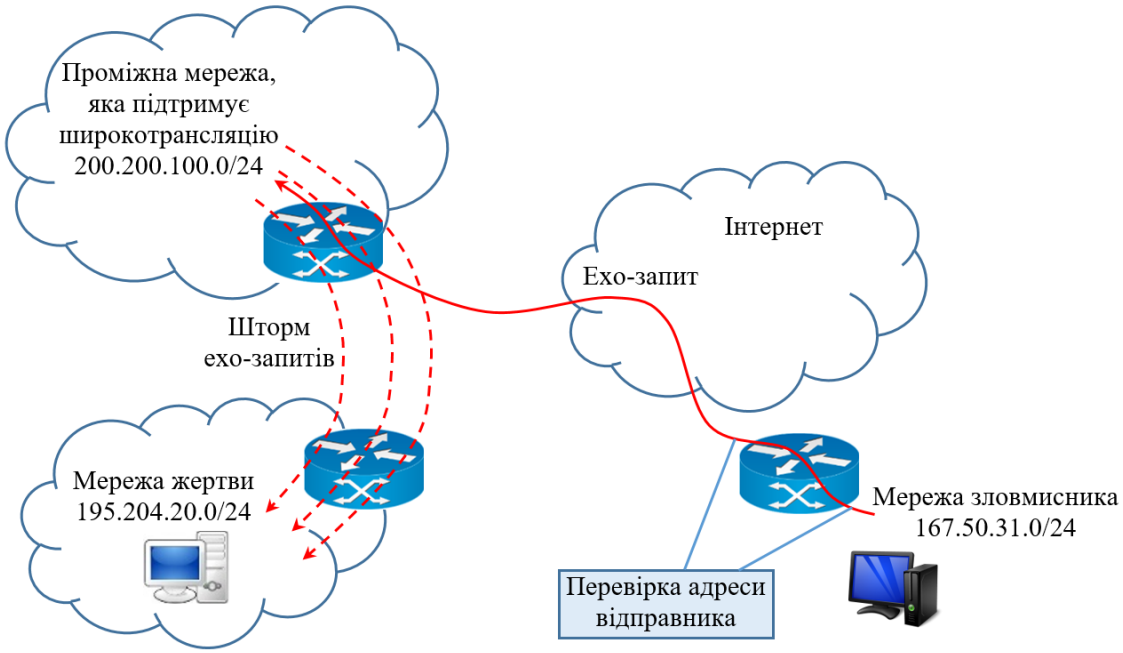


Рис. 6.4. Компоненти ICMP-атаки Smurf

ICMP-атака Smurf представляє сьогодні швидше історичний інтерес. До 1999 року передача через Інтернет IP-пакета з широкотрансляційною адресою була обов'язковою для маршрутизаторів Інтернету, але через атаки, подібні Smurf, в стандарти було внесено зміну, і сьогодні, за замовчуванням, використовується режим фільтрації пакетів з широкотрансляційними адресами.

Крім того, проміжна мережа, вузли якої використовуються для відображення ехо-запиту, може бути екранована за допомогою брандмауера від ехо-запитів, що приходять із зовнішніх мереж. А щоб запобігти ICMP-атаці Smurf з внутрішньої мережі, можна заборонити всім комп'ютерам цієї мережі реагувати на широкотрансляційні ехо-запити.

6.2.3. 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.

Атака Пінг смерті вже давно має тільки історичний інтерес, так як розробники ОС в середині 90-х років ввели в стек IP необхідну перевірку довжини фрагментованого IP-пакета і тим самим ліквідували саму базу для атаки.

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. До того ж атакований комп'ютер буде встигати відповідати на частину ехо-запитів ехо-відповідями, що призведе до часткового вичерпання пропускної спроможності в вихідному напрямку, а також до уповільнення роботи програм через відволікання центрального процесора на обробку ехо-запитів.

6.3. UDP-атаки

6.3.1. UDP-затоплення

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. Оскільки протокол UDP працює без встановлення з'єднання, то атакований комп'ютер зобов'язаний

приймати усі направлені йому UDP-датаграми – він не може, як це відбувається при обміні даними по протоколу TCP, змусити передаючий комп'ютер обмежити інтенсивність потоку направлених йому пакетів, зменшивши розмір вікна прийому. Зловмисник може використовувати апаратний генератор трафіку для того, щоб генерувати UDP-трафік з максимально можливою швидкістю вихідного інтерфейсу, ігноруючи відповідні ICMP-повідомлення в тих випадках, коли у атакованого комп'ютера програмний порт, зазначений в UDP-пакетах, не відкритий.

Слабким місцем такого виду атак є те, що їх інтенсивність принципово обмежена продуктивністю інтерфейсу атакуючого комп'ютера. Маючи стандартний для користувача комп'ютера інтерфейс 100 Мбіт/с або 1 Гбіт/с, неможливо затопити UDP-пакетами сервер з інтерфейсом 10 Гбіт/с. Зловмисник може подолати це обмеження, якщо у нього в розпорядженні є мережа ботів. Саме такий підхід був використаний в 2007 році, коли була здійснена масована DDoS-атака UDP-затопленням на кореневі DNS-сервери, при цьому трафік створювався приблизно п'ятьма тисячами ботів.

6.3.2. ICMP/UDP-затоплення

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). При отриманні UDP-пакета з номером пасивного порта комп'ютер відповідно до логіки роботи стеку TCP/IP відповідає ICMP-повідомленням про недосяжність порту призначення, яке направляється атакованому комп'ютеру. В разі використання широкотрансляційної адреси вона стає DDoS-атакою. Для запобігання цієї атаки застосовують ті ж заходи, що і для запобігання ICMP-атаки Smurf, додатково реалізується пропуск фаєрволом тільки тих UDP-пакетів, порти яких відповідають активним додаткам комп'ютерів мережі. Крім того, можна обмежити інтенсивність повідомлень про недосяжність порту призначення комп'ютерів мережі.

6.3.3. UDP/echo/chargen-затоплення

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.

CHARGEN (Character Generator Protocol) – це служба стеку протоколів TCP/IP, яка призначена для тестування, вимірювання і налагодження мережі. Цей сервіс вбудований в ОС Unix для налагодження її мережевих функцій. Аналогічне призначення має сервіс **echo** (не плутати з ехо-запитами і ехо-відповідями протоколу ICMP), він просто повертає рядок будь-якого запиту за адресою хоста, що звернувся.

У найпростішому випадку атакуючий посилає UDP-пакети на порт 7 і/або 19 деякого проміжного хоста і вказує зворотну адресу атакованого хоста. Проміжний хост починає бомбардувати атакований хост відповідями сервісів chargen і/або echo. Для посилення атаки можна використовувати широкотрансляційну адресу проміжної мережі. Більш цікавою виглядає атака, коли атакуючий надсилає пакет з портом 19 і вказує в ньому вихідний порт 7. У цьому випадку єдиний пакет атакуючого викликає нескінченний обмін пакетами між сервісом chargen проміжного хоста і сервісом echo атакованого хоста.

6.4. IP-атаки

6.4.1. Атака на IP-опції

Атака на IP-опції являє собою DoS-атаку на маршрутизатори, в якій використовується поле додаткових опцій протоколу IP.

У IPv4 заголовок IP-пакету може включати поле опцій, які задають деяку нестандартну обробку пакету маршрутизатором. Наприклад, існує опція строгої маршрутизації від джерела, яка дозволяє відправнику IP-пакету задати точний список адрес проміжних маршрутизаторів, через які повинен проходити маршрут доставки пакету, в той час як опція вільної маршрутизації від джерела задає тільки деякі з проміжних маршрутизаторів маршруту. Опція фіксації маршруту вимагає від маршрутизаторів фіксації в пакеті адрес проміжних маршрутизаторів, які передавали пакет. Існує також можливість для виробників маршрутизаторів визначати свої типи опцій.

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. Коли ж зустрічається пакет з полем опцій, то спеціалізований процесор його обробляти не може і передає пакет центральному процесору маршрутизатора, в результаті обробка пакету суттєво сповільнюється. Тому

потік пакетів, у яких присутня одна або кілька опцій, може призвести до серйозного уповільнення роботи маршрутизатора, в крайньому випадку – до відмов в обслуговуванні нормальних пакетів. Погіршує ситуацію присутність в пакеті двох взаємовиключаючих опцій, наприклад строгої маршрутизації від джерела і вільної маршрутизації від джерела з різними проміжними адресами.

Специфікація IPv6 допускає наявність декількох заголовків в пакеті – основного і декількох додаткових. Замість полів опцій в пакеті IPv6 можуть бути присутніми додаткові заголовки, одним з яких є заголовок покрокових опцій (Hop-by-hop Options). Як і у випадку опцій IPv4, опції додаткового заголовка покрокових опцій IPv6 обробляються центральним процесором маршрутизатора. Переміщення в такий заголовок великого числа опцій невизначеного типу буде сповільнювати роботу маршрутизатора IPv6.

Звичайна практика боротьби з цією атакою – фільтрація (відкидання) всіх пакетів, в заголовку яких є опції. Можливо також ігнорування всіх або деяких опцій.

6.4.2. 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). Цей спосіб атаки вже був згаданий при описі атаки Пінг смерті. Максимальне значення зміщення фрагмента рівне $(2^{13} – 1)×8 = 8191×8 = 65\ 528$. Так як максимальна довжина IP-пакету дорівнює 65 535 байт, очевидно, що останній фрагмент не повинен мати довжину більше 7 байт. Ставлячи фрагмент з максимальним зсувом і розміром в 8 і більше байтів, зловмисник переповнює буфер ядра ОС, що може призвести до падіння ОС.
- **Перекриття сегментів за рахунок спеціального підбору зсувів і довжин фрагментів**. Деякі ОС не справляються зі складанням таких пакетів і падають. Наприклад, ця вразливість використовується в атаці Teardrop.
- **Заміщення фрагментів**. Ця DoS-атака використовується для обману таких захисних засобів, як фаєрволи і системи виявлення вторгнень. Пакети атаки фрагментуються і надсилаються разом з фрагментами-дублікатами, в яких міститься нешкідлива інформація. Першим надсилається нешкідливий фрагмент, а потім – фрагмент, що містить код

атаки, але з такими ж зміщенням і довжиною. В результаті фрагмент атаки заміщає нешкідливий фрагмент. Не всі фаєрволи і системи виявлення вторгнень розпізнають фрагментовану таким чином атаку.

- **Незавершені фрагменти**. Ця DoS-атака спрямована на вичерпання буферів збірки фрагментів. Атакуючий надсилає велику кількість малих фрагментів, по парі на кожен пакет, що збирається. Перший фрагмент з пари надсилається з нульовим зміщенням, другий – з максимальним, тому вони займають максимальний обсяг пам'яті, що відводиться під буфер. При відправці великого числа таких фрагментів за час тайм-ауту збірки вся пам'ять ядра ОС, що відводиться під складання пакетів, виявляється вичерпаною, в результаті настає відмова в обслуговуванні фрагментованих пакетів.

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. Наприклад, сучасні ОС при використанні протоколу IPv6 запобігають перевищенню максимальної довжини результуючого сегмента.

6.5. Мережева розвідка

6.5.1. Завдання і різновиди мережевої розвідки

Як можна побачити з опису атак на мережеву транспортну інфраструктуру, багато з них вимагають попередніх знань про атаковані мережі і її хости. Наприклад, для проведення ICMP-атаки Smurf потрібно знайти проміжну мережу з великою кількістю хостів, що відповідають на ехо-запити, при цьому така мережа повинна бути досяжна для пакетів, які будуть надіслані з мережі зловмисника з широкотрансляційною адресою цієї мережі; ну і зрозуміло, повинна бути відома IP-адреса атакованого комп'ютера. Для атаки ICMP/UDP-затопленням потрібно знати адреси хостів проміжної мережі, а також номери пасивних портів цих хостів; для атаки ICMP/chargen/echo-затопленням – адреси хостів проміжної мережі з активними портами 7 і 19 і т. д.

Якщо зловмисник хоче задіяти мережу ботів, заражених вірусом певного типу, то йому потрібно буде просканувати велику кількість комп'ютерів на відгук по певному порту, який використовується цим вірусом для отримання команд від контролера атаки. Справа в тому, що віруси намагаються поширитися на якомога більшу кількість комп'ютерів, але заздалегідь не можна сказати, чи буде успішним таке впровадження для якогось певного хоста, – це залежить від

конфігурації засобів захисту та інших параметрів ОС хоста. Тому зловмисник заздалегідь не знає, які хости він може використовувати в якості членів мережі ботів, навіть якщо це він ініціював поширення цього вірусу. А можливо, він просто вирішить скористатися відомим вірусом, поширеним іншими особами, і тому йому потрібно зібрати відомості про заражені комп'ютери.

Тому майже 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.

6.5.2. Сканування мережі

Виявлення IP-адрес активних хостів мережі називають **скануванням мережі** (Network Scanning), а активних і пасивних портів – **скануванням портів** (Port Scanning). Сам термін «сканування» говорить про те, що зловмисник тестує один за одним всі можливі значення IP-адрес деякої підмережі (наприклад, для підмережі з маскою /24 це 254 значення) або номера портів (65 535 для TCP і стільки ж для UDP).

Для сканування мережі та портів використовуються більш витончені засоби, ніж утиліта ping або стандартна процедура встановлення TCP-з'єднання, які легко блокуються фаєрволами.

Найбільш поширеними прийомами сканування мережі є:

Пінг TCP SYN до одного з публічно доступних портів, найчастіше до порту 80 (порт веб-сервера), який з великим ступенем ймовірності (але, звичайно, не обов'язково) відкритий для зовнішнього доступу. Якщо хост відповідає пакетом *SYN/ACK*, то сканер вважає, що хост активний, і завершує TCP-з'єднання пакетом з ознакою *RST*.

Пінг TCP АСК дозволяє в багатьох випадках обійти брандмауер, якщо той блокує обраний порт. Звичайною практикою конфігурації брандмауера є дозвіл трафіку вже встановлених TCP-з'єднань, а ознакою приналежності пакета до такого з'єднанню є наявність встановленого прапора АСК. У тому випадку, коли пінг TCP SYN до деякого порту не проходить, а TCP АСК проходить, сканер вважає, що даний хост активний, але захищений файерволом, – така інформація може бути цінною для зловмисника.

Пінг UDP. На тестований хост направляється UDP-пакет з номером порту, який, як розраховує зловмисник, з великим ступенем ймовірності є пасивним. У тому випадку, коли комп'ютер включений і цей порт пасивний, сканер отримує

у відповідь ICMP-повідомлення про недоступність порту; якщо ж комп'ютер відключений, то зловмисник отримує повідомлення від маршрутизатора про недоступність хоста.

Пінг ICMP. Адміністратори мереж найчастіше блокують ехо-запити протоколу ICMP, однак для перевірки активності хоста зловмисник може використовувати інші типи ICMP-запитів, наприклад запит про довжину маски IP-адреси (код 17) або запит синхронізації часу протоколу ICMP (код 13).

Пінг IP. На досліджуваний комп'ютер направляється IP-пакет з кодом протоколу, що відрізняється від кодів протоколів TCP, UDP і ICMP. Швидше за все, такий тип протоколу не підтримується стеком TCP/IP на тестованому комп'ютері, і в тому випадку, якщо хост активний, у відповідь повернеться ICMP-повідомлення про недосяжність протоколу.

6.5.3. Сканування портів

Дуже схожі методи застосовуються і для сканування портів. Тут перевага віддається SYN-скануванню протоколу TCP, так як це найшвидший спосіб, що в даному випадку має значення, адже на відміну від сканування хостів тут перевіряються десятки тисяч портів (по 65 535 портів для TCP і UDP). Сканування портів часто здійснюється за допомогою тих же спеціалізованих програмних засобів, що і для інвентаризації мережі та аудиту її захищеності.

Сканування мережі і портів зазвичай не проходить непоміченим – дуже ймовірно, що засоби протоколювання подій ОС і фаєрволів зафіксують цей процес, і адміністратор сканованої мережі почне розслідувати інцидент. І перше питання, що виникає при цьому: з якої адреси виконувалося сканування? Щоб уникнути розкриття, зловмисники часто використовують спуфінг IP-адреси при атаках. На перший погляд здається, що в мережевій розвідці цей прийом не може спрацювати, так як зловмисникові потрібно отримувати відповіді на свій комп'ютер, інакше він не може отримувати інформацію. Проте спуфінг IP-адреси можливий і при скануванні. Одним із прийомів є маскування його серед безлічі інших адрес. В цьому випадку тестові скануючі пакети відправляються з дійсної IP-адреси поряд з безліччю таких же пакетів, але з підробленими адресами. Розрахунок тут на те, що під час розслідування факту сканування важко буде встановити, хто був справжнім організатором сканування, а кого просто використовували як прикриття. Ще більш витонченим є так зване порожнє сканування, коли істинна адреса ніколи не вказується, а результати сканування зловмисники намагаються зрозуміти по реакції третього комп'ютера, чию адресу підробляється.

6.6. Атаки на DNS

6.6.1. DNS-спуфінг

У **DNS-спуфінг атаці** DNS є не метою, а засобом (рис. 6.5). Нехай зловмисник намагається отримати доступ до корпоративного сервера www.example.com. Для цього йому потрібні автентифікаційні дані будь-якого його клієнта.

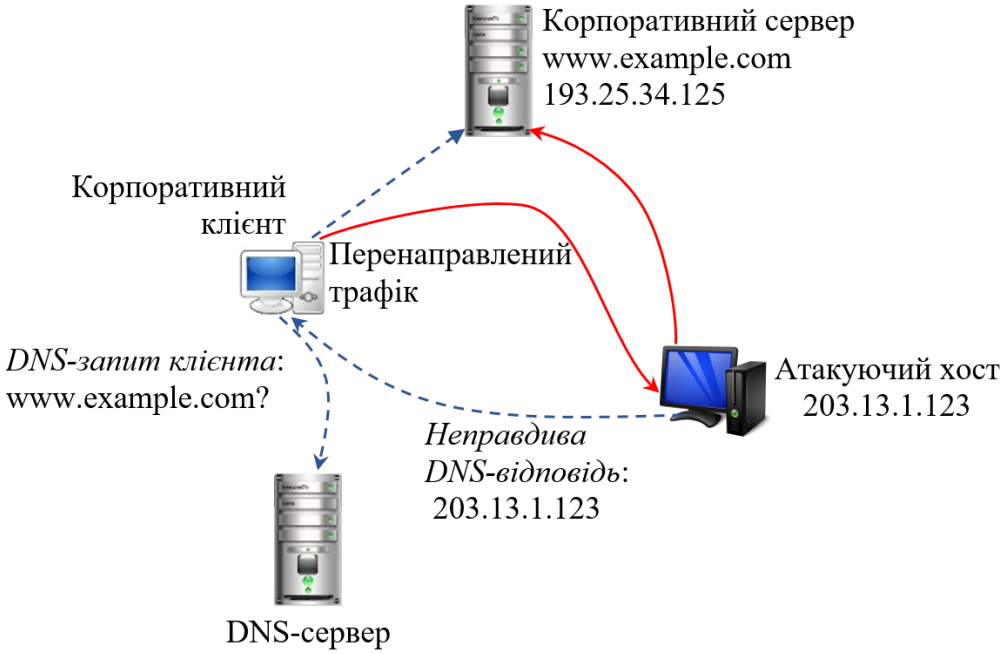


Рис. 6.5. Схема перенаправлення трафіку з використанням неправдивих DNS-відповідей

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). На шляху реалізації цього плану є кілька серйозних перешкод.

Перш за все, необхідно затримати відповідь DNS-сервера, наприклад, піддавши його DoS-атаці. Інша проблема пов'язана з визначенням номера порта DNS-клієнта, який необхідно вказати в заголовку пакета, щоб дані дійшли до додатка, так як якщо серверна частина DNS має постійно закріплений за нею номер порту 53, то клієнтська частина протоколу DNS отримує номер порту динамічно при запуску, причому операційна система вибирає його з досить

широкого діапазону. Цю задачу зловмисник вирішує шляхом прямого перебору всіх можливих номерів. Також шляхом перебору можливих значень зловмисник долає проблему визначення ідентифікаторів DNS-повідомлень. Ці ідентифікатори передаються в DNS-повідомленнях і використовуються для того, щоб DNS-клієнт міг встановити відповідність отриманих відповідей надісланим запитам. Отже, зловмисник бомбардує клієнтську машину неправдивими DNS-відповідями, перебираючи всі можливі значення ідентифікуючих полів так, щоб клієнт в кінці кінців прийняв один з них за істинну DNS-відповідь. Як тільки це відбудеться, мета зловмисника стане досягнутою – пакети від клієнта направляються на адресу атакуючого хоста, зловмисник отримує в своє розпорядження ім'я і пароль легального користувача, а з ними і доступ до корпоративного сервера.

6.6.2. 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. Ця атака ефективніша, ніж DNS-спуфінг, так як, будучи успішною вона впливає на велику кількість клієнтів протягом тривалого часу (часу життя підробленого запису в кеші). Атаку отруєнням кешу DNS ілюструє рис. 6.6.

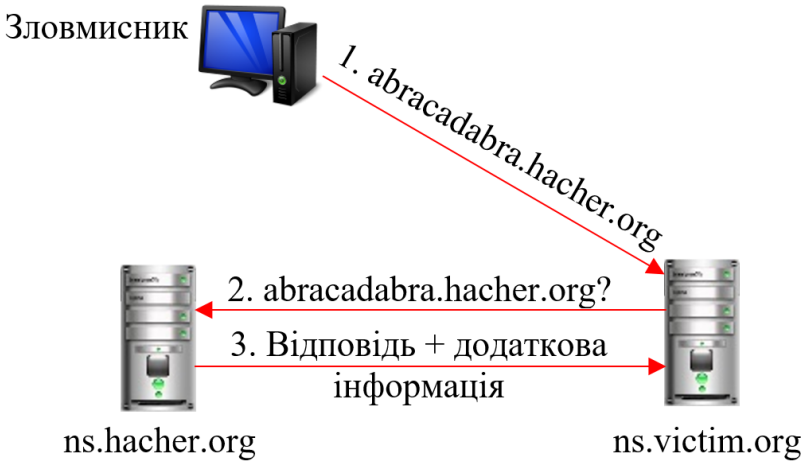


Рис. 6.6. Загальна схема отруєння кешу DNS

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).

DNS-сервер зони ns.hacker.org знаходиться під контролем зловмисника. У відповідь на запит неіснуючого імені він відправляє особливим чином сформовану відповідь. Основне поле відповіді, куди поміщається запис про відповідність імені IP-адресі, зазвичай залишається порожнім (воно в атаці не використовується), а ось в поле додаткової інформації хакер поміщає запис, який і повинен отруїти сервер ns.victim.org. Наприклад, це може бути запис про деякий хост, який не належить до зони victim.org, тому сервер його кешує і надалі використовує при запитах своїх клієнтів. Це може бути і запис, в якому замість імені легітимного DNS-сервера деякого домену aaa.com вказано ім'я DNS-сервера хакера, - в цьому випадку всі запити клієнтів сервера ns.victim.org до хостів домену aaa.com будуть направлятися DNS-серверу хакера.

Атаки отруєнням DNS-кешу носять історичний характер, так як в сучасних програмних реалізаціях BIND DNS-сервер не кешує інформацію, якщо вона безпосередньо не відноситься до запиту (як в даному прикладі) або виходить за межі зони, для якої відповідаючий сервер є повноважним.

6.6.3. Атаки на кореневі DNS-сервери

Найбільш потужними і відчутними за своїми наслідками були дві DDoS-атаки на кореневі сервери, що трапилися 21 жовтня 2002 року і 6/7 лютого 2007 року.

Подробиці **атаки 21 жовтня 2002 року** наводяться в звіті фахівців, що адмініструють 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.

Служба DNS показала хорошу стійкість до атаки – користувачі помічали тільки невелике збільшення часу очікування при відкритті сайту в браузері; всі кореневі сервери продовжували працювати, і на всі вжиті ними запити були

видані відповіді, але через перевантаження вхідних інтерфейсів деяких серверів не всі запити були прийняті. Після цієї атаки були проведені додаткові роботи по підвищенню стійкості служби DNS, які включали підвищення швидкості інтерфейсів і ліній зв'язку, що з'єднують кореневі сервери з Інтернетом, і збільшення числа кореневих серверів. Крім того, кореневі сервери були більш рівномірно розподілені по автономних системах і географічних регіонах.

Атака 6/7 лютого 2007 року тривала 24 години (тому в назві фігурують дві дати). Ця атака була набагато потужнішою, ніж атака 21 жовтня 2002 року, інтенсивність трафіку досягала 1 Гбіт/с на один пул кореневих серверів, але атаковано було тільки чотири з них. В атаці було використано 4500-5000 комп'ютерів під управлінням Microsoft Windows, причому члени цієї мережі ботів були розподілені по мережах кількох країн. При атаці мало місце затоплення кореневих серверів UDP-пакетами, спрямованими на порт 53 (порт DNS), тобто атака відносилась до типу UDP-затоплення, а використання порту 53 допомагало пакетам дістатися до серверів, так як у фаєрволів, що захищають DNS-сервери цей порт завжди відкритий, інакше сервер не зміг би виконувати свою роботу. Атака привела до майже повного вичерпання пропускної спроможності двох з чотирьох атакованих пулів серверів, в той час як інші два постраждали не так істотно і могли відповідати на більшу частину запитів.

Атака практично негайно була виявлена центрами, відповідальними за адміністрування атакованих пулів кореневих серверів (по попереджуючим повідомленням самих серверів і даним хостів, що виконують постійний моніторинг кореневих серверів шляхом відправки на них контрольних запитів). Для зниження ефекту атаки було вжито низку заходів, першим з яких було блокування будь-яких DNS-запитів, довжина яких перевищувала 300 байт, так як, зазвичай, DNS-запит не перевищує 100 байт, а в атакуючих повідомленнях для посилення ефекту затоплення розміри полів даних UDP-потоку доходили до 1023 байт. Однак таке блокування допомогло лише частково, так як подальший аналіз показав, що розмір поля даних трафіку атаки змінювався випадковим чином від 0 до 1023 байт. Аналіз атаки також показав, що атакуючі комп'ютери не використали спуфінг IP-адрес, що дало можливість відстежити розміщення ботів (в процентному відношенні): Південна Корея - 65%, США - 19%, Канада - 3,5%, Китай - 2,5 %, решта країн - 10%. Хост, який координував атаку, перебував в США, хости мережі ботів зверталися до нього по протоколу HTTP.

Причини атаки так і залишилися нез'ясованими; в звіті **ICANN** (Internet Corporation for Assigned Names and Numbers – Інтернет корпорація з присвоєння імен та номерів) передбачається, що це могло бути просто марнославство хакерів, так як спроба зупинити весь Інтернет є викликом для будь-якого хакера.

Розглянуті атаки дають хороше уявлення про масштаби сучасних DDoS-атак і про те, що захиститися від них дуже складно навіть таким досвідченим фахівцям, які обслуговують кореневі DNS-сервери. Таке архітектурне рішення, як віртуалізація серверів, коли логічний сервер представлений великим пулом фізичних серверів, розосереджених по різних мережах і автономних системах, є дуже потужним фактором, що гасить ефект навіть дуже інтенсивної DDoS-атаки.

6.6.4. DDoS-атаки відбиття від DNS-серверів

Основна ідея атаки відбиття в даному випадку полягає в наступному. 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.

Розглянемо схему атаки такого роду на прикладі атаки, якій в березні 2013 року піддався веб-сервер компанії Spamhouse – некомерційної організації, що бореться зі спамом. Загальна схема атаки зображена на рис. 6.7. 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.

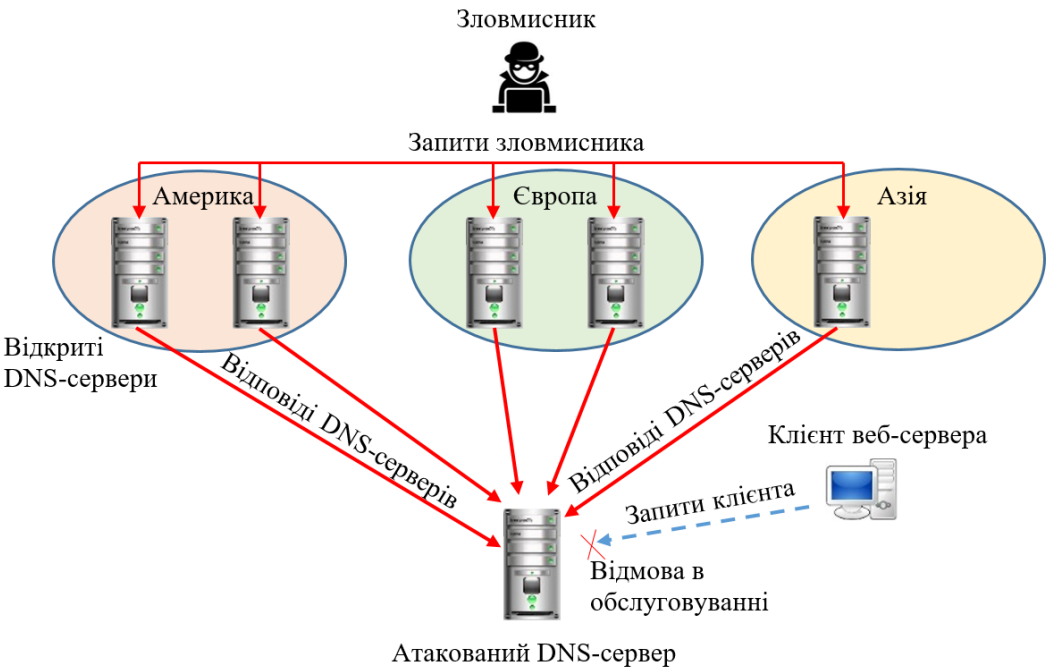


Рис. 6.7. Атака відбиття від DNS-серверів

Рекурсивний режим тут є важливим елементом атаки, так як нерекурсивні DNS-сервери тільки перенаправляють запити користувача на інший DNS-сервер, тому їх відповідь є короткою і не може підсилити атаку. Загальною практикою є

підтримка рекурсивного режиму відповідей тільки для «своїх» клієнтів – співробітників підприємства для корпоративного DNS-сервера або ж передплатників сервісу для інтернет-провайдера. Проте в Інтернеті працює близько 28 мільйонів відкритих рекурсивних DNS-серверів, так що знайти такі сервери для атаки не так вже й складно.

Зловмисником був посланий потік запитів на 30000 відкритих DNS-серверів. У запитах в якості адреси відправника зловмисник вказував адресу атакованого веб-сервера. Таким чином, усі відповіді від 30000 DNS-серверів обрушилися на веб-сервер компанії Spamhouse.

Для посилення атаки використовувалися не звичайні запити на розв'язання імені, а запити на передачу об'ємного файлу з усіма записами зони ripe.net (RIPE NCC – це регіональний інформаційний інтернет-центр по Європі). Файл зони ripe.net має розмір близько 3000 байт, так що при розмірі запиту в 28 байт коефіцієнт посилення склав близько 100. Таке потужне посилення дозволило створити атаку із загальною інтенсивністю в 75 Гбіт/с, використовуючи потік запитів до одного DNS-сервера інтенсивністю всього в 2,5 Мбіт/с. Для окремого DNS-сервера такий потік запитів не є чимось незвичайним, так що власники цих серверів, швидше за все, цю атаку не помітили, а от результуючий потік атаки в 75 Гбіт/с вивів веб-сервер компанії Spamhouse з ладу.

Точніше, веб-сервер Spamhouse був виведений з ладу тільки до певного моменту, поки його власники не перевели його «під крило» CloudFlare – провайдера хмарних сервісів, який до того ж, спеціалізується на захисті від DDoS-атак. Перевід допоміг, так як розподілена віртуальна структура CloudFlare, яка використовує техніку anycast і фаєрволи, змогла абсорбувати велику частину трафіку атаки, і веб-сервер Spamhouse знову став доступний користувачам Інтернету.

6.6.5. 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.

6.7. Технології захищеного каналу

6.7.1. Способи утворення захищеного каналу

Відомо, що задачу захисту даних можна розділити на дві підзадачі: захист даних всередині комп'ютера і захист даних в процесі їх передачі від одного комп'ютера до іншого. Для забезпечення безпеки даних при їх передачі по публічних мережах використовуються різні технології 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. 6.8, а);
- схема з обладнанням постачальника послуг публічної мережі, розташованим на межі між приватною і публічною мережами (рис. 6.8, б).

У першому випадку захищений канал утворюється програмними засобами, встановленими на двох віддалених комп'ютерах, що належать двом різним

локальним мережам одного підприємства і пов’язаних між собою через публічну мережу. Перевагою цього підходу є повна захищеність каналу вздовж усього шляху прямування, а також можливість використання будь-яких протоколів створення захищених каналів, щоб лише на кінцевих точках каналу підтримувався один і той же протокол. Недоліки полягають в надмірності і децентралізованості рішення. Надмірність полягає в тому, що навряд чи варто створювати захищений канал на всьому шляху проходження даних: вразливими для зловмисників, зазвичай, є мережі з комутацією пакетів, а не канали телефонної мережі або виділені канали, через які локальні мережі підключені до територіальної мережі. Тому захист каналів доступу до публічної мережі можна вважати надмірним. Децентралізація полягає в тому, що для кожного комп’ютера, до якого потрібно надати послуги захищеного каналу, необхідно окремо встановлювати, конфігурувати і адмініструвати програмні засоби захисту даних. Підключення кожного нового комп’ютера до захищеного каналу вимагає виконувати ці трудомісткі операції заново.

Рис. 6.8. Схеми утворення захищеного каналу

У другому випадку клієнти і сервери не беруть участі в створенні захищеного каналу – він прокладається тільки всередині публічної мережі з комутацією пакетів, наприклад всередині Інтернету. Так, канал може бути прокладений між сервером віддаленого доступу постачальника послуг публічної

мережі і прикордонним маршрутизатором корпоративної мережі. Це добре масштабоване рішення, кероване централізовано адміністраторами як корпоративної мережі, так і мережі постачальника послуг. Для комп'ютерів корпоративної мережі канал прозорий – програмне забезпечення цих кінцевих вузлів залишається без змін. Такий гнучкий підхід дозволяє легко утворювати нові канали захищеної взаємодії між комп'ютерами незалежно від місця їх розташування. Реалізація цього підходу складніша - потрібен стандартний протокол утворення захищеного каналу, потрібно встановлювати у всіх постачальників послуг програмне забезпечення, що підтримує такий протокол, необхідна підтримка протоколу виробниками прикордонного комунікаційного обладнання. Однак варіант, коли підтримку захищеного каналу бере на себе постачальник послуг публічної мережі, залишає сумніви в надійності захисту: по-перше, незахищеними виявляються канали доступу до публічної мережі, по-друге, споживач послуг відчуває себе в повній залежності від надійності постачальника послуг.

6.7.2. Ієрархія технологій захищеного каналу

Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі OSI (табл. 6.1).

Таблиця 6.1. Протоколи, які формують захищений канал на різних рівнях моделі OSI

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		

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. У той же час додатки при цьому стають залежними від конкретного протоколу захищеного каналу, так як в них повинні бути вбудовані явні виклики функцій цього протоколу.

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. При такому підході для кожної служби необхідно розробляти власну захищену версію протоколу.

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. При цьому не має значення, пакет якого протоколу, в свою чергу, упакований в даному PPP-кадрі: IP, IPX, SNA або NetBIOS. З одного боку, це робить сервіс PPTP досить універсальним, так як клієнт сервісу захищеного каналу може задіяти будь-які протоколи в своїй мережі. З іншого боку, така схема висуває жорсткі вимоги до типу протоколу канального рівня, що використовується на ділянці доступу клієнта до захищеного каналу, – для протоколу PPTP таким протоколом може бути тільки PPP. Хоча протокол PPP дуже поширений в каналах доступу, сьогодні конкуренцію йому складають протоколи Gigabit Ethernet і Fast Ethernet, які все частіше працюють не тільки в локальних, але і в глобальних мережах.

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.).

6.7.3. Протокол SSL

SSL (Secure Sockets Layer — рівень захищених сокетів) — криптографічний протокол, який забезпечує встановлення безпечного з’єднання між клієнтом і сервером.

Протокол SSL розроблений компанією Netscape Communications в 1995 році. В 1999 році, на основі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC 2246, який отримав ім’я TLS.

Протокол SSL забезпечує конфіденційність обміну даними між клієнтом і сервером, які використовують стек TCP/IP. Для шифрування використовується асиметричний алгоритм з відкритим ключем.

Протокол SSL передбачає наступні етапи взаємодії клієнта і сервера при формуванні і підтримці захищеного з'єднання:

- встановлення SSL-сесії;
- захищена взаємодія.

Процедура встановлення SSL-сесії, звана також **процедурою рукостискання**, відпрацьовується перед безпосереднім захистом інформаційного обміну і виконується по **протоколу початкового вітання** (Handshake Protocol), що входить до складу протоколу SSL.

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.

На цьому рукостискання завершується, і починається **захищена взаємодія**, яка зашифровується і розшифровується за допомогою ключових даних. Якщо будь-яка з перерахованих вище дій не вдається, то рукостискання SSL не відбулось, і з'єднання не створюється.

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.

При встановленні повторних з'єднань між клієнтом і сервером сторони можуть, за взаємною угодою, формувати нові сеансові ключі на основі «старого» загального «секрету» (ця процедура називається «продовженням SSL сесії»).

Автентифікація сторін

Взаємна автентифікація обох сторін в SSL виконується шляхом обміну цифровими сертифікатами відкритих ключів користувачів (клієнта і сервера),

завіреними цифровим підписом спеціальних сертифікаційних центрів. Протокол SSL підтримує сертифікати, що відповідають загальноприйнятому стандарту X.509, а також стандарти інфраструктури відкритих ключів PKI (Public Key Infrastructure), за допомогою якої організовується видача і перевірка достовірності сертифікатів.

Цифрові сертифікати в основному служать двом цілям:

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

Цифровий сертифікат випускається перевіреною повноважною організацією – Центром сертифікації (Certificate Authority, CA) і видається тільки на обмежений час. Після закінчення терміну дії сертифікату його необхідно замінити. Протокол SSL використовує цифрові сертифікати для обміну ключами, автентифікації серверів і, при необхідності, автентифікації клієнтів.

Підключення по SSL завжди ініціюється клієнтом викликом URL-адреси, що починається з https:// замість http://.

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. Наприклад, такий сертифікат можна отримати від компанії VeriSign. Щоб отримати сертифікат, підписаний Центром, необхідно надати йому достатньо інформації, щоб він зміг перевірити особу пред’явника. Тоді Центр створить новий сертифікат, підпише його і доставить його вам. Популярні Web-браузери заздалегідь налагоджені довіряти сертифікатам, виданим певними Центрами, так що не потрібно додаткової конфігурації для підключення клієнта через SSL до сервера, для якого був виданий сертифікат.

Самопідписаний сертифікат – це сертифікат, створений самим користувачем. При використанні такого сертифікату видавець співпадає з власником сертифікату. Зручність такого рішення в тому, що для створення самопідписаного сертифікату треба менше часу, ніж для отримання сертифікату, підписаного Центром сертифікації. Проте самопідписаний сертифікат вимагає, щоб будь-який клієнт, який підключається по SSL до сервера, встановив такий сертифікат на сервері і налаштував його довіряти підписнику сертифікату. Самопідписані сертифікати корисні тільки тоді, коли кожного клієнта, що взаємодіє з сервером, можна налаштувати так, щоб він довіряв цьому сертифікату.

В загальному, «порожні» сертифікати містять фіктивну інформацію, яку використовують як тимчасове рішення для налаштування SSL і перевірки його функціонування в конкретному середовищі. Додаток ISC надає «порожній» сертифікат разом з ключами і файлами довірених джерел для сервера і клієнта.

Після того, як сертифікат був отриманий, необхідно встановити його достовірність (автентифікувати). У протоколі SSL є два типи автентифікації :

- автентифікація на стороні клієнта;
- автентифікація на стороні сервера.

SSL-автентифікація сервера дозволяє клієнтові перевірити достовірність сервера. Клієнтське ПЗ з підтримкою SSL, може за допомогою стандартних прийомів криптографії з відкритим ключем, перевірити, що сертифікат сервера і відкритий ключ дійсні і були видані Центром, що знаходиться в списку довірених Центрів сертифікації цього клієнта. Це підтвердження може бути важливим, якщо користувач, наприклад, відправляє номер кредитної карти по мережі і хоче перевірити достовірність сервера-одержувача.

SSL-автентифікація клієнта дозволяє серверу перевірити особу користувача. Використовуючи ті ж прийоми, що і у випадку з автентифікацією сервера, серверне ПЗ з підтримкою SSL може перевірити, що сертифікат клієнта і відкритий ключ дійсні і були видані Центром сертифікації, наявним в списку довірених Центрів сервера. Це підтвердження може бути важливим, якщо, наприклад, сервер – це банк, що відправляє конфіденційну фінансову інформацію замовникові, і він хоче перевірити особу одержувача.

Методи обміну ключами

Головна мета процесу обміну ключами – це створення **головного секретного коду** (pre-master secret), який відомий тільки клієнту і серверу. Головний секретний код необхідний для того, щоб створити повідомлення для перевірки сертифіката, ключів шифрування, секрету MAC (Message Authentication Code) і повідомлення «finished». При надсиланні вірного повідомлення «finished», сторони доведуть тим самим, що вони знають вірний секрет (pre-master secret).

SSL визначає наступні методи обміну ключами, щоб встановити попередній головний секретний код:

- Анонімний обмін ключами;
- Обмін ключами при використанні RSA;
- Обмін ключами при використанні алгоритму Діффі-Хеллмана;

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. Відкритий ключ клієнт дізнається з повідомлення обміну ключами від сервера. Результат надсилається в повідомленні обміну ключами від клієнта. Оскільки перехоплювач не знає закритого ключа сервера, то йому буде неможливо розшифрувати секрет (pre-master secret). При використанні алгоритму Діффі-Хеллмана відкриті параметри сервера містяться в повідомленні обміну ключами від сервера, і клієнтові посилають в повідомленні обміну ключами. Перехоплювач, який не знає приватних значень, не зможе знайти секрет (pre-master secret).

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. Коли використовується тимчасовий ключ RSA, повідомлення обміну підписуються серверами RSA або сертифікатом DSS (Data Security Standard). Сигнатура включає поточне значення повідомлення Client_Hello.random, таким чином старі сигнатури і старі тимчасові ключі не можуть повторюватися. Сервер може використовувати тимчасовий ключ RSA тільки одного разу для створення сесії. Після перевірки сертифіката сервера клієнт шифрує секрет (pre-master secret) за допомогою відкритого ключа сервера. Після успішного декодування секрету (pre-master secret) створюється повідомлення «finished», тим самим сервер демонструє, що він знає приватний ключ, що відповідає сертифікату сервера.

Коли RSA використовується для обміну ключами, для автентифікації клієнта використовується повідомлення перевірки сертифіката клієнта. Клієнт підписується значенням, обчисленим з master_secret і всіх попередніх повідомлень протоколу рукостискання. Ці повідомлення рукостискання включають сертифікат сервера, який ставить у відповідність сигнатурі сервера, повідомлення Server_Hello.random, якому ставить у відповідність сигнатуру поточного повідомлення рукостискання.

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. Тимчасові параметри хешуються з повідомленням hello.random перед

підписанням, для того, щоб зловмисник не зміг здійснити повтор старих параметрів. У будь-якому випадку, клієнт може перевірити сертифікат або сигнатуру, для впевненості, що параметри належать сервера.

Якщо клієнт має сертифікат, що містить параметри алгоритму Діффі-Хеллмана, то сертифікат також має інформацію необхідну для того, щоб завершити обмін ключами. Параметри клієнта повинні бути сумісні з тими, які підтримує сервер для того, щоб працював обмін ключами.

Використання протоколу SSL призвело до формування протоколу **HTTPS** (Hypertext Transfer Protocol Secure), що підтримує шифрування. Дані, які передаються по протоколу HTTPS, «упаковуються» в криптографічний протокол SSL або TLS, тим самим забезпечуючи захист цих даних. Такий спосіб захисту широко використовується для додатків, в яких важлива безпека з'єднання, наприклад у платіжних системах. HTTPS підтримується всіма браузерами. На відміну від HTTP, для HTTPS за замовчуванням використовується TCP-порт 443.

Атаки проти протоколу SSL

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

- розкриття шифрів;
- атака «зловмисник посередині»;
- атака відбиттям;
- атака проти протоколу рукостискання.

Розкриття шифрів

Як відомо, SSL залежить від різних криптографічних параметрів. Шифрування з відкритим ключем RSA необхідне для пересилки ключів і автентифікації сервера/клієнта. Проте, в якості шифру використовуються різні криптографічні алгоритми. Таким чином, якщо здійснити успішну атаку на ці алгоритми, то SSL не може вже вважатися безпечним. Атака на певні комунікаційні сесії проводиться записом сесії, і потім, протягом довгого часу підбирається ключ сесії або ключ RSA. SSL ж робить таку атаку невигідною, так як витрачається велика кількість часу і грошей.

Атака «зловмисник посередині»

Також відома як MitM (Man-in-the-Middle) атака. Передбачає участь трьох сторін: сервера, клієнта і зловмисника, що знаходиться між ними. У даній ситуації 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. Однак така атака неможлива при використанні протоколу SSL, так як для перевірки автентичності джерела (зазвичай сервера) використовуються сертифікати, завірені центром сертифікації.

Атака буде успішною, якщо:

- Сервер не має підписаного сертифіката.
- Клієнт не перевіряє сертифікат сервера.
- Користувач ігнорує повідомлення про відсутність підпису сертифікату Центром сертифікації.

Атака відбиттям

Зловмисник записує комунікаційну сесію між сервером і клієнтом. Пізніше, він намагається встановити з'єднання з сервером, відтворюючи записані повідомлення клієнта. Але SSL відбиває цю атаку за допомогою особливого унікального ідентифікатора з'єднання (ІЗ). Теоретично третя сторона не в змозі передбачити ІЗ, оскільки він базується на наборі випадкових подій. Однак, зловмисник з великими ресурсами може записати велику кількість сесій і спробувати підібрати «правильну» сесію, ґрунтуючись на коді *nonce*, який надіслав сервер в повідомленні Server_Hello. Але коди *nonce* SSL мають, щонайменше, довжину 128 біт, а значить, зловмисникові необхідно записати 2^{64} кодів *nonce*, щоб отримати ймовірність вгадування 50%. Але 2^{64} досить велике число, що робить ці атаки безглуздими.

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. Для такої атаки зловмисникові необхідно швидко підмінити одне або більше повідомлень рукостискання. Якщо це відбувається, то клієнт і сервер обчислюють різні значення хеш-функцій в повідомленнях рукостискання. У результаті чого сторони не приймуть один від одного повідомлення «finished». Без знання секрету зловмисник не зможе виправити повідомлення «finished», тому атака може бути виявлена.

6.7.4. Протокол TLS

TLS (Transport Layer Security – протокол безпеки транспортного рівня) – криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі Інтернет.

TLS протокол побудований на основі протоколу Netscape SSL версії 3.0 і складається з двох частин – TLS Record Protocol і TLS Handshake Protocol.

Відмінності між SSL 3.0 і TLS 1.0 незначні. TLS надає можливості автентифікації і безпечної передачі даних через Інтернет з використанням криптографічних засобів. Часто відбувається лише автентифікація сервера, тоді як клієнт залишається неавтентифікованим. Для взаємної автентифікації кожна із сторін повинна підтримувати інфраструктуру відкритого ключа (PKI), яка дозволяє захистити клієнт-серверні додатки від перехоплення повідомлень, редагування існуючих повідомлень і створення підробних.

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.

Алгоритм процедури встановлення з'єднання по протоколу рукостискання

Клієнт і сервер, що працюють по протоколу TLS, встановлюють з'єднання, використовуючи процедуру рукостискання (Handshake). Протягом процедури рукостискання клієнт і сервер приймають угоду відносно параметрів, що будуть використовуватись для встановлення захищеного з'єднання.

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.

Нижче описаний простий приклад встановлення з'єднання :

1. Клієнт посилає повідомлення **ClientHello**, вказуючи останню версію підтримуваного TLS протоколу, випадкове число і список підтримуваних методів шифрування і стискання, що сумісні для роботи з TLS.
2. Сервер відповідає повідомленням **ServerHello**, що містить вибрану сервером версію протоколу, випадкове число надіслане клієнтом, відповідний алгоритм шифрування і стискання із списку наданого клієнтом.
3. Сервер надсилає повідомлення **Certificate**, яке містить цифровий сертифікат сервера (залежно від алгоритму шифрування цей етап може бути пропущений).
4. Сервер може запитати сертифікат у клієнта, у такому разі з'єднання буде взаємно автентифікованим.
5. Сервер надсилає повідомлення **ServerHelloDone**, що ідентифікує закінчення процедури рукостискання.
6. Клієнт відповідає повідомленням **ClientKeyExchange**, яке містить відкритий ключ pre-master secret або нічого (знову ж таки залежить від алгоритму шифрування).
7. Клієнт і сервер, використовуючи ключ pre-master secret і випадково згенеровані числа, обчислюють загальний секретний ключ. Уся інша інформація про ключ буде отримана із загального секретного ключа (згенерованих і клієнтом і сервером випадкових значень).
8. Клієнт надсилає повідомлення **ChangeCipherSpec**, яке вказує на те, що вся наступна інформація буде зашифрована, встановленим в процесі Handshake алгоритмом, використовуючи загальний секретний ключ.
9. Клієнт надсилає повідомлення **Finished**, яке містить хеш-функцію і код автентичності повідомлення (Message Authentication Code, MAC), згенеровані на основі попередніх повідомлень Handshake.
10. Сервер намагається розшифрувати **Finished**-повідомлення клієнта і перевірити хеш і MAC. Якщо процес розшифровки або перевірки не вдається, Handshake вважається невдалим, і з'єднання має бути обірване.

11. Сервер надсилає повідомлення **ChangeCipherSpec** і зашифроване повідомлення **Finished**, і у свою чергу клієнт теж виконує розшифрування і перевірку.

З цього часу процедура рукостискання вважається завершеною, протокол встановленим. Усі дані в наступних пакетах будуть передаватись в зашифрованому виді.

6.7.5. Протокол IPSec

Розподіл функцій між протоколами IPSec

Протокол IPSec в стандартах Інтернету називають системою. IPSec – це погоджений набір відкритих стандартів, що має сьогодні цілком окреслений ядро, яке в той же час може бути досить просто доповненое новими функціями і протоколами.

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.

Як видно з короткого опису функцій, можливості протоколів AH і ESP частково перекриваються (табл. 6.2). У той час як AH відповідає тільки за забезпечення цілісності і автентифікації даних, ESP може шифрувати дані і, крім того, виконувати функції протоколу AH (хоча автентифікація і цілісність забезпечуються ним в дещо скороченому вигляді). ESP може підтримувати функції шифрування і автентифікації/цілісності в будь-яких комбінаціях, тобто або всю групу функцій, або тільки автентифікацію/цілісність, або тільки шифрування.

Поділ функцій захисту між протоколами AH і ESP викликано застосовуваною у багатьох країнах практикою обмеження експорту і/або імпорту засобів, що забезпечують конфіденційність даних шляхом шифрування. Кожен з цих протоколів може використовуватися як самостійно, так і одночасно з іншим, так що в тих випадках, коли шифрування через діючі обмеження застосовувати

не можна, систему можна постачати тільки з протоколом AH. Подібний захист даних у багатьох випадках виявляється недостатнім. Приймаюча сторона отримує лише можливість перевірити, що дані були відправлені саме тим вузлом, від якого вони очікуються, і дійшли в тому вигляді, в якому були відправлені. Однак від несанкціонованого перегляду даних на шляху їх просування по мережі протокол AH захистити не може, тому що не шифрує їх. Для шифрування даних необхідний протокол ESP.

Таблиця 6.2. Розподіл функцій між протоколами IPSec

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

Безпечна асоціація

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. 6.9), яке в стандартах IPSec носить назву **безпечної асоціації** (Security Association, **SA**).

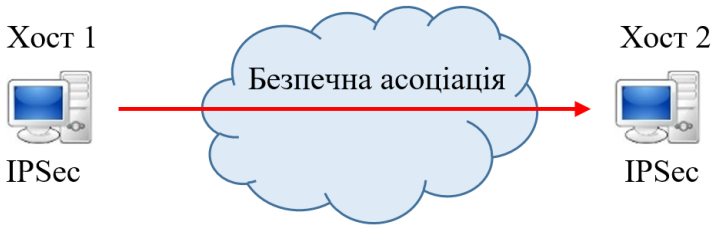


Рис. 6.9. Безпечна асоціація

Стандарти IPSec дозволяють кінцевим точкам захищеного каналу використовувати єдину безпечну асоціацію для передачі трафіку всіх взаємодіючих через цей канал хостів або створювати для цієї мети довільне число безпечних асоціацій, наприклад по одній на кожне TCP-з'єднання. Це дає можливість вибирати потрібну ступінь деталізації захисту – від однієї загальної

асоціації для трафіку безлічі кінцевих вузлів до індивідуально налаштованих асоціацій для захисту кожної програми.

Безпечна асоціація в протоколі IPSec являє собою односпрямоване (симплексне) логічне з'єднання, тому, якщо потрібно забезпечити безпечний двосторонній обмін даними, необхідно встановити дві безпечні асоціації. Ці асоціації в загальному випадку можуть мати різні характеристики: наприклад, в одну сторону при передачі запитів до бази даних досить лише автентифікації, а для зворотних даних, що несуть цінну інформацію, додатково можна забезпечити конфіденційність.

Встановлення безпечної асоціації починається зі взаємної автентифікації сторін, тому що всі заходи безпеки втрачають сенс, якщо дані передаються або приймаються не тією особою або не від тієї особи. Параметри SA визначають, який з двох протоколів, AH або ESP, буде застосовуватися для захисту даних, які функції буде виконувати протокол (наприклад, можна виконувати тільки автентифікацію і перевірку цілісності, а можна, крім того, ще й забезпечувати конфіденційність). Дуже важливими параметрами безпечної асоціації є також секретні ключі, що використовуються в роботі протоколів AH і ESP.

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. 6.10). Це робить протокол IPSec дуже гнучким засобом.

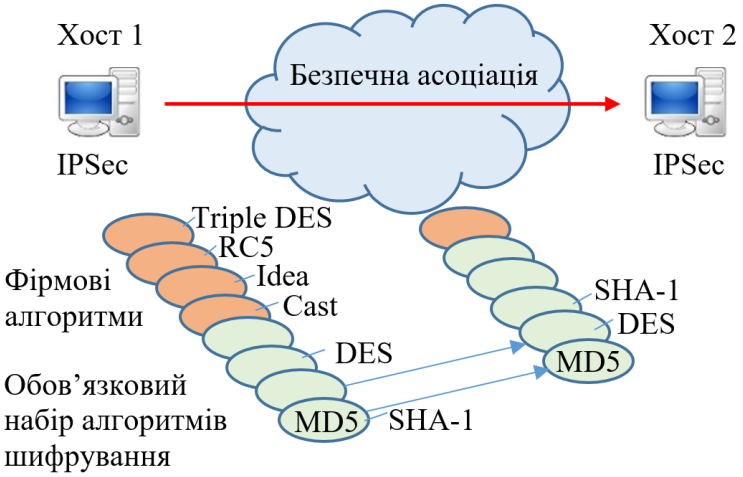


Рис. 6.10. Узгодження параметрів в протоколі ESP

Для забезпечення сумісності в стандартній версії IPSec визначено певний обов'язковий «інструментальний» набір; зокрема, для автентифікації даних завжди може бути використана одна з стандартних дайджест-функцій MD5 або SHA-1, а в число алгоритмів шифрування неодмінно входить DES. При цьому виробники продуктів, в яких використовується IPSec, можуть розширювати протокол шляхом включення інших алгоритмів автентифікації і симетричного шифрування. Наприклад, багато реалізацій IPSec підтримують популярний алгоритм шифрування Triple DES, а також порівняно нові алгоритми: Blowfish, Cast, CDMF, Idea, RC5.

Транспортний і тунельний режими

Протоколи AH і ESP можуть захищати дані в двох режимах: транспортному і тунельному. У **транспортному режимі** передача IP-пакета через мережу виконується за допомогою оригінального заголовка цього пакета, а в **тунельному режимі** вихідний пакет поміщається в новий Р-пакет, і передача даних по мережі виконується на підставі заголовка нового IP-пакету.

Застосування того чи іншого режиму залежить від вимог, що висуваються до захисту даних, а також від ролі, яку відіграє в мережі вузол, що завершає захищений канал. Так, вузол може бути хостом (кінцевим вузлом) або шлюзом (проміжним вузлом). Відповідно є три схеми застосування протоколу IPSec:

- хост-хост;
- шлюз-шлюз;
- хост-шлюз.

У схемі хост-хост захищений канал, або, що в даному контексті одне і те ж, безпечна асоціація, встановлюється між двома кінцевими вузлами мережі (рис. 6.9). Тоді протокол IPSec працює на кінцевих вузлах і захищає дані, що передаються від хоста 1 до хоста 2. Для схеми хост-хост найчастіше використовується транспортний режим захисту.

У відповідності зі схемою шлюз-шлюз захищений канал встановлюється між двома проміжними вузлами, так званими **шлюзами безпеки** (Security Gateway, **SG**), на кожному з яких працює протокол IPSec (рис. 6.11). Захищений обмін даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, які розташовані позаду шлюзів безпеки. Від кінцевих вузлів підтримка протоколу IPSec не потрібна, вони передають свій трафік в незахищеному вигляді через внутрішні мережі підприємств, які заслуговують на довіру. Трафік, що направляється в загальнодоступну мережу, проходить через шлюз безпеки, який і забезпечує його захист за допомогою протоколу IPSec. Шлюзам доступний тільки тунельний режим роботи.

На рисунку користувач комп'ютера з адресою IP1 надсилає пакет за адресою IP2, використовуючи тунельний режим протоколу IPSec. Шлюз SG1 зашифровує пакет повністю, разом із заголовком, і додає до нього новий IP-заголовок, в якому в якості адреси відправника вказує свою адресу – IP3, а в якості адреси одержувача – адреса IP4 шлюзу SG2. Передача даних по публічній IP-мережі виконується на підставі заголовка зовнішнього пакету, а внутрішній пакет стає при цьому полем даних для зовнішнього пакета. На шлюзі SG2 протокол IPSec витягує інкапсульований пакет і розшифровує його, приводячи до початкового стану.

Схема хост-шлюз часто застосовується при віддаленому доступі. В цьому випадку захищений канал прокладається між віддаленим хостом, на якому працює протокол IPSec, і шлюзом, який захищає трафік для всіх хостів, що входять у внутрішню мережу підприємства. Цю схему можна ускладнити, створивши паралельно ще один захищений канал – між віддаленим хостом і будь-яким хостом, що належить внутрішній мережі, що захищається шлюзом (рис. 6.12). Таке комбіноване використання двох безпечних асоціацій дозволяє надійно захистити трафік у внутрішній мережі.

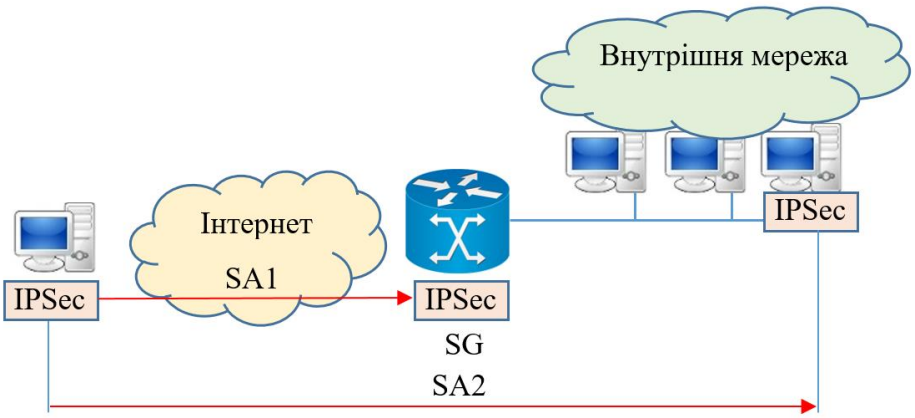


Рис. 6.12. Схема захищеного каналу хост-шлюз

Протокол AH

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.

Дві перші функції обов'язкові для протоколу AH, а остання вибирається за бажанням при встановленні асоціації. Для виконання цих функцій протокол AH використовує спеціальний заголовок (рис. 6.13).

Рис. 6.13. Структура заголовку протоколу AH

В полі **наступного заголовка** (Next Header) вказується код протоколу більш високого рівня, тобто протоколу, повідомлення якого розміщено в полі даних IP-пакета. Швидше за все, ним буде один з протоколів транспортного рівня (TCP або UDP) або протокол ICMP, але може зустрітися і протокол ESP, якщо він використовується в комбінації з AH.

В полі **корисне навантаження** (Payload Length) міститься довжина заголовка AH.

Індекс параметрів безпеки (Security Parameters Index, SPI) використовується для зв'язку пакета з передбаченою для нього безпечною асоціацією.

Поле **порядкового номера** (Sequence Number, SN) вказує на порядковий номер пакета і застосовується для захисту від його зловмисного відтворення (коли третя сторона намагається повторно використовувати перехоплені захищені пакети, відправлені реально автентифікованим відправником). Відправник послідовно збільшує значення цього поля в кожному новому пакеті, що передається в рамках даної асоціації, так що прихід дубліката виявиться приймаючою стороною (якщо, звичайно, в рамках асоціації буде активована функція захисту від зловмисного відтворення). Однак, в будь-якому випадку у функції протоколу AH не входить відновлення загублених і упорядкування вхідних пакетів – він просто відкидає пакет, коли виявляє, що аналогічний пакет вже отримано. Щоб скоротити необхідну для роботи протоколу буферну пам'ять, використовується механізм ковзаючого вікна – на предмет дублювання перевіряються тільки ті пакети, чий номер знаходиться в межах вікна. Вікно, зазвичай, вибирається розміром в 32 або 64 пакети.

Поле **даних автентифікації** (Authentication Data), яке містить **значення перевірки цілісності** (Integrity Check Value, ICV), служить для автентифікації і перевірки цілісності пакету. Це значення, зване також дайджестом, обчислюється за допомогою однієї з двох обов'язково підтримуваних

протоколом AH односторонніх функцій (One-way function, OWF) MD5 або SAH-1, але може використовуватися і будь-яка інша функція, про яку сторони домовилися в ході встановлення асоціації. При обчисленні дайджесту пакета в якості параметра функції OWF виступає симетричний секретний ключ, який був заданий для даної асоціації вручну або автоматично за допомогою протоколу IKE. Так як довжина дайджесту залежить від обраної функції, це поле має в загальному випадку змінний розмір.

Протокол AH намагається охопити при обчисленні дайджесту якомога більше число полів вихідного IP-пакета, але деякі з них в процесі передачі пакета по мережі змінюються непередбачуваним чином, тому не можуть включатися в автентифіковану частину пакету. Наприклад, цілісність значення поля часу життя (TTL) в приймальній точці каналу оцінити не можна, так як воно зменшується на одиницю кожним проміжним маршрутизатором і ніяк не може збігатися з вихідним.

Місцезнаходження заголовка AH в пакеті залежить від того, в якому режимі – транспортному або тунельному – налаштований захищений канал. Результуючий пакет в транспортному режимі виглядає так, як показано на рис. 6.14.

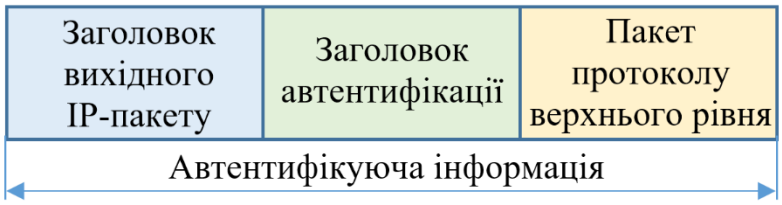


Рис. 6.14. Структура IP-пакету, обробленого протоколом AH в транспортному режимі

При використанні тунельного режиму, коли шлюз IPSec приймає вихідний пакет, що проходить через нього транзитом і створює для нього зовнішній IP-пакет, протокол AH захищає всі поля вихідного пакета, а також незмінні поля нового заголовку зовнішнього пакета (рис. 6.15).

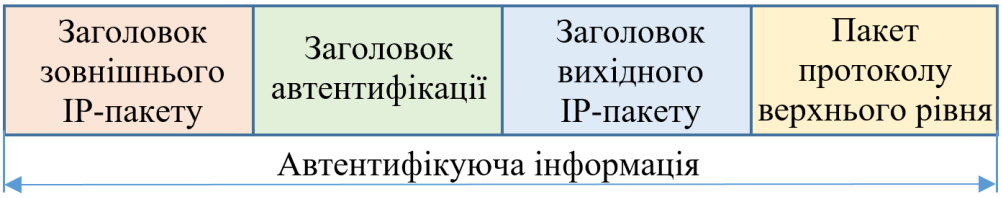


Рис. 6.15. Структура IP-пакету, обробленого протоколом AH в тунельному режимі

Протокол ESP

Протокол ESP вирішує дві групи завдань. До першої групи належать завдання забезпечення автентифікації і цілісності даних на основі дайджесту, аналогічні завданням протоколу AH, до другої – захист переданих даних шляхом їх шифрування від несанкціонованого перегляду.

Як видно на рис. 6.16, заголовок ділиться на дві частини, що розділяються полем даних. Перша частина, яка називається **заголовком ESP**, утворюється двома полями (SP1 і SN), призначення яких аналогічно однойменним полям протоколу AH, і розміщується перед полем даних. Інші службові поля протоколу ESP, які називаються **кінцевиком ESP**, розташовані в кінці пакета.

Рис. 6.16. Структура IP-пакету, обробленого протоколом ESP в транспортному режимі

Два поля кінцевика – **наступного заголовку** і **дані автентифікації** – також аналогічні полям заголовка AH. Поле даних автентифікації відсутнє, якщо при встановленні безпечної асоціації прийнято рішення не використовувати засоби протоколу ESP, що стосуються забезпечення цілісності. Крім цих полів кінцевик містить два додаткових поля – **заповнювач** і **довжина заповнювача**. Заповнювач може знадобитися в трьох випадках. По-перше, для нормальної роботи деяких алгоритмів шифрування необхідно, щоб шифрований текст містив кратне число блоків певного розміру. По-друге, формат заголовка ESP вимагає, щоб поле даних закінчувалося на межі чотирьох байтів. І нарешті, заповнювач можна використовувати, щоб приховати дійсний розмір пакета з метою забезпечення так званої часткової конфіденційності трафіку.

На рис. 6.16 показано розміщення полів заголовка ESP в транспортному режимі. В цьому режимі ESP не шифрує заголовок IP-пакету, інакше маршрутизатор не зможе прочитати поля заголовка і коректно здійснити просування пакета між мережами. У число шифрованих полів не потрапляють також поля SPI і SN, які повинні передаватися у відкритому вигляді для того,

щоб вхідний пакет можна було віднести до певної асоціації і запобігти зловмисному відтворенню пакета.

У тунельному режимі заголовок вихідного IP-пакета поміщається після заголовка ESP і повністю потрапляє в число захищених полів, а заголовок зовнішнього IP-пакета протоколом ESP не захищається (рис. 6.17).

Бази даних SAD і SPD

Отже, технологія IPSec пропонує різні методи захисту трафіку. 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).

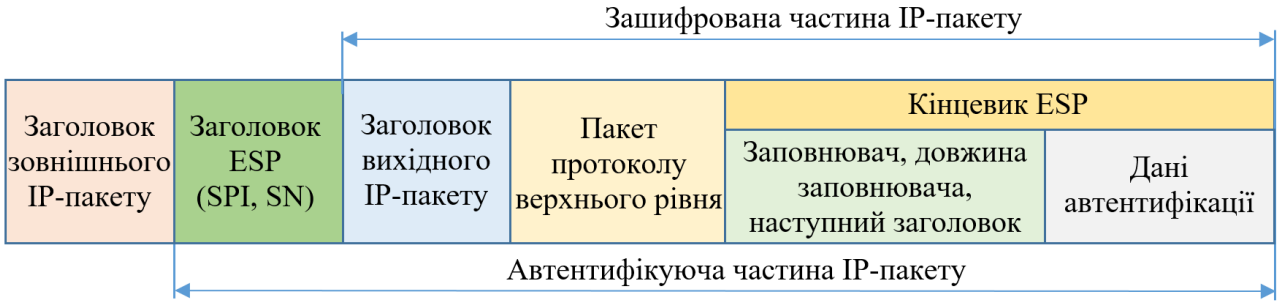


Рис. 6.17. Структура IP-пакету, обробленого протоколом ESP в тунельному режимі

При встановленні безпечної асоціації, як і при будь-якому іншому логічному з'єднанні, дві сторони приймають ряд угод, що регламентують процес передачі потоку даних між ними. Угоди фіксуються у вигляді набору параметрів. Для безпечної асоціації такими параметрами є, зокрема, тип і режим роботи протоколу захисту (AH або ESP), методи шифрування, секретні ключі, значення поточного номера пакета в асоціації та інша інформація. Набори поточних параметрів, що визначають всі активні асоціації, зберігаються на обох кінцевих вузлах захищеного каналу у вигляді **баз даних безпечних асоціацій** (SAD). Кожен вузол IPSec підтримує дві бази SAD – одну для вихідних асоціацій, іншу для вхідних.

Інший тип бази даних – **база даних політики безпеки** (SPD) – визначає відповідність між IP-пакетами та встановленими для них правилами обробки.

Записи SPD складаються з полів двох типів – полів селектора пакета і полів політики захисту для пакета з даними значенням селектора (рис. 6.18).

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.

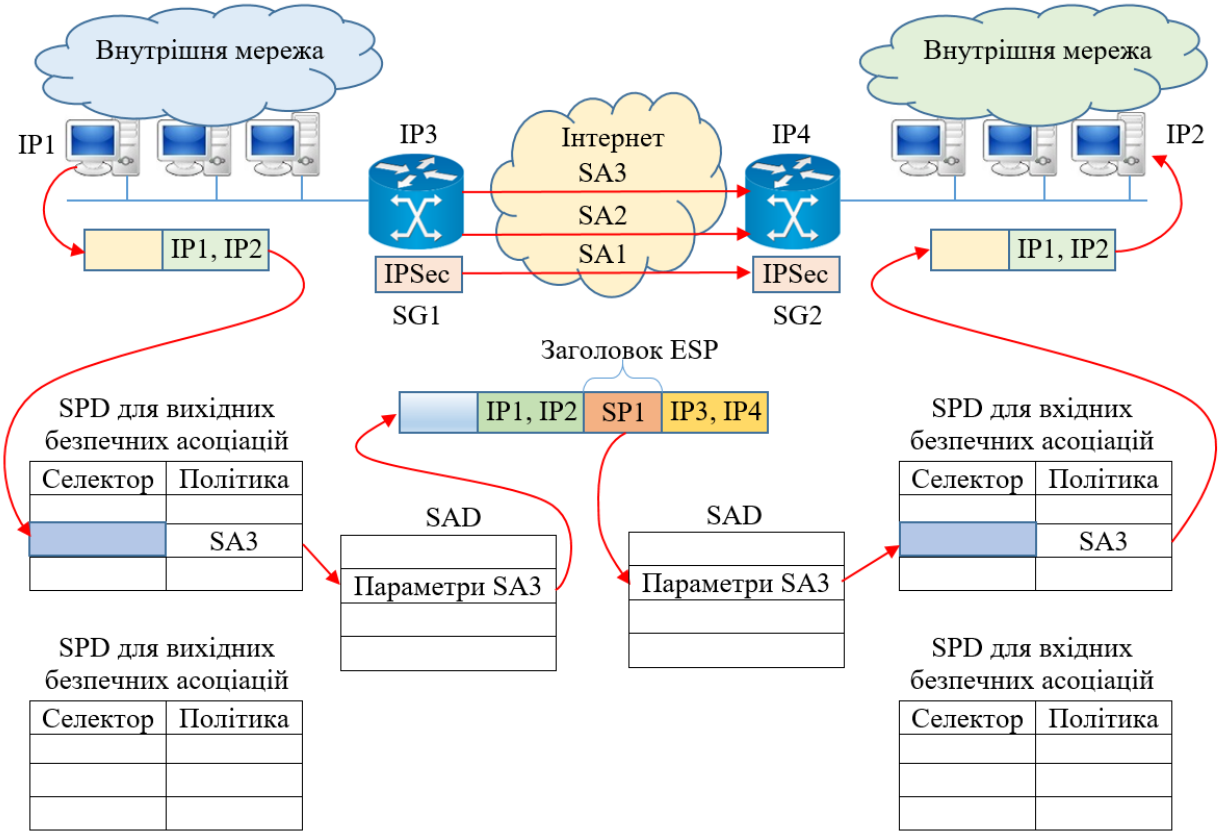


Рис. 6.18. Використання баз даних SAD і SPD

Для кожного нового пакета, що надходить в захищений канал, IPSec переглядає всі записи в базі SPD і порівнює значення селекторів цих записів з відповідними полями IP-пакета. Якщо значення полів збігається з будь-яким селектором, то над пакетом виконуються дії, визначені в полі політики безпеки

цього запису. Політика передбачає передачу пакета без зміни, відкидання або обробку засобами IPSec.

В останньому випадку поле політики захисту повинно містити посилання на запис в базі даних SAD, в яку поміщений набір параметрів безпечної асоціації для даного пакета (на рисунку для вихідного пакету встановлено зв'язок SA3). На підставі заданих параметрів безпечної асоціації до пакету застосовується відповідний протокол (на рисунку – ESP), функції шифрування і секретні ключі.

Якщо до вихідного пакету потрібно застосувати деяку політику захисту, але покажчик запису SPD показує, що в даний час немає активної безпечної асоціації з необхідною політикою, то IPSec створює нову асоціацію з допомогою протоколу IKE, поміщаючи нові записи в бази даних SAD і SPD.

Бази даних політики безпеки створюються і адмініструються або користувачем (цей варіант більше підходить для хоста), або системним адміністратором (варіант для шлюзу), або автоматично (додатком).

Встановлення зв'язку між вихідним IP-пакетом і заданою для нього безпечною асоціацією відбувається шляхом селекції. Для того, щоб приймаючий вузол IPSec визначив спосіб обробки вхідного пакету (при шифруванні багато ключових параметрів пакету, що відображені в селекторі, виявляються недоступними, а значить, неможливо визначити відповідний запис в базах даних SAD і SPD) в заголовках AH і ESP передбачено поле SPI. У це поле поміщається покажчик на той рядок бази даних SAD, в якому записані параметри відповідної безпечної асоціації. Поле SPI заповнюється протоколом AH або ESP під час обробки пакета в відправній точці захищеного каналу. Коли пакет приходить в кінцевий вузол захищеного каналу, з його зовнішнього заголовка ESP або AH (на рисунку з заголовка ESP) зчитується значення SPI, і подальша обробка пакету виконується з урахуванням всіх параметрів, що задані цим вказівником асоціації.

Таким чином, для розпізнавання пакетів, що відносяться до різних безпечних асоціацій, використовуються:

- на вузлі-відправнику – селектор;
- на вузлі-отримувачі – індекс параметрів безпеки (SPI).

Після дешифрування пакету приймальний вузол IPSec перевіряє його ознаки (що стали тепер доступними) на предмет збігу з селектором запису SPD для вхідного трафіку, щоб переконатися, що не відбулося помилки і виконувана обробка пакету відповідає політиці захисту, що задана адміністратором.

Використання баз SPD і SAD для захисту трафіку дозволяє досить гнучко поєднувати механізм безпечних асоціацій, який передбачає встановлення логічного з'єднання, з датаграмним характером трафіку протоколу IP.

7. Організація запровадження системи інформаційної безпеки

7.1 Потреба в запровадженні окремої системи інформаційної безпеки

Більшість сучасних інформаційних ресурсів, а також інформаційних систем практично не можуть розглядатися у відриві від комплексу чинників, пов’язаних із забезпеченням інформаційної безпеки: загроз для інформаційних ресурсів, різних засобів і заходів захисту, бар’єрів для проникнення, а також вразливостей в системах захисту інформації. Таким чином, для дотримання заходів з інформаційної безпеки потрібна сукупність засобів, методів і процесів (процедур), які забезпечують комплексний захист інформаційних активів і гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і відомостей, які в таких системах зберігаються і обробляються. Мета інформаційної безпеки полягає в тому, щоб зберегти цілісність, повноту та точність інформації, зменшити ризик несанкціонованих змін в інформаційних системах. Для того, щоб забезпечити підприємству розвиток та конкурентоспроможність, необхідно створити систему управління інформаційною безпекою, яка буде частиною загальної системи управління, яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення заходів із інформаційної безпеки.

7.1.1. Класифікація ризиків

Ризики в розумінні системи інформаційної безпеки можуть мати різну природу і характеристики; однією з основних класифікацій ризиків для інформаційної безпеки (так само, як і багатьох інших ризиків в економіці та управлінні) є їх поділ на:

- системні ризики – некеровані ризики, пов'язані з тим середовищем і технічною інфраструктурою, в якій функціонують інформаційні системи;
- операційні ризики – як правило, керовані ризики, пов'язані з особливостями використання певних інформаційних систем, їх технічної реалізації, застосовуваними алгоритмами, апаратними засобами тощо.

Всі негативні впливи на інформаційні активи, захист від яких (впливів) передбачає інформаційна безпека, можуть бути розділені на три основні види:

- порушення конфіденційності інформації;
- руйнування (втрата, необоротна зміна) інформації;
- недоступність інформаційних ресурсів – виникнення ситуацій, коли користувачі (всі або їх частина) на деякий період часу втрачають можливість доступу до необхідних даних (або інформаційних систем).

Безпосереднім джерелом ризиків і негативних впливів є загрози, під якими розуміються потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що порушують інформаційну безпеку. Виділяється безліч типів загроз і безліч критеріїв для класифікації загроз інформаційній безпеці. Одним з основних таких критеріїв є розташування джерела порушень до інформаційних ресурсів, щодо яких здійснюється негативний вплив. Відповідно до цього критерію порушення можуть бути розділені:

- на обумовлені внутрішніми факторами (персоналом підприємства, роботою власних інформаційних систем);
- обумовлені зовнішніми факторами (зловмисниками, які не мають безпосереднього відношення до компанії – власника інформаційних активів, природними факторами тощо).

Іншим важливим критерієм є наявність намірів здійснити порушення. Відповідно до нього виділяють:

- цілеспрямовані дії (можуть бути здійснені як власним персоналом, так і зовнішніми противниками);
- випадковий вплив (помилки користувачів та адміністраторів, збої і випадкові порушення в роботі обладнання, непередбачений вплив природних факторів).

Також можна виділити наступні класифікації загроз:

- за об'єктом (персонал, матеріальні та фінансові кошти, інформація);
- за величиною збитку (граничний, значний, незначний);
- за ймовірністю виникнення (дуже вірогідні, ймовірні, малоймовірні);
- за типом збитку (моральний, матеріальний);
- деякі інші.

На практиці основними найбільш поширеними способами порушення інформаційної безпеки є:

- отримання несанкціонованого доступу (у тому числі і шляхом перевищення прав при санкціонованій роботі з інформаційними системами) до певних відомостей або масивів даних, поширення яких обмежене, з метою їх вивчення, копіювання, поширення, незаконного використання тощо;
- несанкціоноване використання інформаційних ресурсів (ресурсів обчислювальних і телекомунікаційних систем) з метою отримання

вигоди або нанесення збитку (як тим системам, які незаконно використовуються, так і третім особам);

- несанкціонована зловмисна модифікація (зміна) даних;
- крадіжка грошових коштів в електронних платіжних системах і системах «клієнт-банк»;
- виведення з ладу (повне або часткове) програмних і апаратних засобів обробки, передачі та зберігання інформації;
- здійснення атак типу «відмова в обслуговуванні» – DoS (зокрема, щодо серверів в мережі Інтернет);
- поширення вірусів і інших шкідливих програм, що здійснюють різні негативні впливи.

Сучасна практика використання інформаційних систем характеризується великою кількістю і постійним зростанням числа порушень інформаційної безпеки. Одним з важливих чинників цього є постійно зростаюча доступність сучасних інформаційних технологій для злочинців, а також постійно зростаюча привабливість інформаційних систем як потенційних об'єктів нападу. Також важливою обставиною є постійне ускладнення і зростання різноманітності інформаційних систем, що використовуються, і, зокрема, програмних продуктів. З урахуванням того, що в середньому кожна тисяча рядків програмного коду може містити від 5 до 15 помилок, поява все більшого числа різних вразливостей, що створюють загрози для інформаційної безпеки, стає практично неминучою.

Результатом цього є постійне зростання кількості різних порушень, пов'язаних з інформаційною безпекою.

Таким чином, всі перераховані обставини: зростання різноманіття можливих порушень, збільшення їх кількості, збільшення складності інформаційних технологій, постійно зростаюча доступність комп'ютерів і телекомунікаційних засобів для злочинців – пояснюють зростання потреби власників інформаційних ресурсів (підприємств, організацій, державних відомств) у реалізації систематичних, всеосяжних заходів щодо забезпечення інформаційної безпеки.

Окремі процеси, процедури, механізми та інструменти захисту інформації, використовувані власниками інформаційних ресурсів та інформаційних систем, можуть бути спрямовані:

- на обмеження і розмежування доступу;

інформаційне приховування;

введення надлишкової інформації і використання надлишкових інформаційних систем (засобів зберігання, обробки і передачі інформації);

використання методів надійного зберігання, перетворення і передачі інформації;

нормативно-адміністративне спонукання і примус.

На практиці сучасні технології захисту інформації побудовані на різних базових сервісах (таких, як автентифікація, забезпечення цілісності, контроль доступу та ін.), і використовують різні механізми забезпечення безпеки (такі, як шифрування, цифрові підписи, управління маршрутизацією тощо). Однак комплексність і масовість використання інформаційних технологій, їх інтеграція в повсякденну діяльність підприємств, організацій, урядових установ не дозволяють вирішувати завдання інформаційної безпеки тільки одними технічними засобами.

7.1.2 Організація забезпечення системи інформаційної безпеки

У всьому комплексі діяльності із захисту інформації одне з найбільш важливих місць займає організаційно-управлінська діяльність – організаційне забезпечення інформаційної безпеки, яке являє собою один з чотирьох основних напрямків роботи в загальній системі заходів у сфері інформаційної безпеки, що включає в себе також розробку спеціалізованого програмного забезпечення, виготовлення і використання спеціальних апаратних засобів і вдосконалення криптографічних (математичних) методів захисту інформації (рисунок 1.2).

Основними завданнями організаційно-управлінської діяльності (менеджменту) у сфері інформаційної безпеки є:

- забезпечення комплексності всіх рішень, реалізованих у процесі забезпечення інформаційної безпеки;
- забезпечення безперервності і цілісності процесів інформаційної безпеки;
- вирішення методичних завдань, що лежать в основі ефективного управління інформаційною безпекою, таких, як питання управління ризиками, економічне моделювання, тощо;
- управління людськими ресурсами та поведінкою персоналу з урахуванням необхідності вирішення завдань інформаційної безпеки.

Під комплексністю вирішення завдань інформаційної безпеки маються на увазі взаємопов'язані виявлення всіх значущих інформаційних об'єктів, а також існуючих і потенційно можливих загроз. На основі цього аналізу необхідно забезпечити вичерпно повне (комплексне) впровадження і застосування засобів захисту інформації, які в тій чи іншій мірі могли б нейтралізувати всі істотні загрози на всіх потенційно вразливих ділянках проходження інформаційних потоків протягом всіх етапів життєвого циклу інформаційних систем та

організаційних процедур. Заходи щодо нейтралізації ризиків також повинні бути реалізовані в комплексі з іншими механізмами, такими, як, наприклад, страхування. Іншими словами, завданням менеджменту є системне використання всіх необхідних (вузькоспеціальних) технологій і рішень для кожної конкретної ситуації таким чином, щоб у всій системі заходів із захисту інформаційних ресурсів не залишилося «вузьких місць» – уразливих ділянок, через які можуть бути здійснені напади і в яких можуть відбутися ненавмисні порушення. Складність такого роду завдань пов'язана з тим, що вони припускають по можливості вичерпний аналіз як всіх інформаційних ресурсів, так і всіх можливих сценаріїв нападу на них та подальший підбір найбільш придатних засобів захисту.

Неперервність процесів забезпечення інформаційної безпеки передбачає виділення необхідних ресурсів та організацію виконання необхідних функцій із захисту інформації протягом усього часу функціонування інформаційних систем і виконання бізнес-функцій.

Розробка, вдосконалення та підтримка в актуальному стані методичних основ управління інформаційною безпекою включає в себе, головним чином, застосування загальних для багатьох сфер менеджменту концепцій і теорій – таких як, наприклад, математичні моделі оцінки ризиків або теорія інвестиційного аналізу – стосовно до ресурсів, що використовуються для забезпечення інформаційної безпеки та інформаційних процесів.

Управління людськими ресурсами в рамках управління інформаційною безпекою включає в себе комплекс завдань, що охоплює всі основні аспекти діяльності людей: відбір і допуск персоналу до роботи з певними інформаційними ресурсами, навчання, контроль правильності виконання обов'язків, створення необхідних умов для роботи тощо.

При цьому конкретна структура і склад всіх основних завдань управління та організації у сфері інформаційної безпеки, а також методи, що безпосередньо використовуються, будуть визначатися як рівнем, на якому здійснюється управлінська та організаційна діяльності, так і конкретними умовами, в яких функціонують інформаційні системи, які потребують захисту. Курс заснований на концепції поділу усього різноманіття методів і завдань організації та управління у сфері інформаційної безпеки на кілька основних рівнів і подальшому поданні організаційно-управлінських методів для кожного з цих рівнів.

Під організаційним забезпеченням та менеджментом у сфері інформаційної безпеки зазвичай прийнято розуміти рішення управлінських питань на рівні окремих суб'єктів (підприємств, організацій) або груп таких

суб'єктів (партнерів по бізнесу, організацій, що спільно вирішують певні завдання і потребують захисту інформації).

Однак складність і комплексність сучасних проблем у сфері інформаційної безпеки, глобалізація інформаційних взаємодій вимагають більш повного і широкого розуміння організаційної роботи та менеджменту в цій галузі.

Зокрема, в час глобалізації інформаційних взаємодій, ускладнення програмних і апаратних засобів обробки інформації, проникнення інформаційних технологій у повсякденну діяльність всіх організацій і життя більшості людей з'явилася необхідність в спеціальних організаційних і управлінських зусиллях, спрямованих не скільки на забезпечення захищеності окремих інформаційних активів, як на підтримку різних елементів інформаційної інфраструктури, яка в тій чи іншій мірі працює на забезпечення інформаційної безпеки певних спільнот (заздалегідь не визначеної множини користувачів інформаційних систем і власників інформаційних ресурсів).

Таким чином, з розвитком інформаційних технологій і інтенсифікацією інформаційного обміну організаційна та управлінська робота у сфері інформаційної безпеки виявляється спрямованою не тільки на власне захист певних інформаційних ресурсів, але і на більш «глобальний» об'єкт – створення і розвиток безпечної інформаційної інфраструктури (у різних значеннях цього терміну і з урахуванням різних його аспектів). На практиці така інфраструктура може включати в себе:

- надійну інфраструктуру передачі інформації і ринок послуг доступу до таких каналів зв'язку;
- ринок програмних і апаратних засобів, що забезпечують захист інформації;
- систему підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері інформаційної безпеки;
- загальні правила використання інформації, а також її передачі, спільної експлуатації інформаційних мереж (у тому числі протоколи інформаційного обміну);
- систему обміну інформацією та поширення знань про існуючі вразливості тих чи інших інформаційних технологій, про можливі загрози інформаційній безпеці та способи їх нейтралізації;
- законодавчу і правочинну систему, що забезпечує охорону майнових та інших інтересів всіх учасників інформаційного обміну;
- інші складові.

Потреба в цілеспрямованому розвитку та підтримці такої інфраструктури породжує необхідність у виробленні специфічних організаційних і

управлінських прийомів, як правило, не характерних для інформаційної безпеки в звичному («вузькому») її розумінні.

Таке розширення сфери інтересів менеджменту інформаційної безпеки пояснює причини, за якими необхідно розділяти кілька відносно самостійних організаційних рівнів, що характеризуються специфічними завданнями, підходами до вирішення цих завдань і організаційними методами, які застосовуються.

- Рівень міжнародних професійних об'єднань (як правило, неурядових і некомерційних), так чи інакше пов'язаних зі сферою інформаційних технологій, телекомунікацій та інформаційної безпеки.
- Рівень великих компаній, що працюють у сфері інформаційних технологій і значною мірою визначають (прямо чи опосередковано) стан інформаційної безпеки в співтоваристві користувачів інформаційних систем, а також впливають на безпеку різних елементів інформаційної інфраструктури.
- Державний рівень – рівень державних і міжурядових організацій, які так чи інакше впливають на життя суспільства, стан правової системи, розвиток економіки і технологій.
- Рівень окремих компаній (підприємств та організацій) – спільнота користувачів інформаційних систем, так чи інакше зацікавлених у власній інформаційній безпеці та забезпечують захист наявних у них інформаційних ресурсів власними силами.

Також окремо можна виділити додатковий проміжний рівень, до складу якого входять консалтингові та впроваджувальні компанії, навчальні центри (включаючи також спільноту фахівців, що займаються консультаціями, впровадженням і навчанням в індивідуальному порядку), що працюють у сфері інформаційної безпеки та діють як сполучна ланка між різними організаційними рівнями, а також представляють інтереси різних учасників інформаційної взаємодії.

7.2. Управління інформаційною безпекою на рівні підприємства

Забезпечення власної інформаційної безпеки на підприємствах, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань та має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика, тощо.

7.2.1. Передумови розвитку менеджменту в сфері інформаційної безпеки на рівні підприємств

Забезпечення власної інформаційної безпеки на підприємствах, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань. Значимість систематичної цілеспрямованої діяльності щодо забезпечення інформаційної безпеки стає тим більш високою, чим вище ступінь автоматизації бізнес-процесів підприємства, і чим більше "інтелектуальна складова" в його кінцевому продукті, тобто чим більшою мірою успішність діяльності залежить від наявності та збереження певної інформації (технологій, ноу-хау, комерційних баз даних, маркетингової інформації, результатів наукових досліджень тощо), забезпечення її конфіденційності та доступності для власників і користувачів. Роль інформації в діяльності підприємств зростає в міру лібералізації світових ринків, коли матеріальні активи меншою мірою є джерелами конкурентних переваг в силу значного зменшення торгівельних бар'єрів. Нематеріальні активи, існуючі зазвичай у вигляді інформації, в цих умовах починають грати роль однієї з провідних засад для підвищення конкурентоспроможності та розвитку бізнесу.

Забезпечення інформаційної безпеки також, як правило, має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика, тощо. Крім того, значимість забезпечення інформаційної безпеки в деяких випадках може визначатися наявністю в загальній системі інформаційних потоків підприємства відомостей, що становлять не тільки комерційну, а й державну таємницю, а також інші види конфіденційної інформації (відомості, що становлять банківську таємницю, лікарську таємницю, інтелектуальну власність компаній-партнерів тощо).

Так само як і на державному рівні, управління інформаційною безпекою на рівні підприємств націлене на нейтралізацію різних видів загроз:

- зовнішніх, таких як неправомірні дії державних органів (у тому числі і закордонних), протиправна діяльність злочинців і злочинних угруповань, незаконні дії компаній-конкурентів та інших господарюючих суб'єктів, недобросовісні дії компаній-партнерів, невідповідність чинної нормативно-правової бази фактичному розвитку технологій і суспільних відносин, збої і порушення в роботі глобальних інформаційних та телекомунікаційних систем та інформаційних систем компаній-партнерів (контрагентів) та ін.;

- внутрішніх, таких як помилки і халатність персоналу підприємства, а також навмисно допускаються порушення, збої і порушення в роботі власних інформаційних систем та ін.

Таким чином, управління інформаційною безпекою на кожному окремому підприємстві має здійснюватися в контексті його загальної господарської діяльності: з урахуванням характеру діяльності компанії (технології виробництва, специфіки ринків збуту тощо), а також як фактично складається ситуація у ринковій конкурентній боротьбі, державній політиці, розвитку правової та правоохоронної системи, рівня розвитку окремих використовуваних інформаційних і телекомунікаційних технологій та інших факторів, що формують загальні умови поточної діяльності.

Формальною підставою (передумовою) для здійснення цілеспрямованої діяльності у сфері захисту інформації, крім загальнодержавних вимог до захисту інформації, що становить державну, військову, лікарську та банківську таємницю, також є перелік відомостей, що становлять комерційну таємницю підприємства, який визначається підприємством самостійно з урахуванням вимог чинного законодавства.

Крім того, необхідність розробки і впровадження політики інформаційної безпеки може бути обумовлена такими обставинами як:

- необхідність зменшення вартості страхування інформаційних ризиків або певних бізнес-ризиків;
- необхідність впровадження міжнародних стандартів, таких як ISO/IEC 27002.

На рисунку 7.1 представлено передумови розробки політики безпеки підприємства.

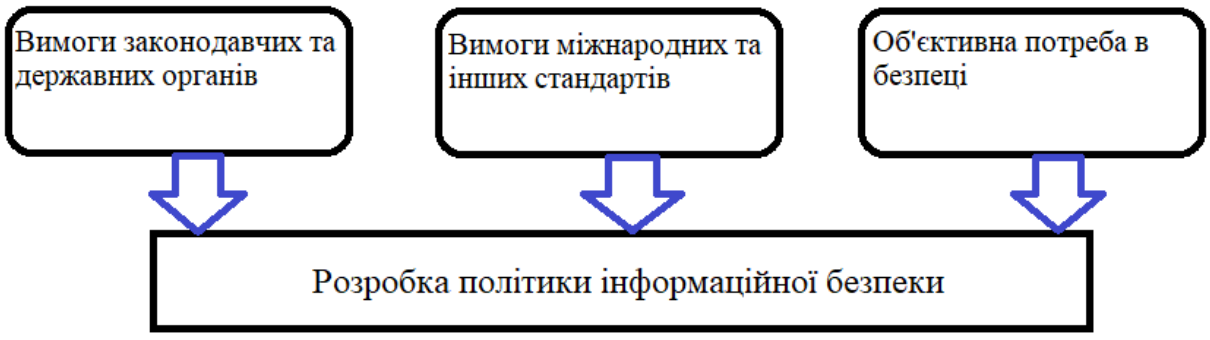


Рисунок 7.1 – Передумови розробки політики безпеки підприємства

7.2.2. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства

Для нейтралізації існуючих загроз і забезпечення інформаційної безпеки підприємства створюють систему менеджменту у сфері інформаційної безпеки, в рамках якої (системи) проводять роботу за кількома напрямками:

- формування та практична реалізація комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;
- організація департаменту (служби, відділу) інформаційної безпеки;
- розробка системи заходів і дій на випадок виникнення непередбачених ситуацій («Управління інцидентами»);
- проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.

Кожен з цих напрямків організаційної роботи має свої особливості і має реалізовуватися з використанням специфічних методів менеджменту та у відповідності зі своїми правилами. Політики і правила інформаційної безпеки є організаційними документами, регулюючими діяльність всієї організації або окремих підрозділів (категорій співробітників) в роботі з інформаційними системами та інформаційними потоками. Департамент інформаційної безпеки є вузько спеціалізованим підрозділом, який вирішує специфічні питання захисту інформації. Система заходів з реагування на інциденти забезпечує готовність всієї організації (включаючи Департамент інформаційної безпеки) до осмислених цілеспрямованих дій у разі будь-яких подій, пов'язаних з інформаційною безпекою. Проведення внутрішніх аудитів інформаційної безпеки (періодичних або пов'язаних з певними подіями) має забезпечити контроль за поточним станом системи заходів щодо захисту інформації та, зокрема, незалежну перевірку відповідності реального стану справ встановленим правилам і вимогам.

При цьому кожен з напрямків діяльності має постійно вдосконалюватися, а конкретні завдання повинні постійно уточнюватися відповідно до зміни в організаційній структурі, виробничих процесах або зовнішньому середовищі.

7.2.3. Формування політики інформаційної безпеки на підприємстві

Структура політики інформаційної безпеки та процес її розробки.

Політика інформаційної безпеки являє собою комплекс документів, що відображають всі основні вимоги до забезпечення захисту інформації та

напрямки роботи підприємства в цій сфері. При побудові політики безпеки можна умовно виділити три її основні рівні: верхній, середній і нижній.

Верхній рівень політики інформаційної безпеки підприємства служить:

- для формулювання і демонстрації ставлення керівництва підприємства до питань інформаційної безпеки та відображення загальних цілей всього підприємства в цій галузі;
- основою для розробки індивідуальних політик безпеки (на більш низьких рівнях), правил та інструкцій, що регулюють окремі питання;
- засобом інформування персоналу підприємства про основні завдання та пріоритети підприємства у сфері інформаційної безпеки.

Політики інформаційної безпеки середнього рівня визначають ставлення підприємства (керівництва підприємства) до певних аспектів його діяльності та функціонування інформаційних систем:

- ставлення і вимоги (більш детально в порівнянні з політикою верхнього рівня) підприємства до окремих інформаційних потоків та інформаційних систем, обслуговуючим різні сфери діяльності, ступінь їх важливості та конфіденційності, а також вимоги до надійності (наприклад, відносно фінансової інформації, а також інформаційних систем і персоналу, які відносяться до неї);
- відношення і вимоги до певних інформаційних та телекомунікаційних технологій, методів і підходів до обробки інформації і побудови інформаційних систем;
- відношення і вимоги до співробітників підприємства як до учасників процесів обробки інформації, від яких безпосередньо залежить ефективність багатьох процесів і захищеність інформаційних ресурсів, а також основні напрями і методи впливу на персонал з метою підвищення інформаційної безпеки.

Політики безпеки на найнижчому рівні відносяться до окремих елементів інформаційних систем і ділянок обробки та зберігання інформації і описують конкретні процедури і документи, пов'язані із забезпеченням інформаційної безпеки.

Розробка політики безпеки передбачає здійснення низки попередніх кроків:

- оцінку особистих (суб'єктивних) відносин до ризиків підприємства його власників і менеджерів, відповідальних за функціонування і результативність роботи підприємства в цілому або окремі напрями його діяльності;
- аналіз потенційно вразливих інформаційних об'єктів;
- виявлення загроз для значущих інформаційних об'єктів (відомостей, інформаційних систем, процесів обробки інформації) і оцінку

відповідних ризиків.

Здійснення попередніх кроків (аналізу) дозволяє визначити, наскільки інформаційна безпека в цілому важлива для стійкого здійснення основної діяльності підприємства, його економічної безпеки. На основі цього аналізу з урахуванням оцінок менеджерів і власників визначаються конкретні напрямки роботи щодо забезпечення інформаційної безпеки. При цьому в деяких випадках особиста думка окремих керівників може і не мати вирішального значення.

Таким чином, політика інформаційної безпеки (практично на всіх рівнях) в частині роботи з такими даними буде заснована на загальних строго формалізованих правилах, процедурах і вимогах (таких, як використання сертифікованого обладнання та програмного забезпечення, проходження процедур допуску, обладнання спеціальних приміщень для зберігання інформації тощо).

При розробці політик безпеки всіх рівнів необхідно дотримуватися наступних основних правил.

- Політики безпеки на більш низьких рівнях повинні повністю підкорятися відповідній політиці верхнього рівня, а також чинному законодавству і вимогам державних органів.
- Текст політики безпеки повинен містити тільки чіткі і однозначні формулювання, що не допускають подвійного тлумачення.
- Текст політики безпеки повинен бути доступний для розуміння тих співробітників, яким він адресований.

Загалом політика інформаційної безпеки повинна давати чітке уявлення про необхідну поведінку користувачів, адміністраторів та інших фахівців при впровадженні та використанні інформаційних систем і засобів захисту інформації, а також при здійсненні інформаційного обміну та виконанні операцій з обробки інформації. Крім того, з політики безпеки, якщо вона відноситься до певної технології та/або методології захисту інформації, повинні бути зрозумілі основні принципи роботи цієї технології. Важливою функцією політики безпеки є чітке розмежування відповідальностей в процедурах інформаційного обміну: всі зацікавлені особи повинні ясно усвідомлювати межу як своєї відповідальності, так і відповідальності інших учасників відповідних процедур і процесів. Також одним із завдань політики безпеки є захист не тільки інформації та інформаційних систем, а й захист самих користувачів (співробітників підприємства і його клієнтів і контрагентів).

Загальний життєвий цикл політики інформаційної безпеки включає в себе ряд основних кроків.

- Проведення попереднього дослідження стану інформаційної безпеки.
- Власне розробку політики безпеки.

- Впровадження розроблених політик безпеки.
- Аналіз дотримання вимог впровадженої політики безпеки та формулювання вимог щодо її подальшого вдосконалення (повернення до першого етапу, на новий цикл вдосконалення).

Цей цикл (рисунок 10.3) може повторюватися кілька разів з метою вдосконалення організаційних заходів у сфері захисту інформації та усунення виявлених недоробок.

Політика інформаційної безпеки підприємства: верхній рівень

Політика інформаційної безпеки верхнього рівня фактично є декларацією керівників і/або власників підприємства про необхідність вести цілеспрямовану роботу із захисту інформаційних ресурсів, що має стати основою для більш успішного функціонування підприємства в основному напрямку його діяльності, а також усунути різні ризики, які можуть призвести до фінансових втрат, збитку для репутації підприємства, адміністративному і кримінальному переслідуванню керівників та інших негативних наслідків.

Політика інформаційної безпеки на цьому рівні може визначати й описувати:

- власне рішення про здійснення цілеспрямованої систематичної діяльності щодо забезпечення інформаційної безпеки підприємства;
- перелік основних інформаційних ресурсів, таких як інформаційні системи, масиви даних, інформація про окремі факти та явища (конструкторських розробках, комерційних угодах, результатах НДДКР тощо), захист яких має найбільший пріоритет для всього підприємства;
- загальний підхід до розподілу відповідальності за забезпечення інформаційної безпеки всередині організації;
- необхідність для всього персоналу дотримуватися певних запобіжних заходів при роботі з інформацією та інформаційними системами, підвищувати свою кваліфікацію в даній області і усвідомлювати міру відповідальності за можливі порушення;
- відношення керівництва підприємства до фактів порушення вимог щодо забезпечення інформаційної безпеки та осіб, що чинять такі порушення, а також загальний підхід до їх переслідування в разі виявлення таких фактів.

Одним із завдань політики верхнього рівня є формулювання і демонстрація того, що захист інформації є одним з ключових механізмів забезпечення конкурентоспроможності підприємства та обумовлює як його здатність досягати поставлених цілей, так іноді і здатність виживання і збереження можливості продовжувати діяльність. Для цього можуть бути позначені пріоритетні

напрямки господарської діяльності та відповідні їм інформаційні системи і потоки інформації, описаний причинно-наслідковий зв'язок між можливими порушеннями конфіденційності та/або порушеннями в стабільній роботі інформаційних систем, з одного боку, та порушеннями нормального ходу поточних господарських операцій, з іншого боку. На основі цього можуть бути визначені пріоритетні напрямки діяльності щодо забезпечення інформаційної безпеки. Найбільшою мірою залежність загальної ефективності діяльності від інформаційної безпеки характерна для таких компаній, які:

- займаються т.зв. електронною комерцією або працюють у суміжних сферах (електронні платежі, Інтернет-реклама тощо);
- безпосередньо пов'язані з обігом (створенням, купівлею-продажем, охороною, оцінкою) об'єктів інтелектуальної власності і, зокрема, наукомістких технологій;
- безпосередньо пов'язані із обігом великих обсягів інформації, що становить таємницю інших осіб (банки, медичні установи, аудиторські компанії тощо).

При цьому робота над політикою інформаційної безпеки повинна включати в себе не тільки її початкову розробку, але й постійний моніторинг загроз, змін у зовнішньому середовищі для подальшого уточнення (або навіть повної переробки) політики відповідно до змінення умов роботи.

Політика інформаційної безпеки підприємства: середній рівень

Політики інформаційної безпеки середнього рівня безпосередньо деталізують вимоги, завдання та правила, позначені в політиці верхнього рівня, і окремо описують основні сфери, в яких необхідне системне здійснення тих чи інших організаційних і/або технічних заходів.

Політика інформаційної безпеки середнього рівня повинна містити наступні основні розділи.

- Загальний опис тієї сфери діяльності (інформаційної технології, аспекту інформаційної системи, бізнес-процесів підприємства), на яку вона поширюється.
- Область застосування політики безпеки - перелік всіх осіб, організацій, інформаційних систем, до яких вона застосовується або які виключаються зі сфери її застосування.
- Безпосереднє відношення підприємства до даного аспекту інформаційних технологій та інформаційної безпеки - основна частина політики безпеки, що визначає конкретні правила, критерії та вимоги до процедур обігу інформації, елементів інформаційної інфраструктури, програмних і апаратних засобів тощо

- Розподіл ролей і функцій, необхідних для вирішення конкретних питань – закріплення за певними співробітниками (фахівцями, керівниками) обов'язків з виконання необхідної роботи з метою вирішення завдань в рамках даної політики безпеки.
- Порядок вирішення питань , що виникають, – під час основних процедур вирішення з'являються труднощі у поточній роботі і прийняття рішень про можливі винятки з загальних правил, а також перелік осіб (підрозділів), відповідальних за безпосередню роботу з персоналом підприємства з питань, що належать до даної політики безпеки.

Однією з основ для реалізації заходів у сфері інформаційної безпеки і детальної розробки політики безпеки є укрупнена класифікація інформаційних ресурсів, наявних на підприємстві. Усі наявні на підприємстві інформаційні об'єкти (і відповідні елементи інформаційної інфраструктури), як правило, можуть бути розділені на п'ять або шість основних груп за рівнем своєї значущості і конфіденційності.

1. Критично важлива (абсолютно секретна) інформація – інформація, що вимагає особливих гарантій безпеки.
2. Важлива інформація (інформація, що становить комерційну таємницю) – інформація, яка використовується тільки всередині підприємства, порушення конфіденційності якої може завдати серйозної шкоди самому підприємству або його партнерам.
3. Значна (конфіденційна) інформація – інформація, призначена для використання обмеженим колом співробітників і керівників підприємства.
4. Персональна інформація – інформація про співробітників, що не підлягає розголошенню.
5. Інформація для внутрішнього використання – інформація для використання всередині підприємства, порушення конфіденційності якої не може завдати шкоди.
6. Інша інформація – відкрита інформація, конфіденційність якої не має особливого значення для діяльності підприємства.

У всьому обсязі політик середнього рівня необхідно виділити два їх основних види.

1. Політики, які відносяться до визначених сфер діяльності підприємства і відповідних інформаційних потоків (фінансів, комерційної діяльності тощо).

2. Політики, які відносяться до певних аспектів використання інформаційних технологій, організації інформаційних потоків та організації роботи персоналу на всьому підприємстві – незалежно від тієї сфери, де використовуються ці технології або зайнятий персонал.

До політик **першого типу** можуть належати:

- політики поводження з інформацією, що становить державну таємницю;
- політики поводження з результатами науково-дослідної, конструкторської та технологічної документації, складової "ноу-хау" підприємства або його партнерів
- інші.

Політики безпеки такого типу уточнюють і доповнюють загальні для всього підприємства правила, що поширюються на всі інші інформаційні системи та об'єкти, і, відповідно, мають найбільший пріоритет. Вони, наприклад, можуть містити:

- спеціальні вимоги до резервного копіювання інформації (такі як більш висока частота резервного копіювання та використання більш надійних носіїв для цього);
- спеціальні вимоги до ідентифікації і автентифікації користувачів (такі як комбінування біометричної ідентифікації та ідентифікації за допомогою паролів);
- спеціальні вимоги до копіювально-розмножувальної техніки, використовуваної для роботи з конфіденційною інформацією;
- спеціальні вимоги до приміщень, в яких проводяться наради з секретної тематики і обробляється відповідна інформація (товщина і матеріал стін, розташування приміщень в будівлях, захищеність вікон, надійність дверей і замків, а також охоронної та пожежної сигналізації, обстеження на предмет виявлення підслуховуючих пристроїв тощо) та інші.

До політик **другого типу** можуть належати:

- політика опублікування відкритих інформаційних матеріалів, в тому числі політика організації веб-сайту підприємства і його внутрішнього інформаційного порталу (в частині запобігання можливих витоків і спотворень інформації);
- політика використання мережі Інтернет (у частині запобігання можливих витоків інформації);
- політики використання окремих інформаційних і комунікаційних технологій, у тому числі спільні для всього підприємства правила використання мобільних комп'ютерів і КПК, віддаленого доступу до

корпоративної інформаційної системи, а також використання особистих комп'ютерів співробітників підприємства в службових цілях;

- класифікації інформаційних систем, інформаційних ресурсів та об'єктів інформації з точки зору їх значимості і зусиль, які необхідно вживати для їх захисту;
- політика придбання, установки, модифікації та оновлення програмного забезпечення, а також аутсорсингу розробки і проектування програмного забезпечення;
- політика закупівлі апаратних засобів інформаційних систем, систем інформаційної безпеки;
- політика використання користувачами власного програмного забезпечення (тобто ПЗ, самостійно розробляється підприємством);
- загальні для всього підприємства правила використання паролів та інших засобів персональної ідентифікації;
- політика використання електронно-цифрового підпису та інфраструктури відкритих ключів;
- політика (регламент) забезпечення внутрішньо-об'єктного режиму і фізичної захищеності інформаційних активів;
- політика доступу до внутрішніх інформаційних ресурсів сторонніх користувачів (організацій);
- загальний для всього підприємства порядок притягнення до відповідальності за порушення певних правил інформаційної безпеки.

Політика інформаційної безпеки підприємства: нижній рівень

Даний рівень включає в себе документи, які є інструкціями і методиками прямої дії, що використовуються в повсякденній діяльності співробітників підприємства. Ці документи відносяться до окремих сервісів, процедур та інформаційних систем. Основним завданням розробки організаційної документації на цьому рівні є забезпечення якомога більш детального і формалізованого опису всіх процедур і вимог, що відносяться до забезпечення безпеки окремих елементів інформаційних систем, інформаційних потоків і масивів інформації. Зокрема, для забезпечення повноти формування політики інформаційної безпеки підприємства необхідно сформувати якомога більш повний комплект організаційної документації, що включає в себе:

- бланки типових заявок на надання доступу окремих співробітників до певних інформаційних ресурсів та інформаційних систем, а також регламенти надання такого доступу;
- регламенти (процедури) роботи з певними інформаційними і телекомунікаційними системами, програмним забезпеченням і базами

даних;

- посадові обов'язки окремих категорій співробітників щодо забезпечення інформаційної безпеки, а також вимоги, що пред'являються до персоналу;
- типові договори з зовнішніми контрагентами, пов'язані з передачею або отриманням інформації, або основні вимоги, що пред'являються до таких договорів.

Процедурні документи, які стосуються надання доступу до ресурсів (таких як мережа Інтернет, корпоративне інформаційні системи і бази даних, апаратні засоби, засоби передачі інформації тощо) можуть включати як типові бланки заявок на надання доступу, так і опис основних процедур (регламенту) прийняття рішень про надання такого доступу та надання конкретних прав при роботі з інформаційними ресурсами, а також переліки критеріїв, необхідних для надання тих чи інших прав в інформаційних системах.

Процедури роботи з окремими інформаційними системами і/або модулями інформаційних систем (базами даних, модулями корпоративної ERP-системи, системами електронного документообігу тощо) можуть перераховувати всі основні вимоги, правила і обмеження, наприклад, заборона використовувати дискети для копіювання та перенесення інформації або обмеження, що накладаються на можливість віддаленого доступу до тих чи інших інформаційних сервісів. Вимоги і правила, пов'язані із забезпеченням інформаційної безпеки, можуть бути включені як в загальні інструкції по використанню інформаційних систем або регламенти здійснення бізнес-процесів, так і в оформлені у вигляді спеціальних інструкцій і пам'яток, що містять виключно вимоги і правила інформаційної безпеки.

Посадові обов'язки персоналу підприємства, пов'язані із забезпеченням інформаційної безпеки, повинні входити до посадових інструкцій для кожного співробітника. Крім того, політика безпеки може передбачати підписання (як під час вступу на роботу або переведенні на певну посаду, так і при звільненні з неї) окремими категоріями персоналу додаткових угод, зобов'язань і підписок про нерозголошення певної інформації. Також політика безпеки може вводити додаткові вимоги до персоналу, що працює з певними відомостями або інформаційними системами. Прикладами таких обмежень можуть бути відсутність судимості, наявність певних навичок або спеціальної кваліфікації, проходження професійної сертифікації або психологічної перевірки.

Політики безпеки, що стосуються роботи з зовнішніми контрагентами, можуть передбачати типові форми і окремі інструкції щодо складання комерційних контрактів (для кожного типу контрактів, а також для окремих груп контрагентів) і обміну інформацією з постачальниками, покупцями,

консультантами, посередниками, субпідрядниками, постачальниками фінансових та інформаційних послуг та іншими учасниками господарської діяльності. Зокрема, в політиці для кожної з цих категорій може передбачатися специфічний порядок інформаційного обміну, взаємні вимоги щодо забезпечення конфіденційності і можливих заходів відповідальності в разі порушення узгоджених вимог будь-якої зі сторін.

У тих випадках, коли певна політика безпеки описує складну інформаційну систему і систему захисту інформації, призначену для виконання найбільш відповідальних операцій (таких як, наприклад, електронні грошові перекази), вона може бути розділена на дві складові:

- внутрішній регламент роботи підрозділів (груп, адміністраторів), що відповідають за виконання найбільш важливих адміністративних функцій (наприклад, видача та обслуговування електронних сертифікатів Інфраструктури публічних ключів);
- політику, яка безпосередньо відображає вимоги до користувачів і процесів, а також опису процедур роботи та взаємодії всіх учасників інформаційного обміну.

7.3 Зміст деталізованої політики безпеки

Політика інформаційної безпеки – набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації. Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора – організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Розглянемо основний зміст розділів політики безпеки за окремими напрямами захисту інформації.

7.3.1. Організація режиму охорони приміщень

Організація внутрішньооб'єктного режиму, охорони приміщень і територій є частиною загальної роботи підприємства щодо забезпечення збереження майна та безперервності поточної діяльності. Основним завданням забезпечення внутрішньооб'єктного режиму є недопущення сторонніх осіб до інформаційних активів і запобігання загроз інформаційній безпеці.

Основою внутрішньооб'єктного режиму є пропускний режим, в рамках якого, як правило, встановлюються:

- документи, що дають право проходу на територію підприємства – як пропуску і карти доступу, видані самим підприємством, так і документи, видані сторонніми організаціями (наприклад, службові посвідчення посадових осіб деяких органів державної влади);
- категорії перепусток, які використовуються на підприємстві, відповідно до яких обмежується термін дії перепусток, час можливого проходу на територію підприємства (дні тижня, години доби) і деякі інші параметри;
- порядок видачі, обміну, продовження і вилучення перепусток, а також порядок дій співробітників і посадових осіб при втраті пропуску;
- порядок організації пропуску осіб, автотранспорту і проносу (провозу) майна: розміщення і порядок роботи контрольно-пропускних пунктів, можливість пропуску тих чи інших осіб, засобів автотранспорту і вантажів через ті чи інші КПП та ін .;
- основні положення документообігу, використовуваного при проході відвідувачів на територію підприємства - вимоги до ведення журналу реєстрації проходу відвідувачів, вимоги до документів, на основі яких видаються разові перепустки, порядок видачі разових перепусток і т.п.;
- порядок огляду транспортних засобів, що допускаються на територію підприємства.

Крім того, в рамках організації внутрішньооб'єктного режиму може бути передбачено поділ приміщень і територій на окремі зони з обмеженням доступу (в тому числі на основі поділу приміщень і територій на різні категорії), а також розмежування доступу окремих співробітників (категорій персоналу) і відвідувачів в різні зони; також можуть бути визначені основні вимоги до технічних засобів розмежування доступу і організації їх використання.

З технічної точки зору заходи щодо забезпечення пропускного та внутрішньооб'єктного режимів можуть бути реалізовані тими ж засобами, які використовуються для забезпечення безпеки в інших сферах, крім інформаційної (захист майна та персоналу, забезпечення безперервності виробничого процесу), – засобами контролю доступу, відеоспостереження, сигналізації і фізичного захисту.

В основі засобів контролю доступу лежать механізми розпізнавання особистості і порівняння з встановленими параметрами. Політика підприємства може встановлювати як спрощені підходи до розпізнання, коли охоронці підприємства перевіряють документи (підтвердження особи, підтвердження можливості проходу на територію в даний час через даний КПП), так і

використання автоматизованих засобів, коли впізнання відвідувача і підтвердження (або заборона) можливості проходу на територію (виходу з території, з будівлі) проводиться автоматизованою системою контролю доступу на основі наявних у відвідувача машинозчитних засобів персональної ідентифікації (пластикових карт, жетонів тощо) або на основі зчитування і аналізу його фізичних особливостей (геометрії особи, відбитків пальців, малюнка райдужної оболонки ока, голосу і т.п.).

При виборі конкретних засобів біометричної ідентифікації фахівцям і керівникам підприємства слід пам'ятати, що різні технології мають різну ступінь надійності, а також можуть бути більш-менш зручними в повсякденному використанні великою кількістю людей. Так, наприклад, вважається, що одна з передових технологій біометричної ідентифікації – ідентифікація по кровоносним судинам пальця (коли інфрачервоний промінь просвічує палець і створює тривимірне зображення унікальної для кожної людини структури кровоносних судин).

7.3.2. Фізичний захист

Фізичний захист об'єктів, як правило, передбачає посилення конструкцій огорож, елементів будівель, споруд і окремих приміщень. До таких засобів відносяться захист віконних прорізів металевими гратами і віконницями, спеціальне скління вікон, використання броньованих дверей, запірних пристроїв, сейфів для зберігання коштів обчислювальної техніки і носіїв інформації. Відповідно до особливостей використовуваних приміщень і територій політика безпеки підприємства також може передбачати розташування місць зберігання і обробки інформації (наприклад, архівів або серверних кімнат) в приміщеннях, найменш доступних для проникнення, найбільш віддалених від місць зберігання вибухонебезпечних і легкозаймистих речовин, найменш схильних до затоплення (для об'єктів розташованих в долинах річок і на узбережжі), найбільш захищених від ударів блискавки і т.п.

З фізичним захистом безпосередньо пов'язано використання засобів сигналізації та відеоспостереження. Залежно від характеру об'єкту, що охороняється (територія, будівля, прохід, приміщення, окремий шафа або сейф) в засобах сигналізації можуть застосовуватися датчики, що працюють на різних фізичних принципах (фотоелектричні датчики, датчики обсягу, акустичні датчики і т.п.), що мають різні настройки і використовують різні канали зв'язку.

На відміну від засобів сигналізації засоби відеоспостереження дозволяють не тільки встановити факт порушення, а й в деталях відстежувати його, контролювати ситуацію, а також вести відеозапис, який можна буде

використовувати для прийняття подальших заходів (пошук порушників, кримінальне переслідування і т.п.).

Окремим завданням є забезпечення інформаційної безпеки при процесі транспортування носіїв інформації та інших об'єктів, що вимагає використання як спеціальних організаційних прийомів, так і спеціальних технічних засобів. До організаційних методів відноситься залучення спеціально підготовлених кур'єрів, а також поділ носіїв інформації (об'єктів) на частини і їх роздільне транспортування з метою мінімізації можливостей витоку інформації. До технічних засобів, що застосовуються при транспортуванні об'єктів, відносяться захищені контейнери, спеціальні пакувальні матеріали, а також тонкоплівкові матеріали і голографічні мітки, що дозволяють ідентифікувати справжність об'єктів і контролювати несанкціонований доступ до них.

7.3.3. Організація режиму секретності в установах і на підприємствах

Організація режиму секретності в установах і на підприємствах ґрунтується на вимогах законодавства, що стосується питань державної таємниці, і відповідних підзаконних актів. Відповідно до діючих норм до державної таємниці може бути віднесена інформація, що стосується обороноздатності країни, її економіки, міжнародних відносин, державної безпеки та охорони правопорядку (в тому числі відомості про методи та засоби захисту секретної інформації, а також про державні програми і заходи в області захисту державної таємниці); в законодавстві також спеціально уточнюються області діяльності, інформація про які не може бути віднесена до державної таємниці. Віднесення конкретної інформації до державної таємниці здійснюється рішенням спеціально призначених посадових осіб, а загальний Перелік відомостей, віднесених до державної таємниці, затверджується Президентом і підлягає обов'язковому опублікуванню. Для відомостей, що становлять державну таємницю, встановлюються три ступені секретності: "особливої важливості", "цілком таємно" та "таємно", а носії таких відомостей (документи) повинні мати відповідні реквізити.

Основним елементом організації режиму секретності є допуск посадових осіб і громадян до відомостей, що становлять державну таємницю. Він передбачає виконання керівництвом підприємства і підрозділів із захисту державної таємниці (у взаємодії з уповноваженими правоохоронними органами) наступних основних заходів.

- Ознайомлення посадових осіб і громадян з нормами законодавства, які передбачають відповідальність за порушення вимог.
- Отримання згоди на тимчасові обмеження їх прав відповідно до

законодавства.

- Отримання згоди на проведення щодо них перевірочних заходів.
- Прийняття рішення про допуск до відомостей, що становлять державну таємницю.
- Висновок щодо осіб, які отримали допуск, що відображає взаємні зобов'язання таких осіб і адміністрації підприємства (в т.ч. зобов'язання таких осіб перед державою з нерозповсюдження довірених їм відомостей, що становлять державну таємницю).

Крім віднесення відомостей до державної таємниці та допуску посадових осіб і громадян до засекречених відомостей, важливим елементом системи забезпечення режиму секретності є організація інформаційного обміну між підприємствами при спільному виконанні робіт. Зокрема, передача засекречених відомостей від одного підприємства до іншого повинна проводитися з дозволу уповноваженого державного органу, договір на виконання робіт повинен передбачати зобов'язання сторін щодо забезпечення схоронності відомостей, а замовник робіт повинен контролювати виконання нормативних вимог контрагентами за такими договорами (наявність ліцензій, оформлення допуску співробітників і т.п.) і вживати необхідних заходів у разі виявлення порушень. Також важливим елементом забезпечення режиму секретності є організація передачі відомостей, що становлять державну таємницю, іншим державам (в тому числі ознайомлення з такими відомостями і надання можливості доступу до них).

Політика опублікування матеріалів у відкритих джерелах (таких як газети, журнали, виставки, мережа Інтернет, радіо- і телепередачі, конференції, музейні експозиції і т.п.) повинна забезпечувати запобігання випадкових і організованих витоків конфіденційної інформації при взаємодії підприємства із засобами масової інформації, громадськими і державними органами, науковими, академічним і бізнес-спільнотою. Для того щоб уникнути шкоди інтересам підприємства, така політика повинна містити основні правила і процедури підготовки інформаційних матеріалів до відкритої публікації. Зокрема, в політиці безпеки слід передбачати створення спеціальної експертної ради, відповідальної за розгляд всіх інформаційних матеріалів, які передбачається опублікувати у відкритих джерелах (політика безпеки повинна містити конкретні обмеження на опублікування інформаційних матеріалів без їх розгляду експертною радою). Основним завданням такої ради є підготовка висновків про можливість або неможливість опублікування певних інформаційних матеріалів, а також підготовка конкретних пропозицій щодо вилучення певних відомостей з матеріалів, підготовлених до публікації. При відсутності єдиної думки у членів експертної комісії рішення про можливість

опублікування може бути прийнято керівником підприємства з урахуванням рекомендацій експертів. Для ефективного вирішення завдань члени експертної ради повинні детально знати всі існуючі обмеження (зокрема, встановлені законодавством) і володіти ситуацією в тій сфері, в якій функціонує підприємство. При цьому, як правило, сам автор підготовлених до публікації матеріалів не може входити до експертної ради, а редактор або керівник, який відповідає за підготовку матеріалів, не може бути головою експертної ради.

Політика управління паролями (або, в більш загальному вигляді, політика ідентифікації і аутентифікації) може визначати періодичність заміни паролів, дії, які необхідно здійснити при компрометації паролів, основні вимоги до їх якості, процедур їх генерації, розподілу основних обов'язків, пов'язаних з генерацією паролів, їх зміною і доведенням до користувачів, а також основні заходи відповідальності за порушення встановлених правил і вимог. Політика на цьому рівні також може встановлювати заборону зберігання записаних паролів, заборона повідомляти будь-кому свій пароль (в тому числі керівникам і адміністраторам інформаційних систем) та інші аналогічні обмеження.

Політика встановлення та оновлення версій програмного забезпечення може включати в себе деякі обмеження на самостійне придбання і установку програмного забезпечення окремими підрозділами та користувачами, а також певні вимоги до кваліфікації фахівців, які здійснюють їх установку, настройку і підтримку.

Політика придбання інформаційних систем і їх елементів (програмних і апаратних засобів) може включати в себе вимоги до ліцензування та сертифікації використовуваного програмного забезпечення і устаткування, а також певні вимоги до фірм, які здійснюють їх поставку та впровадження.

Політика доступу сторонніх користувачів (організацій) в інформаційні системи підприємства може містити перелік основних ситуацій, коли такий доступ можливий, а також основні критерії і процедури, відповідно до яких здійснюється доступ. Також політика може передбачати розподіл відповідальності співробітників самого підприємства за дії зовнішніх користувачів, які отримують такий доступ.

Політика щодо розробки ПЗ може містити вимоги як до питань безпеки і надійності програмних засобів, самостійно розроблених підприємством, так і щодо передачі розробки програмних засобів (модулів інформаційних систем, окремих програмних бібліотек і т.п.) стороннім спеціалізованим організаціям (т.зв. "аутсорсинг"), а також щодо придбання та використання тиражованих програмних бібліотек (модулів), які розповсюджуються компаніями-виробниками. Зокрема, політика може містити вимоги до тестування самостійно

розробленого ПЗ, аналізу його вихідних кодів, описувати основні критерії надійності і т.п.

Політики використання окремих універсальних інформаційних технологій в масштабі всього підприємства можуть включати в себе:

- політику використання електронної пошти (e-mail);
- політику використання засобів шифрування даних;
- політику захисту від комп'ютерних вірусів і інших шкідливих програм;
- політику використання модемів і інших аналогічних комунікаційних засобів;
- політику використання інфраструктури публічних ключів;
- політику використання технології віртуальних приватних мереж (Virtual Private Network - VPN).

Політика використання електронної пошти може включати в себе як загальні обмеження на її використання певними категоріями співробітників, так і вимоги до управління доступом і збереження конфіденційності повідомлень, а також до адміністрування поштової системи і зберігання електронних повідомлень. Крім того, політика може передбачати:

- заборону на використання електронної пошти в особистих цілях;
- спеціальні вимоги до відправлення та одержання приєднаних файлів, які потенційно можуть містити шкідливі програми;
- заборону на використання електронної пошти тимчасовими співробітниками;
- вимоги шифрування переданих повідомлень;
- спостереження за всіма переданими і одержуваними повідомленнями;
- обмеження на передачу конфіденційної інформації за допомогою електронної пошти та інші положення.

Політика використання комунікаційних засобів може визначати межі використання технологій, що дозволяють підключити комп'ютери та інформаційні системи підприємства до інформаційних систем і комунікаційних каналів за його межами.

Зокрема, така політика може вводити певні обмеження на використання модемів для телефонних ліній, пристроїв, що використовують сучасні бездротові технології, такі, як GSM (GPRS), Wi-Fi, передача даних в мережах стандарту CDMA і т.п.

Політика використання мобільних апаратних засобів може ставитися до різних пристроїв, таким як мобільні ПК, КПК (PDA), переносні пристрої зберігання інформації (дискети, USB-flash, карти пам'яті, що підключаються жорсткі диски і т.п.). Вона може відображати загальне ставлення підприємства до використання співробітниками таких пристроїв, визначати вимоги і

встановлювати конкретні області, в яких їх використання допустимо. Також можуть встановлюватися додаткові загальні вимоги до стаціонарного обладнання з метою обмеження підключення до них мобільних комп'ютерів і засобів передачі даних.

7.4 Департамент інформаційної безпеки і робота з персоналом

Робота департаменту інформаційної безпеки є основною структурною одиницею, що відповідає за комплексний захист інформації на підприємстві. Внутрішня структура департаменту, основні завдання та напрями його діяльності, методи роботи, основні аспекти роботи з персоналом підприємства, спрямованої на захист інформаційних активів (як в частині підбору і розстановки співробітників, пов'язаних з обробкою інформації, так і в частині поточної роботи з персоналом) є важливими завданнями департаменту інформаційної безпеки.

7.4.1. Департамент інформаційної безпеки

Департамент інформаційної безпеки (далі – департамент) підприємства є самостійним структурним підрозділом підприємства, безпосередньо виконує ключові функції захисту інформаційних ресурсів.
Його основними завданнями, як правило, є:

- організація та координація робіт із забезпечення комплексного захисту інформації на підприємстві;
- контроль за виконанням встановлених вимог та оцінка ефективності роботи підрозділів і персоналу підприємства щодо забезпечення інформаційної безпеки;
- виконання окремих адміністративних і технічних функцій щодо забезпечення інформаційної безпеки;
- формування, підтримка та документальне забезпечення політики інформаційної безпеки на всіх рівнях;
- впровадження різних засобів захисту інформації;
- адміністрування окремих інформаційних систем.

Склад завдань департаменту і його внутрішня організаційна структура в кожному конкретному випадку визначається такими особливостями функціонування підприємства, як:

- значимість інформаційних ресурсів у роботі підприємства і характер існуючих загроз;

- ставлення керівництва і власників підприємства до питань інформаційної безпеки та їх управлінська кваліфікація;
- функціональність і характер використовуваних інформаційних систем, їх роль у бізнес-процесах;
- організація роботи та структура IT-служби;
- фінансовий стан підприємства.

Таким чином, рішення про склад і структуру департаменту в кожному випадку має бути індивідуальним і враховує всі основні умови.

Функції, пов'язані **з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства,** можуть включати в себе:

- консультування керівників і власників підприємства з питань розробки та вдосконалення політики інформаційної безпеки;
- самостійну розробку політики безпеки, її узгодження і подання її керівництву підприємства для затвердження, а також внесення необхідних змін у міру зміни умов роботи підприємства;
- самостійну розробку політик безпеки, що стосуються окремих питань захисту інформації (правил застосування телекомунікаційних технологій, вимог, обов'язкових для всіх персональних комп'ютерів, що використовуються на підприємстві, тощо);
- формування вимог і регламенту процедур перегляду політики безпеки, окремих правил, типових форм та інших документів;
- аналіз окремих договорів і угод зі сторонніми організаціями (постачальниками, покупцями, партнерами по проведенню науково-дослідних робіт тощо) на предмет відповідності вимогам політики інформаційної безпеки;
- аналіз та узагальнення передового досвіду та сучасних теорій у сфері управління інформаційною безпекою з метою їх практичного застосування на підприємстві;
- залучення сторонніх фахівців, дослідників, консультантів (консалтингових компаній) для розробки та вдосконалення політики безпеки підприємства та впровадження розвинених методів управління в цій сфері;
- управління навчанням персоналу компанії (контроль за повнотою та правильністю матеріалів навчальних програм, пов'язаних з інформаційною безпекою, забезпечення своєчасності проходження навчання тощо);
- консультування фахівців та керівників підрозділів підприємства з питань відповідності розроблюваних внутрішніх документів окремих

підрозділів вимогам політики безпеки підприємства;

- контроль відповідності внутрішніх організаційних документів підприємства (правил внутрішнього розпорядку, посадових інструкцій, інструкцій з використання інформаційних систем, типових форм договорів тощо) вимогам політики інформаційної безпеки, а також узгодження таких документів при їх затвердженні.

Функції, пов'язані з **впровадженням засобів захисту інформації,** можуть включати в себе:

- аналіз сучасних програмних і апаратних засобів захисту інформації та пов'язаних з ними методик захисту, а також ринку доступних засобів захисту інформації, що застосовуються для різних цілей, і підготовка обгрунтованих пропозицій щодо придбання певних продуктів у певних постачальників;
- аналіз закуповуваних інформаційних систем (операційних систем, прикладних програм, телекомунікаційного устаткування, обчислювальної техніки тощо) на предмет їхньої потенційної надійності і наявності вразливостей;
- залучення сторонніх експертів і консультантів для аналізу закуповуваних і використовуваних засобів захисту інформації з точки зору їх надійності, а також з точки зору доцільності їх застосування (впровадження);
- формулювання вимог (пов'язаних із забезпеченням інформаційної безпеки) до самостійно розроблюваних програмних продуктів або програмного забезпечення, що створюється на замовлення сторонніх розробників;
- участь у проектуванні нових інформаційних систем, а також тестуванні знову розроблених і впроваджуваних програмних продуктів;
- розробку техніко-економічного обґрунтування для проектів впровадження засобів захисту інформації, а також залучення для цих цілей сторонніх аналітиків і консультантів, що спеціалізуються на питаннях аналізу засобів захисту інформації;
- підготовку обгрунтованих рішень про вибір між самостійною розробкою засобів захисту інформації (наприклад, програмних модулів, що здійснюють шифрування даних) і передачею їх розробки стороннім компаніям.

Функції, пов'язані з адмініструванням **інформаційних систем і систем захисту інформації** можуть включати в себе:

- виконання деяких функцій з адміністрування окремих інформаційних систем (баз даних, систем колективної роботи з документами, поштових систем тощо), а також адміністрування та конфігурування систем захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо);
- визначення необхідних типових налаштувань і конфігурацій робочих станцій (персональних комп'ютерів), що мають відношення до інформаційних систем підприємства (зокрема, підключених до його локальної мережі);
- залучення сторонніх організацій для здійснення поточного адміністрування інформаційних систем і систем захисту інформації, а також для консультаційної та технічної підтримки при виникненні інцидентів, пов'язаних з інформаційною безпекою (зокрема, при здійсненні нападів на інформаційні системи підприємства);
- установку (в тому числі і спільно з фахівцями IT-підрозділу) програмних і апаратних засобів захисту інформації на робочі місця користувачів і в інші елементи інформаційних систем;
- консультування користувачів з питань, пов'язаних з інформаційною безпекою, і оперативне вирішення проблем;
- реагування на різні інциденти, пов'язані з порушенням інформаційної безпеки;
- прийняття активних зустрічних заходів при виявленні вторгнень в інформаційну систему (інформування правоохоронних органів, самостійний пошук нападників тощо);
- генерування паролів користувачів інформаційних систем та забезпечення їх збереження;
- участь у відновленні працездатності інформаційних систем після збоїв та порушень у роботі.

Функції, пов'язані з **контролем виконання вимог політики інформаційної безпеки та проведення аудитів** можуть включати в себе:

- збір та аналіз відомостей про порушення різних вимог політики безпеки, що надходять з різних джерел (у тому числі і від адміністраторів інформаційних систем) і визначення пріоритетних напрямів контрольної роботи;
- перевірку організаційної документації окремих підрозділів підприємства на предмет відповідності вимогам політики інформаційної безпеки (у тому числі і своєчасності внесення всіх необхідних змін до чинних внутрішніх документів організації);
- перевірку стану (правильності ведення) поточної господарської та

кадрової документації окремих підрозділів підприємства, пов'язаної із забезпеченням інформаційної безпеки (правильності і своєчасності заповнення журналів, своєчасність оформлення зобов'язань про нерозголошення відомостей співробітниками тощо);
- проведення комплексних аудитів інформаційної безпеки на підприємстві;
- організацію контрольних перевірок захищеності окремих елементів інформаційних систем (серверів, сегментів мережі тощо);
- залучення сторонніх організацій для проведення аудитів інформаційної безпеки на підприємстві, перевірок надійності інформаційних систем.

Крім перерахованих функцій, безпосередньо пов'язаних із захистом інформаційних ресурсів, також велике значення має виконання функцій, пов'язаних з охороною майна підприємства і вирішенням завдань, які пов'язані з забезпеченням безпеки підприємства у більш широкому сенсі. Зокрема, для забезпечення інформаційної безпеки має значення виконання таких функцій як:

- охорона території та майна підприємства, а також охорона персоналу;
- забезпечення дотримання пропускного режиму;
- спостереження за територією і приміщеннями (у тому числі за допомогою відеокамер);
- контроль за ввезенням на територію підприємства та вивезенням готової продукції, матеріалів, документів та іншого майна;
- організацію внутрішніх службових перевірок та розслідувань, а також взаємодію з правоохоронними органами;
- контроль за дотриманням тимчасового режиму роботи, а також за дотриманням правил внутрішнього розпорядку.

7.4.2. Організаційна структура та персонал департаменту інформаційної безпеки

На практиці департамент є підрозділом, або безпосередньо підпорядковується першій особі підприємства, або входить, як структурна одиниця, в службу безпеки підприємства. Співробітники департаменту знаходяться в адміністративному та функціональному підпорядкуванні у керівника департаменту, який несе відповідальність за забезпечення інформаційної безпеки на підприємстві. Висновок департаментів інформаційної безпеки зі структури IT-служб на підприємствах є однією з важливих сучасних тенденцій в управлінні бізнесом, інформаційними технологіями та інформаційною безпекою, тому, на думку деяких фахівців, у цих підрозділів є

деякі частково взаємосуперечні інтереси і тому деякі завдання не можуть бути ефективно вирішені в рамках одного структурного підрозділу.
У складі департаменту для підвищення ефективності роботи можуть бути виділені самостійні групи (відділи), що спеціалізуються на виконанні певних функцій:

- відділ (група, бюро) нормативної (організаційної) документації;
- відділ (група, бюро) адміністрування інформаційних систем;
- відділ (група, бюро) аудиту інформаційної безпеки;
- відділ (група, бюро) впровадження інформаційних систем і систем захисту інформації.

Відділ нормативної документації вирішує завдання, пов'язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства, і повинен, головним чином, включати в себе фахівців з менеджменту та бізнес-аналізу, що пройшли додаткову підготовку у сфері управління інформаційною безпекою. Також до складу такого відділу можуть входити юристи. Аналогічний кадровий склад може бути і у **Відділу внутрішнього аудиту інформаційної безпеки.** При цьому до кваліфікації співробітників Відділу нормативної документації, як правило, повинні пред'являтися набагато більш високі професійні вимоги.

Відділ адміністрування інформаційних систем, а також **Відділ впровадження інформаційних систем і захисту систем інформації,** як правило, повинні включати в себе фахівців з інформаційних технологій та засобів захисту інформації, що мають значний досвід впровадження та експлуатації корпоративних інформаційних систем.

7.4.3. Робота з персоналом підприємства

Практична реалізація всіх положень сформованої політики інформаційної безпеки потребують від підприємства тривалих практичних зусиль. Одним з основних і найбільш складних напрямків роботи є робота з персоналом, цілі якої:

- відбір і попередня перевірка персоналу, прийнятого на роботу (на службу);
- навчання співробітників;
- досягнення взаєморозуміння керівників і співробітників в питаннях забезпечення інформаційної безпеки;
- психологічна підготовка з метою протистояння методам т.зв. "соціальної інженерії".

Основною причиною, що визначає значущість людського фактора в загальній системі захисту інформації, є те, що при всій розвиненості сучасних

засобів автоматизації інформаційні системи як і раніше представляють собою людино-машинні комплекси і їх функціонування багато в чому залежить від роботи окремих людей. Саме з цієї причини неадекватне поводження службовців підприємства з компонентами інформаційної системи може завдати серйозної шкоди інформаційній безпеці навіть при наявності детально опрацьованих політик безпеки і високоефективних програмних і апаратних засобів захисту інформації.

Початкова стадія роботи - підбір і розстановка кадрів - може мати кілька аспектів. У першу чергу, основним критерієм для призначення на певні посади, пов'язані з роботою з відомостями, які становлять державну таємницю, є отримання відповідної форми допуску. Відповідно до вимог чинних нормативно-правових актів Перелік посад, при призначенні на які необхідно оформляти спеціальний допуск, встановлюється керівником підприємства і може періодично переглядатися. Ця вимога пов'язана, з одного боку, з тим, що керівник підприємства несе відповідальність за забезпечення режиму секретності, а з іншого – з тим, що для виконання функціональних обов'язків співробітникам підприємства необхідно працювати з певними відомостями і, відповідно, мати певний рівень допуску.

Також при підборі і розстановці кадрів можуть застосовуватися і менш формалізовані методи. Це можуть бути різні методики психологічної оцінки, що включають в себе:

- аналіз мотиваційних аспектів особистості;
- оцінку психологічної стійкості особистості;
- оцінку рівня пізнавальних здібностей особистості (успішність придбання нових знань і навичок і здатність до їх практичного застосування);
- оцінку активності особистості в досягненні поставленої мети, уміння об'єктивно оцінювати ситуацію і людей, вміння виробляти оптимальну стратегію поведінки.

Такого роду аналіз може бути необхідний як щодо фахівців і керівників, які працюють з інформацією, що підлягає захисту, у зв'язку з виконанням своїх посадових обов'язків за основним профілем роботи підприємства, так і фахівців і керівників, чиїм основним завданням є забезпечення інформаційної безпеки підприємства (аудиторів ІБ, проектувальників і адміністраторів інформаційних систем і систем захисту інформації тощо).

Крім ретельного підбору, однією з важливих основ роботи з персоналом є його навчання способам забезпечення інформаційної безпеки і безпечній роботі з інформаційними системами. Навчання і наступний контроль отриманих (наявних) знань може бути як первинним, так і повторним. У загальному випадку

співробітник підприємства не може бути допущений до виконання своїх посадових обов'язків і роботі з інформаційними системами доти, поки він не пройде навчання з питань інформаційної безпеки і не буде:

- детально ознайомлений з усіма діючими на підприємстві вимогами і загальними правилами;
- повністю навчений методам і прийомам забезпечення інформаційної безпеки, необхідним для виконання його посадових обов'язків;
- ознайомлений з усіма можливими заходами відповідальності (дисциплінарної, адміністративної, кримінальної), які можуть бути до нього застосовані в разі порушення вимог, а також у випадку нанесення шкоди за його вини.

У завершенні всієї попередньої роботи співробітник повинен дати всі необхідні зобов'язання про нерозголошення конфіденційних відомостей, а також письмово засвідчити, що він повністю ознайомлений з основними положеннями політики безпеки. У процесі роботи підприємство також може проводити періодичний контроль знань і навичок, пов'язаний із забезпеченням інформаційної безпеки з тією метою, щоб засвідчити компетентність працівників у цій сфері. Також одним з інструментів навчання може бути періодичне ознайомлення персоналу з реальними прикладами інцидентів, що недавно відбулися, пов'язаних з інформаційною безпекою. Крім того, додаткове навчання персоналу підприємства може проводитись у випадках:

- впровадження нових автоматизованих інформаційних систем;
- зміни бізнес-процесів підприємства;
- зміни вимог політик безпеки (наприклад, у зв'язку зі зміною вимог законодавства).

Необхідність додаткового навчання при впровадженні нових інформаційних систем і, зокрема, інтегрованих систем управління підприємством, як правило, може бути обумовлене появою нових функціональних можливостей програмного забезпечення і зміною процедур обробки інформації. Також доступ до інтегрованих інформаційних систем потенційно може дати доступ до раніше недоступної інформації та надати раніше відсутні можливості впливати на різні інформаційні потоки. У зв'язку з цим може виникнути потреба в тому, щоб співробітники мали додаткові зобов'язання про дотримання заходів інформаційної безпеки. Аналогічні організаційні заходи щодо забезпечення захисту інформації можуть бути необхідні і під час зміни бізнес-процесів підприємства, коли змінюється його структура, розподіл функцій між підрозділами і обов'язків співробітників, і відповідно, вносяться зміни в організаційні схеми, штатні розписи і посадові інструкції персоналу. Зміни вимог політики безпеки можуть бути пов'язані з появою нових загроз,

зміною законодавчих вимог, розширенням ринків, зміною ставлення керівництва і власників підприємства до питань інформаційної безпеки та іншими факторами, - всі ці уточнення і зміни також повинні своєчасно і в повному обсязі доводитися до персоналу.

У процесі навчання певну значимість може мати роз'яснення раціональних причин, з яких підприємство застосовує саме таку політику безпеки. Це може служити як для кращого розуміння та засвоєння положень політики безпеки, так і для певної розрядки психологічної напруженості.

Окремим напрямом навчання та підвищення кваліфікації може бути розвиток у персоналу компанії навичок протидії методам т.зв. соціальної інженерії. Використання для незаконного проникнення в інформаційні системи методів соціальної інженерії пов'язано з т.зв. "людським фактором", який являє собою сукупність певних психологічних схильностей і особливостей мислення і поведінки, які властиві практично всім людям. До числа таких схильностей і особливостей можна віднести:

- нездатність адекватно оцінити небезпеку в деяких ситуаціях;
- специфічне ставлення до подій, що відбуваються рідко (притуплення уваги);
- зайва довіра і покладання на засоби автоматизації;
- схильність до маніпулювання, що ґрунтується, наприклад, на бажанні допомогти людям (у тому числі і незнайомим) або на зайвій довірі людям, одягненим в спеціальну уніформу, тощо

Саме з використанням деяких психологічних особливостей такого роду здійснюється багато найбільш успішних (для нападників) проникненнь в корпоративні інформаційні системи. Прикладами таких проникнень є ситуації, коли зловмисник:

- здійснює телефонний дзвінок, представляється адміністратором і, пославшись на певні обставини (такі як збій в системі), просить повідомити йому пароль;
- приходить в офіс в спеціальній уніформі (наприклад, у формі співробітника компанії, займається обслуговуванням і ремонтом комп'ютерів) і просить надати йому доступ до інформаційної системи;
- надсилає повідомлення електронною поштою від імені адміністратора інформаційної системи або керівництва підприємства і просить повідомити пароль або вчинити певні дії.

Велику значимість у системі заходів з подолання впливу людського фактора має повсякденна робота з персоналом. Крім навчання персоналу і застосування дисциплінарних заходів впливу, одним з основних завдань такої роботи є постійне нагадування всім співробітникам про необхідність дотримання

правил інформаційної безпеки. Конкретні способи, за допомогою яких такі нагадування можуть бути зроблені, будуть залежати від уподобань керівників підприємства, сформованої корпоративної культури, специфіки бізнес-процесів та інших обставин. Характерними способами того, як підприємство може постійно нагадувати своїм співробітникам про необхідність дотримуватися обережності, є:

- розміщення та періодична зміна (оновлення дизайну та змісту) нагадувань про необхідність дотримуватися вимог політики інформаційної безпеки на предметах, які постійно перебувають у полі зору співробітників протягом робочого дня: настінних і настільних календарях, кавових чашках, обкладинках блокнотів, настільних експонатах, ручках, олівцях та іншому канцелярському приладді;
- періодична розсилка відповідних брошур, бюлетенів і буклетів, а також повідомлень по електронній пошті;
- використання скрінсейверів, що містять відповідні нагадування;
- використання голосової пошти і гучного зв'язку для періодичної передачі повідомлень про необхідність дотримання правил інформаційної безпеки тощо

Таким чином, комплекс всіх організаційних заходів по роботі з персоналом підприємства, що включає в себе систему навчання персоналу, систему притягнення порушників до відповідальності, і постійне підтримання атмосфери відповідального ставлення до питань безпеки, повинен в певній мірі зменшити негативний вплив людського фактора на захищеність інформаційних систем і стан інформаційної безпеки.

7.5. Організація реагування на інциденти

Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як і побудова системи захисту та запобігання порушень. Під інцидентом, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди.

7.5.1. Визначення інциденту

Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як

і побудова системи захисту та запобігання порушень. Під інцидентом, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди.

Надзвичайна ситуація (інцидент), пов'язана з порушенням інформаційної безпеки, може бути обумовлена:

- руйнівним впливом на весь майновий комплекс підприємства при виникненні стихійних факторів (повінь, пожежа, землетрус тощо) або цілеспрямованим нападом (підрив, підпал, руйнування будівель та приміщень тощо);
- негативним впливом виключно на інформаційні ресурси підприємства (як правило, здійснюваним віддалено, з використанням телекомунікаційних каналів).

У загальному випадку організаційні процедури (регламенти) реагування на надзвичайні ситуації повинні включати в себе:

- регламенти альтернативних процесів обробки інформації (у тому числі, можливо, і без використання засобів автоматизації) на період виходу з ладу основних інформаційних ресурсів;
- визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації, а також визначення процедур взаємодії між групами і окремих груп з керівництвом підприємства;
- технічну та організаційну документацію, необхідну для відновлення інформаційних систем і даних після надзвичайної ситуації;
- порядок зберігання архівних (резервних) копій даних і програмних додатків обробки даних в місцях, захищених від механічних впливів, крадіжок, повеней, пожеж;
- угоди з постачальниками програмних і апаратних засобів, що входять в інформаційну інфраструктуру підприємства, про термінову поставку компонент, що вийшли з ладу і вимагають заміни в випадку надзвичайної ситуації.

Далі в даному розділі найбільш докладно розглядаються інциденти, причиною яких є навмисно здійснювані напади на інформаційні ресурси підприємства.

Процес реагування на такого роду інциденти включає в себе чотири основні етапи:

- виявлення нападу;
- локалізація нападу;

- ідентифікація нападників;
- оцінка і подальший аналіз процесу нападу і його обставин.

7.5.2. Виявлення атак і розпізнавання вторгнень

Виявлення атак і розпізнавання вторгнень, як правило, є інженерно-технічним завданням, що вирішується за допомогою спеціальних програмних і іноді апаратних засобів. Зокрема, виявлення може здійснюватися на основі аналізу мережевого трафіку і журналів (лог-файлів), в яких фіксуються різні дії. Виявлення може здійснюватися на основі сигнатур – формалізованих наборів ознак певних вірусів, типів атак тощо Також, очевидно, джерелом інформації про порушення є повідомлення користувачів про відхилення в роботі інформаційних систем і поява явних негативних наслідків порушень, що сталися.

Для забезпечення своєчасного виявлення порушень підприємство повинно організувати постійну (при необхідності – цілодобову) роботу фахівців, що відповідають за вирішення інцидентів. Для цього може бути вибраний один з можливих підходів.

Організація власної чергової служби, що складається з компетентних фахівців, що несуть позмінне чергування і оснащені засобами мобільного зв'язку.

Залучення сторонньої організації, що спеціалізується на наданні подібних послуг.

При цьому співробітники підприємства повинні знати номери телефонів та інші способи зв'язку, за допомогою яких вони могли б оперативно повідомляти черговим фахівцям про всі події.

Виявлення порушень може бути здійснено не тільки за явними ознаками, такими як повідомлення користувачів про припинення функціонування окремих елементів інформаційних систем, одночасне використання одного облікового запису на кількох робочих станціях або явне виявлення вірусів в даних, переданих локальною мережею, але й за деякими непрямими ознаками (аномальними явищами), які в окремих випадках можуть свідчити (а можуть і не свідчити) про порушення. Прикладами таких непрямих свідчень можуть бути:

- використання інформаційних систем і певних облікових записів в нехарактерний час (рано вранці, пізно ввечері тощо);
- різке нехарактерне підвищення навантаження на інформаційні системи або їх окремі елементи (сегменти мережі, сховища даних і т.п.);
- зміна характеру поведінки користувачів (наприклад, послідовності певних дій при використанні інформаційної системи)
- та інші.

Для більш ефективного аналізу таких непрямих ознак та інтерпретації різних фактів фахівцям з реагування на інциденти може знадобитися аналіз функціональності інформаційних систем і взаємодія аналітиків департаменту інформаційної безпеки з користувачами (вивчення особливостей їх роботи). Також для автоматизації такого аналізу можуть бути використані спеціальні програмні засоби, які автоматично здійснюють статистичний аналіз мережевого трафіку і інших елементів інформаційної інфраструктури та сигналізують при виявленні аномальної активності, для того щоб адміністратори могли провести подальший якісний аналіз виявлених відхилень і при необхідності зробити активні дії у відповідь. В цілому, розробка та вдосконалення таких засобів аналізу в складі комплексних систем виявлення вторгнень є одним з перспективних напрямків розвитку засобів захисту інформації.

Таким чином, основним завданням на початковому етапі реагування є визначення характеру порушень і достовірне встановлення того, що виявлені аномальні події, дії і характеристики є дійсно порушеннями, а, наприклад, не проявом особливостей роботи програмного забезпечення.

Одним з найважливіших організаційних аспектів реагування на інциденти (і, зокрема, на окремі сигнали про деякі події) є та обставина, що може відбуватися більш-менш часте надходження помилкових сигналів (помилкових чи спеціально спровокованих) про деякі події, і реакція персоналу департаменту інформаційної безпеки з часом може поступово слабшати (так само як, наприклад, може притупитися увага при частих помилкових спрацьовуваннях охоронної сигналізації). Зокрема, за оцінкою деяких фахівців, в середньому в 90% випадків, коли користувачі повідомляють про те, що, на їхню думку, комп'ютер заражений вірусом, вони помиляються. У зв'язку з цим при організації реагування на інциденти необхідно приділити особливу увагу психологічній підготовці персоналу, що відповідає за реагування, а також по можливості аналізувати причини появи таких хибних сигналів і запобігати їм надалі.

Також значущим питанням організації роботи з користувачами в ситуаціях реагування на інциденти є те, що взаємодія між користувачами і групами реагування, а також різних груп реагування між собою по можливості необхідно здійснювати спеціальними захищеними каналами зв'язку.

7.5.3. Локалізація та усунення наслідків

Локалізація та усунення наслідків є основним етапом, в рамках якого, власне, здійснюється реагування на інцидент. На цьому етапі відбувається:

- визначення конкретних параметрів порушення (нападу), його характеру (конкретних сегментів мережі, серверів, груп робочих станцій, додатків, порушених нападом);
- попередній аналіз дій порушника і сценарію події (що відбувається) нападу, алгоритму роботи вірусу, що з'явився тощо.;
- блокування дій порушника (якщо порушення триває);
- блокування (повне або часткове) роботи інформаційної системи (сервера, баз даних, сегмента мережі тощо) з метою недопущення подальших руйнівних дій, поширення шкідливих програм або витоку конфіденційної інформації.

Припинення нападу і відновлення нормальної роботи інформаційних систем може зажадати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:

- спеціалістів IT-підрозділів, відповідальних за інформаційні сервіси, що атакуються;
- користувачів атакованих інформаційних систем;
- підприємств-партнерів, які мають відношення до атакованих інформаційних ресурсів;
- розробників і постачальників атакованих інформаційних систем;
- постачальників телекомунікаційних послуг, через яких здійснюється атака;
- сторонніх консультантів, що спеціалізуються на відповідних проблемах інформаційної безпеки.

Одним з найбільш важливих обставин роботи на даному етапі є те, якими повноваженнями володіє спеціаліст (черговий), відповідальний за реагування на інциденти. Зокрема, необхідно заздалегідь передбачити можливість оперативного самостійного відключення тих чи інших інформаційних сервісів фахівцями з реагування на інциденти (самостійно, або через відповідний IT-підрозділ). Особливу важливість має здатність відповідальних фахівців оперативно оцінити ситуацію, провести її аналіз (в більшості практичних ситуацій це необхідно буде робити за неповними даними про сторону, що нападає) і прийняти рішення про припинення роботи тих чи інших інформаційних сервісів, до виявлення і усунення загроз і/або введення в дію додаткових коштів протидії вторгненням. При прийнятті такого рішення необхідно враховувати (як правило, на основі експертних оцінок) як можливий збиток, який може бути викликаний виявленим порушенням, так і можливі збитки від зупинки інформаційних сервісів, як (зупинення) може бути здійснена з метою запобігання збитку від дій сторони, що нападає. Характерним прикладом такої ситуації є напад на систему електронної торгівлі, коли сторона, що нападає,

може завдати серйозної шкоди (викрасти конфіденційну інформацію учасників торговельних угод, самостійно вчинити незаконні угоди від імені учасників торгової системи тощо), а зупинка сервісу з метою запобігання такої шкоди може призвести до втрат, пов'язаних з упущеною вигодою від невиконаних угод і шкодою для ділової репутації. Іншим прикладом такої ситуації є реагування на розподілені атаки типу "відмова в обслуговуванні" (Distributed Deny of Service, DDoS), часто здійснювані на сервери в мережі Інтернет, коли може бути необхідно на деякий час повністю відключити сервер як на шкоду користувачам, так і в збиток власникам інформаційних ресурсів, розташованих на сервері.

Основою для прийняття рішень може бути заздалегідь сформований перелік (довідник) можливих основних інцидентів і ознак порушень (проникнень), в якому може бути приведена оцінка ризиків сумарних втрат і рекомендовані дії для кожного типу порушень (у тому числі і перелік ситуацій, коли необхідно здійснити відключення сервісів, щоб уникнути витоку або порушення цілісності інформації, що є найбільш критичною для всієї діяльності підприємства).

7.5.4. Ідентифікація нападника (або джерела розповсюдження шкідливих програм)

Ідентифікація нападника (або джерела розповсюдження шкідливих програм) є важливим кроком у процесі реагування, наступним безпосередньо за локалізацією нападу. У разі якщо напад здійснювався з локальної мережі підприємства, при належному дотриманні внутрішніх режимних правил ця задача може виявитися досить легкою. У разі якщо напад було скоєно ззовні, завдання ідентифікації нападників принципово ускладнюється і в деяких ситуаціях проблема стає практично нерозв'язною.

Як правило, для виявлення джерела нападу необхідно:

- детально вивчити всі технічні аспекти нападу;
- провести якісний аналіз процесу нападу в контексті функціонування системи захисту інформації, що атакується;
- організувати взаємодію зі сторонніми організаціями, які можуть сприяти в ідентифікації нападника.

Одним з найбільш важливих завдань аналізу процесу нападу є встановлення тієї інформації, яка була відома нападникам до початку нападу і якою вони скористалися для здійснення цього нападу. Зокрема, в процесі такого аналізу з певним ступенем впевненості можна встановити, що до початку нападу зловмисникам були відомі:

- інформація про структуру і склад інформаційної системи, що атакується, (використовувані програмні і апаратні засоби, їх архітектура і використовувані налаштування);
- відомості про режим роботи організації та функціонування окремих елементів інформаційної системи. Відомості про регламент деяких бізнес-процесів підприємства;
- конкретні ідентифікаційні дані (імена користувачів, паролі), необхідні для проникнення в інформаційну систему та/або правила (алгоритми) їх генерації.

Узагальнення всіх цих відомостей може допомогти встановити, які контакти були у нападників з атакованою компанією (а яких не було), і, зіставляючи факти, а також користуючись методом виключення, постаратися обмежити коло осіб, які потенційно могли бути причетні до організації даного інциденту.

У свою чергу, проведення такого аналізу буде можливим тільки в тому випадку, якщо всі інформаційні системи та системи захисту інформації налаштовані належним чином (зокрема, в них ведуться всі необхідні системні журнали) і системні дані не були пошкоджені в процесі нападу.

Другим важливим напрямком організаційної та аналітичної роботи при встановленні (ідентифікації) нападників, які вчинили напад ззовні, є взаємодія з адміністраторами систем (телекомунікаційних мереж, комп'ютерів, що використовувалися в якості проксі-серверів, тощо), з використанням яких було здійснено напад. Підходи до такої взаємодії в кожному конкретному випадку, швидше за все, будуть індивідуальними і можуть залежати від політики розкриття інформації адміністрації тієї мережі або вузла, через який здійснювалася атака. Також можуть бути зроблені дії для того, щоб у судовому порядку або із залученням правоохоронних органів зобов'язати адміністрації таких мереж і вузлів надати необхідну інформацію, пов'язану з подією нападу.

Процес ідентифікації повинен по можливості проводитися з урахуванням того, що згодом необхідно буде використовувати інформацію про нападників як доказ у кримінальному процесі. Зокрема, при знятті (копіюванні) необхідних лог-файлів з атакованих комп'ютерів представниками правоохоронних органів, що проводять слідство у даній справі, повинні бути дотримані всі процесуальні формальності, передбачені кримінально-процесуальним законодавством. Однією з особливостей процедури вилучення доказів у потерпілої сторони в цьому випадку є те, що поняті, присутні при вилученні, повинні по можливості мати хоча б загальне уявлення про сенс проведеної процедури. Також на цьому етапі при необхідності може бути проведена техніко-криміналістична експертиза комп'ютерних систем.

7.5.5. Оцінка і подальший аналіз процесу нападу

Одним із заключних кроків процесу реагування на інцидент є **оцінка та аналіз процесу нападу і його обставин.** Цей аналіз необхідно проводити в контексті цілей і завдань функціонування всього підприємства, з урахуванням результатів роботи з ідентифікації осіб, які вчинили напад. Основні завдання аналітичної роботи на даному етапі:

- аналіз цілей і мотивів нападників;
- аналіз фундаментальних (організаційних і технічних) причин, які зробили напад можливим і успішним (якщо він був успішним);
- аналіз наслідків (у тому числі і довгострокових) нападу для всієї діяльності підприємства;
- аналіз і оцінка роботи персоналу та взаємовідносин з підприємствами-партнерами (у тому числі і з постачальниками інформаційних систем і засобів захисту інформації).

Результатом аналізу повинні бути висновки, які можуть послужити основою для організаційної роботи в різних напрямках:

- коригування та уточнення політики інформаційної безпеки підприємства;
- проведення додаткової роботи з персоналом підприємства (покарання, заохочення, додаткове навчання тощо);
- проведення додаткової роботи з персоналом департаменту інформаційної безпеки підприємства, а також персоналом IT-служб;
- перегляд взаємовідносин з контрагентами підприємства (покупцями, постачальниками тощо), що мають доступ до його інформації, що захищається, або до інформаційних систем;
- залучення сторонніх консультантів з інформаційної безпеки та фахівців із засобів захисту інформації;
- ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства.

Таким чином, аналіз і всебічна оцінка інцидентів є відправною точкою для реалізації комплексу заходів щодо вдосконалення системи забезпечення інформаційної безпеки на підприємстві. Всі ці заходи повинні в майбутньому знизити ймовірність аналогічних інцидентів, а також зменшити ймовірність нанесення істотного збитку в разі їх повторення.

Важливою складовою аналізу нападу також є *оцінка збитку від події порушення інформаційної безпеки.* Збиток може бути оцінений одночасно з декількох точок зору і залежить від характеру позаштатної ситуації, що виникла. Найбільш простим для кількісної економічної оцінки є прямий збиток: витрати

на відновлення втраченої інформації (можуть бути розраховані на основі трудомісткості робіт з відновлення інформації та даних про середню вартість робочого часу відповідних фахівців), витрати на заміну скомпрометованих паролів, кодів і ключів, вартість пошкодженого обладнання, штрафні санкції за розголошення конфіденційної інформації (якщо такі санкції, наприклад, були передбачені договорами з підрядниками, постачальниками або замовниками) і т.п. Також оцінки потребує упущена вигода, яка може бути пов'язана як з безпосереднім припиненням (зупиненням, уповільненням) поточних операцій підприємства, так і з довгостроковим (перспективним) негативним впливом виниклої позаштатної ситуації - втратою довіри до підприємства, що призводить до відтоку замовників, формуванням негативного іміджу підприємства тощо. Окремо також може бути оцінене падіння ринкової вартості підприємства - його акцій (якщо мова йде про підприємство, акції якого котируються на біржовому ринку).

Найбільш складним для оцінки є моральний збиток і наслідки від розголошення інформації особистого характеру (наприклад, відомостей, що становлять лікарську таємницю). Конкретні суми моральної шкоди, як правило, можуть бути встановлені за результатами судових розглядів з окремими особами, яким такий збиток був нанесений, або процедур досудового врегулювання конфліктів (на основі вимог постраждалих осіб).

Заключним етапом процесу реагування також є усунення негативних наслідків нападу - локалізація шкоди, заподіяної подією порушенням. Ця робота може включати в себе:

- зміну скомпрометованих паролів окремих користувачів;
- перевстановлення пошкоджених операційних систем, а також пошкодженого програмного забезпечення;
- відновлення порушеної конфігурації (налаштувань) програмного забезпечення та операційних систем;
- відновлення пошкодженої інформації (баз даних, файлів), як з раніше створених резервних копій, так і іншими способами.

В процесі відновлення працездатності інформаційних систем на деякий час можуть бути задіяні резервні (альтернативні) апаратні і програмні платформи.

Крім того, необхідним завершальним кроком може бути додаткова інформаційна робота, яка може в себе включати:

- розсилку користувачам інформації про інциденти, що відбулися (у вигляді спеціальних листів і бюлетенів);
- передачу деяких відомостей про напад в засоби масової інформації;

- передачу відомостей про напад великим групам реагування на інциденти, пов'язаних з інформаційною безпекою, а також у науково-дослідні центри, що займаються проблемами захисту інформації;
- додаткову інформаційну роботу з постачальниками інформаційних систем та підрядниками, які здійснювали їх поставку, впровадження та налагодження.

З точки зору розподілу обов'язків щодо виконання окремих функцій у рамках процесу реагування на інциденти, одним з ефективних і досить широко використовуваних підходів до організації реагування на інциденти є побудова централізованої системи реагування на інциденти, коли одна група реагування обслуговує декілька підрозділів або підприємств.

7.6 Аудит стану інформаційної безпеки на підприємстві

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства і надійності засобів захисту інформації. Однак ми виходимо з того, що аудит інформаційної безпеки є комплексним дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

7.6.1. Аудит, види аудиту

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. *У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства (сегментів його мережі, окремих серверів, баз даних, Інтернет-сайтів тощо.) і надійності засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо* Однак ми надалі виходимо з того, що аудит інформаційної безпеки є комплексним (по можливості, вичерпним) дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки,

об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

Розрізняють два основних види аудиту: внутрішній (проводиться виключно силами співробітників підприємства) і зовнішній (здійснюваний сторонніми організаціями).

Цілями аудиту можуть бути:

- встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків і визначення напрямів подальшого розвитку системи захисту інформації;
- перевірка керівництвом підприємства та іншими зацікавленими особами досягнення поставлених цілей у сфері інформаційної безпеки, виконання вимог політики безпеки;
- контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;
- сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним і міжнародним стандартам).

Одним із стратегічних завдань, що вирішуються при проведенні аудиту інформаційної безпеки та отриманні відповідного сертифіката, є демонстрація надійності підприємства, його здатності виступати в якості стійкого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливо при здійсненні угод, що передбачають обмін конфіденційною інформацією, яка має велику вартість (фінансовими відомостями, конструкторсько-технологічною документацією, результатами НДДКР тощо).

У тому випадку, якщо аудит є внутрішнім, групу аудиторів необхідно сформувати з числа таких фахівців, які самі не є розробниками і адміністраторами використовуваних інформаційних систем і засобів захисту інформації та не мали відношення до їх впровадження на даному підприємстві.

Як правило, підприємство може вдаватися до допомоги зовнішніх аудиторів з метою:

- підвищення об'єктивності, незалежності та професійного рівня перевірки;
- отримання висновків про стан інформаційної безпеки та відповідності міжнародним стандартам від незалежних аудиторів.

Компанії, що спеціалізуються на проведенні аудитів, можуть здійснювати перевірки стану інформаційної безпеки на відповідність таким загальновизнаним стандартам і вимогам, як:

- ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій);
- BSI\IT: Baseline Protection Manual (Настанова базового рівня із захисту інформаційних технологій Агентства інформаційної безпеки Німеччини);
- COBIT: Control Objectives for Information and related Technology (Основні цілі для інформаційних і пов'язаних з ними технологій);
- та інших документів (таких як SAC, COSO, SAS 55/78).

При цьому організація, що здійснює зовнішній аудит, повинна відповідати певним вимогам:

- мати право (ліцензію) на видачу висновків про відповідність певним вимогам (наприклад, акредитацію UKAS - United Kingdom Accreditation Service);
- співробітники повинні мати право доступу до інформації, що становить державну і військову таємницю (якщо така інформація є на підприємстві, що перевіряється);
- володіти необхідними програмними та апаратними засобами для вичерпної перевірки наявного у підприємства програмного і апаратного забезпечення.

7.6.2. Етапи проведення аудиту

Основними етапами проведення аудиту є:

- ініціювання проведення аудиту;
- безпосереднє здійснення збору інформації та проведення обстеження аудиторами;
- аналіз зібраних даних і вироблення рекомендацій;
- підготовка аудиторського звіту та атестаційного висновку.

Аудит повинен бути ініційований керівництвом підприємства з досить чітко сформульованою метою на певному етапі розвитку інформаційної системи або системи забезпечення інформаційної безпеки підприємства (наприклад, після завершення одного з етапів впровадження). У разі якщо аудит не є комплексним, на початковому етапі необхідно визначити його безпосередні межі:

- перелік обстежуваних інформаційних ресурсів та інформаційних систем (підсистем);

- перелік будівель, приміщень і територій, в межах яких проводитиметься аудит;
- елементи системи забезпечення інформаційної безпеки, які необхідно включити в процес перевірки (організаційне, правове, програмно-технічне, апаратне забезпечення);

Основна стадія – **проведення аудиторського обстеження та збір інформації** – як правило, має включати в себе:

- аналіз наявної політики інформаційної безпеки та іншої документації організації;
- проведення нарад, опитувань, довірчих бесід та інтерв'ю зі співробітниками підприємства;
- перевірку стану фізичної безпеки інформаційної інфраструктури підприємства;
- технічне обстеження інформаційних систем – програмних і апаратних засобів (інструментальна перевірка захищеності).

Перш ніж приступити власне до аудиту інформаційної безпеки, аудиторам (зокрема, якщо проводиться зовнішній аудит) необхідно ознайомитися зі структурою підприємства, його функціями, завданнями та основними бізнес-процесами, а також з наявними інформаційними системами (їх складом, функціональністю, процедурами використання і роллю на підприємстві). На початковому етапі аудитори приймають рішення про те, наскільки глибоко і детально будуть досліджені окремі елементи інформаційної системи та системи захисту інформації. Також необхідно заздалегідь скоординувати з користувачами інформаційних систем процедури перевірки та тестування, що вимагають обмеження доступу користувачів (такі процедури по можливості повинні проводитися в неробочий час або в періоди найменшого завантаження інформаційної системи).

Якісний **аналіз діючої на підприємстві політики безпеки** є відправною точкою для проведення аудиту. Одне з перших завдань комплексного аудиту – встановлення того, якою мірою діюча політика відповідає об'єктивним потребам даного підприємства в безпеці, чи можуть дії в рамках даної політики забезпечити необхідний рівень захищеності інформації і засобів її обробки, зберігання та передачі. Це, в свою чергу, може вимагати проведення додаткової оцінки значущості основних інформаційних активів підприємства, їх вразливості, а також існуючих ризиків і загроз. Аналіз політики також може включати оцінку таких її характеристик, як:

- повнота і глибина охоплення всіх питань, а також відповідність змісту політик нижнього рівня цілям і завданням, встановленим у політиках верхнього рівня;

- зрозумілість тексту політики для людей, які не є технічними фахівцями, а також чіткість формулювань і неможливість їх подвійного тлумачення;
- актуальність всіх положень і вимог політики, своєчасність обліку всіх змін, що відбуваються в інформаційних системах і бізнес-процесах.

Після перевірки основних положень політики безпеки в процесі аудиту можуть бути вивчені (перевірені) діючі класифікації інформаційних ресурсів за ступенем критичності і конфіденційності, а також інші документи, що мають відношення до забезпечення інформаційної безпеки:

- організаційні документи підрозділів підприємства (положення про відділи, посадові інструкції);
- інструкції (положення, методики), що стосуються окремих бізнес-процесів підприємства;
- кадрова документація, зобов'язання про нерозголошення відомостей, дані співробітників, свідоцтва про проходження навчання, професійної сертифікації, атестації та ознайомленні з діючими правилами;
- технічна документація та користувацькі інструкції для різних використовуваних програмних і апаратних засобів (як розроблених самим підприємством, так і придбаних у сторонніх постачальників): міжмережевих екранів, маршрутизаторів, операційних систем, антивірусних засобів, систем управління підприємством тощо.

Основна робота аудиторів у процесі збору інформації полягає у вивченні фактично застосованих заходів щодо забезпечення захисту інформаційних активів підприємства, таких як:

- організація процесу навчання користувачів прийомам і правилам безпечного використання інформаційних систем;
- організація роботи адміністраторів інформаційних і телекомунікаційних систем і систем захисту інформації (правильність використання програмних і апаратних засобів адміністрування, своєчасність створення і видалення облікових записів користувачів, а також налаштування їх прав в інформаційних системах, своєчасність заміни паролів і забезпечення їх відповідності вимогам безпеки, здійснення резервного копіювання даних, ведення протоколів усіх вироблених у процесі адміністрування операцій, вжиття заходів при виявленні несправностей тощо);
- організація процесів підвищення кваліфікації адміністраторів інформаційних систем і систем захисту інформації;
- забезпечення відповідності необхідних (відповідно з політикою безпеки

та посадовими обов'язками) прав користувачів інформаційних систем і фактично наявних;

- організація призначення і використання спеціальних ("суперкористувацьких") прав в інформаційних системах підприємства;
- організація робіт і координації дій при виявленні порушень інформаційної безпеки та відновленні роботи інформаційних систем після збоїв і нападів (практичне виконання "аварійного плану");
- вживаються заходи антивірусного захисту (належне використання антивірусних програм, облік всіх випадків зараження, організація роботи з усунення наслідків заражень тощо);
- забезпечення безпеки придбаних програмних і апаратних засобів (наявність сертифікатів і гарантійних зобов'язань, підтримка з боку постачальника при усуненні виявлених недоліків тощо);
- забезпечення безпеки самостійно розроблюваного програмного забезпечення (наявність необхідних вимог у проектній документації інформаційних систем, якість програмної реалізації механізмів захисту тощо);
- організація робіт з встановлення та оновлення програмного забезпечення, а також контролю за цілісністю встановленого ПЗ;
- вживаються заходи щодо забезпечення обліку і схоронності носіїв інформації (дисків, дискет, магнітних стрічок тощо.), а також з їх безпечного знищення після закінчення використання;
- ефективність організації взаємодії співробітників підприємства – користувачів інформаційних систем – зі службою інформаційної безпеки (зокрема, з питань реагування на інциденти та усунення їх наслідків).

Одним з важливих напрямків аудиторської перевірки є контроль того, наскільки своєчасно і повно положення та вимоги політики безпеки та інших організаційних документів доводяться до персоналу підприємства. В тому числі, необхідно оцінити, наскільки систематично і цілеспрямовано здійснюється навчання персоналу (як при занятті посад, так і в процесі роботи), і, відповідно, дати оцінку тому, якою мірою персонал розуміє всі пропоновані до нього вимоги, усвідомлює свої обов'язки, пов'язані із забезпеченням безпеки, а також можливу відповідальність, яка може настати при порушенні встановлених вимог.

У процес проведення інтерв'ю, нарад і бесід з персоналом необхідно включити якомога більше співробітників підприємства, які мають хоча б якесь відношення до інформаційних систем і процедур обробки інформації : адміністраторів і розробників інформаційних систем, операторів та інших користувачів, допоміжний персонал тощо При безпосередній роботі з

персоналом аудиторам необхідно з'ясувати особливості перебігу окремих бізнес-процесів, ролі окремих співробітників в цих процесах і їх потенційні можливості впливати на інформаційну безпеку. Також необхідно оцінити, якою мірою співробітники фактично виконують свої обов'язки щодо забезпечення інформаційної безпеки.

Одним із важливих завдань аудиту може бути встановлення того, наскільки підприємство здатне протидіяти внутрішнім загрозам в особі співробітників, цілеспрямовано діючих, щоб завдати той чи інший збиток підприємству і мають для цього різні можливості. Зокрема, для цього можуть бути досліджені:

- процедури відбору та прийняття нових співробітників на роботу, а також їх попередньої перевірки;
- процедури контролю за діяльністю співробітників (відстеження їх дій);
- процедури реєстрації користувачів і призначення їм прав в інформаційних системах;
- розподіл функцій між різними співробітниками і мінімізація їхніх привілеїв, а також можливу наявність надлишкових прав у деяких користувачів та адміністраторів.

Перевірка стану фізичної безпеки інформаційної інфраструктури, як правило, включає в себе:

- перевірку того, щоб найбільш важливі об'єкти інформаційної інфраструктури та системи захисту інформації розташовувалися в зонах (частинах будинків, приміщеннях), що мають пропускний режим, а також обладнаних камерами відеоспостереження та іншими засобами контролю (електронними замками, засобами біометричної ідентифікації тощо);
- перевірку наявності та працездатності технічних засобів, що забезпечують стійку роботу комп'ютерного та телекомунікаційного обладнання: джерел безперебійного енергопостачання, кондиціонерів (там, де це необхідно) тощо;
- перевірку наявності та працездатності засобів пожежної сигналізації та пожежогасіння;
- перевірку розподілу відповідальності за фізичний (технічний) стан об'єктів інформаційної інфраструктури підприємства.

Інструментальна перевірка захищеності є в основному технічним завданням і здійснюється з використанням спеціалізованого програмного забезпечення, яке підключається до інформаційної системи підприємства і

автоматично проводить збір всіляких відомостей: версій встановлених операційних систем і програмного забезпечення, даних про мережеві протоколи, що використовуються, номерів відкритих портів, даних про версії встановлених оновлень тощо. До інших напрямків інструментального та технічного контролю також відносяться такі роботи, як:

- безпосереднє вивчення роботи окремих серверів, робочих станцій і мережевого устаткування відповідними технічними фахівцями, які можуть перевірити різні аспекти їх функціонування (процедури завантаження, виконувані процеси, вміст конфігураційних файлів тощо);
- збір і подальший аналіз даних про те, як виконуються процедури резервного копіювання, а також інші необхідні технічні процедури, передбачені регламентом;
- перевірка якості програмного забезпечення, самостійно розробленого підприємством (у тому числі і шляхом аналізу вихідних кодів і проектної документації до нього), виявлення помилок, які можуть стати причиною збоїв, несанкціонованих проникнень, руйнування і витоку інформації та інших інцидентів;
- вивчення роботи мережі (мережевого трафіку, завантаження різних сегментів мережі тощо);
- проведення з метою тестування пробних, контрольованих "порушень" інформаційної безпеки (по можливості без нанесення реальної шкоди і у позаробочий час), таких як атаки типу "відмова в обслуговуванні" (DoS) або проникнення в певні бази даних і на певні сервери, а також використання різних відомих вразливостей з метою з'ясування конкретних параметрів безпеки, стабільності та надійності інформаційної системи, яка перевіряється.

Також в процесі аудиту може бути перевірено ведення журналів (лог-файлів) інформаційних систем і застосування інших інструментів збору та аналізу інформації, необхідних для забезпечення поточного контролю за дотриманням вимог інформаційної безпеки та своєчасного реагування на інциденти (засобів виявлення вторгнень, аналізаторів роботи локальних мереж тощо). Інформація, накопичена в лог-файлах за час використання інформаційних систем, є одним з важливих об'єктів аналізу в процесі аудиту. На основі цих даних можуть бути зроблені оцінки та висновки щодо дотримання встановлених правил використання інформаційних систем, ефективності використовуваних засобів захисту інформації, поведінки користувачів, а також про потенційно можливі проблеми.

Аналіз всієї інформації, отриманої в процесі ознайомлення з документацією, контролю фактичного виконання всіх встановлених вимог, отримання відомостей від співробітників, вивчення роботи апаратних засобів і програмного забезпечення, перевірки фізичної захищеності та проведення інструментальних перевірок повинен бути проведений з урахуванням виявлених ризиків та потреб підприємства в інформаційній безпеці. Зокрема, такий аналіз передбачає виявлення конкретних особливостей програмних і апаратних засобів, бізнес-процедур, організаційних правил і розподілів функціональних обов'язків та повноважень, які можуть негативно вплинути на забезпечення інформаційної безпеки, а також опис причинно-наслідкових взаємозв'язків між виявленими особливостями функціонування підприємства і збільшенням ризиків порушення інформаційної безпеки. Всі досліджені обставини, виявлені недоліки та особливості повинні бути узагальнені, і таким чином має бути сформоване загальне уявлення про стан інформаційної безпеки на підприємстві, відображені основні переваги і недоліки діючої системи захисту інформаційних ресурсів, а також позначені основні пріоритети та напрями її подальшого розвитку та вдосконалення.

Результати аналізу можуть бути представлені як у вигляді узагальнених коротких формулювань, що характеризують захищеність інформації підприємства (адресованих керівництву та власникам підприємства), так і у вигляді переліку конкретних зауважень і пропозицій, що відносяться до окремих ділянок роботи (адресованих керівнику департаменту інформаційної безпеки, керівнику служби безпеки, функціональним директорам та керівникам структурних підрозділів підприємства).

Заключним результатом аналізу та узагальнення даних, отриманих в процесі аудиту, є звіт (висновок), який може включати в себе:

- оцінку стану (рівня) захищеності інформаційних ресурсів та інформаційних систем;
- висновки про практичне виконання вимог, передбачених політикою інформаційної безпеки підприємства та іншими вимогами та документами;
- висновок про ступінь відповідності фактичного рівня інформаційної безпеки вимогам певних стандартів і нормативних документів;
- пропозиції щодо удосконалення політики інформаційної безпеки та реалізації додаткових практичних заходів у цій сфері (як організаційних, так і технічних), а також про ті заходи, які необхідно реалізувати для проходження сертифікації на відповідність певному стандарту (якщо за результатами проведеного аудиту зроблено висновок про те, що

поточний рівень захищеності інформаційних ресурсів підприємства не відповідає таким вимогам);

- висновок про ступінь відповідності політики безпеки підприємства та всього комплексу заходів щодо захисту інформації вимогам чинного законодавства та відомчих нормативних актів;
- оцінки економічної ефективності вкладень у ті чи інші засоби захисту інформації, а також організаційні заходи (віддачі від них);
- кількісна (грошова) оцінка можливих втрат від тих чи інших порушень, які можуть статися при існуючому рівні забезпечення інформаційної безпеки, а також розрахунок необхідних вкладень, які необхідно здійснити для досягнення певного рівня захищеності.

Також за результатами аудиту можуть бути сформульовані додаткові рекомендації, що стосуються:

- перегляду окремих бізнес-процесів і процедур;
- вдосконалення роботи з персоналом підприємства;
- впровадження і використання сучасних технічних (програмних і апаратних) засобів обробки і захисту інформації;
- організації роботи із захисту інформації;
- вибору пріоритетів в процесі усунення існуючих недоліків.

7.7 Надання послуг у сфері інформаційної безпеки

На ринку надання інформаційних послуг представлені різні сфери, пов'язані із забезпеченням інформаційної безпеки: аудиторських, консультаційних, послуг з впровадження технічних засобів захисту, а також послуг зі страхування інформаційних ризиків.

7.7.1. Передумови розвитку ринку послуг із забезпечення інформаційної безпеки і його структура

Розвиток сучасних інформаційних технологій, зростання залежності діяльності багатьох підприємств і установ від функціонування інформаційних систем і постійне наростання обсягів і складності інформаційних потоків призвели до того, що завдання забезпечення інформаційної безпеки стали вимагати використання значних ресурсів. Зокрема, фінансові кошти, що виділяються на забезпечення інформаційної безпеки, займають все більшу частку в бюджетах підприємств, а поточне і стратегічне управління захистом інформації вимагає більшої уваги не тільки з боку фахівців з інформаційних

технологій, але і з боку керівників і власників підприємств. Найчастіше необхідні ресурси і зусилля керівників в цій сфері виявляються порівнянними з тими ресурсами, які витрачаються на здійснення основної діяльності підприємств. Таким чином, склалися передумови для формування ринку різних послуг із забезпечення інформаційної безпеки, які (послуги) допомогли б не тільки підвищити ефективність захисту інформаційних ресурсів, а й оптимізувати витрати підприємств і організацій. Основними факторами, які зумовили появу у підприємств потреб в послугах сторонніх фірм, які вирішують завдання забезпечення інформаційної безпеки, і виділення послуг із захисту інформаційних ресурсів в самостійну сферу бізнесу, стали:

- ускладнення і постійний розвиток сучасних систем обробки, зберігання та передачі інформації;
- ускладнення програмних і апаратних засобів, що використовуються для захисту інформації, необхідність розуміння складного комплексу теоретичних і методичних питань для їх ефективної експлуатації;
- зростання числа інцидентів і різноманітності видів атак на інформаційні системи та їх інтенсивності;
- нестача кваліфікованих фахівців у сфері інформаційної безпеки і зростання витрат на їх утримання і професійну підготовку.

Причиною того, що підприємства виявляються зацікавленими у відмові від самостійного виконання певних функцій і залучення сторонніх спеціалізованих компаній для вирішення цих завдань (в сучасній практиці такий підхід прийнято називати "аутсорсингом" або "передачею на аутсорсинг"), є можливість підвищити ефективність процесів захисту інформації, в певній мірі скоротити витрати на ці процеси, а також більшою мірою сконцентруватися на управлінні основною діяльністю підприємства і не відволікати ресурси і час керівників на вирішення завдань, що є за своєю суттю вторинними і допоміжними по відношенню до основних цілей і завдань діяльності підприємства. Більш висока ефективність роботи спеціалізованих компаній – постачальників послуг в сфері інформаційної безпеки в порівнянні з самостійним рішенням цих завдань самими підприємствами, як правило, пов'язана з тим, що високі витрати розподіляються між безліччю підприємств – клієнтів постачальника послуг. Характерними прикладами таких витрат, які, з одного боку, можуть виявитися неприпустимими для одного підприємства, але, з іншого боку, можуть бути ефективно розподілені між кількома підприємствами, є:

- найм висококваліфікованих фахівців у відносно вузьких дисциплінах і галузях інформаційної безпеки (таких як використання криптографічних засобів, боротьба з вірусами, впровадження віртуальних приватних мереж і т.п.);

- часте перенавчання та підвищення кваліфікації фахівців;
- постійне відстежування нових загроз і глибокий якісний аналіз поточного стану інформаційних технологій і тенденцій їх розвитку;
- придбання спеціалізованих програмних і апаратних засобів, необхідних для захисту інформації та аудиту інформаційних систем;
- забезпечення цілодобового чергування служб реагування на інциденти.

При всіх перевагах передачі окремих завдань забезпечення безпеки на аутсорсинг цей підхід має і ряд недоліків, які в певній мірі можуть обмежувати його застосування.

- Підприємство, яке користується такими послугами, дещо обмежує себе в можливостях керувати своїми витратами і скорочувати витрати (накладні витрати) і, таким чином, потрапляє в певну залежність від цінової політики постачальників послуг, а також від кон'юнктури ринку.
- Співробітники компанії, що надає послуги, отримують доступ до найбільш важливої інформації підприємства-клієнта і його інформаційним системам, що потенційно може бути джерелом додаткових ризиків для інформаційної безпеки.
- Виникають додаткові загрози інформаційній безпеці при взаємодії між компанією-постачальником і підприємством-клієнтом в процесі надання послуг (наприклад, може бути перехоплена інформація при віддаленому адмініструванні інформаційних систем підприємства-клієнта).

Основними послугами, які можуть бути передані на аутсорсинг (як окремо, так і в комплексі), є:

- послуги з проведення комплексних аудитів стану інформаційної безпеки на підприємстві;
- послуги з проведення аудитів (інструментальних перевірок) стійкості і надійності окремих інформаційних підсистем (мереж, програмних і апаратних платформ і т.п.) і засобів захисту інформації, що використовуються підприємством;
- послуги з сертифікації інформаційних систем, вироблених програмних і апаратних засобів захисту інформації;
- консультаційні послуги, пов'язані з формуванням стратегії підприємства в сфері інформаційної безпеки і розробкою політики безпеки;
- послуги з проектування системи захисту інформації;
- консультаційні послуги з вибору та адаптації окремих технологій захисту інформації (криптографії, біометричної ідентифікації і т.п.)

відповідно до певних умов ведення бізнесу;

- послуги по впровадженню системи захисту інформації, а також впровадження окремих технічних (програмних і апаратних) засобів та реалізації організаційних заходів;
- послуги з поточного адміністрування, підтримки та супроводу інформаційних систем і систем захисту інформації;
- послуги з реагування на інциденти, пов'язані з порушеннями інформаційної безпеки;
- послуги з навчання керівників підприємства, фахівців служби інформаційної безпеки та IT-служби, а також користувачів інформаційної системи підприємства.

В цілому, на цей момент складно говорити про формування повноцінного ринку послуг в сфері інформаційної безпеки, так як у більшості менеджерів великих, а особливо середніх і малих підприємств в основному не сформувалися уявлення про необхідні заходи в цій сфері, а фінансування робіт із забезпечення інформаційної безпеки часто здійснюється за залишковим принципом. Деякі великі розробники комплексних рішень у сфері інформаційної безпеки, хоча і функціонують досить активно, але при цьому фактично не є учасниками відкритого ринку, так як їх продукція і послуги практично повністю орієнтовані на певних споживачів в державному секторі. Ще однією важливою особливістю ринку послуг в сфері інформаційної безпеки є те, що надання таких послуг іноді стає "побічним", додатковим видом (напрямом) діяльності для компаній, що займаються постачанням апаратних і програмних засобів захисту інформації, а також для компаній, що займаються розробкою комплексних рішень по автоматизації підприємств.

Можливим недоліком такого підходу потенційно може бути те, що консультанти і аналітики виявляються жорстко "прив'язані" до певних програмних і апаратних засобів (виробникам, торговим маркам) і не мають можливості гнучко підбирати окремі засоби захисту і формувати найбільш ефективні комплексні рішення відповідно до потреб кожного конкретного підприємства.

Проте, не дивлячись на певні недоліки в розвитку ринку послуг із забезпечення інформаційної безпеки, незаперечним фактом є те, що багато таких послуги вже представлені на ринку, а основні ринкові і організаційні механізми починають відпрацьовуватися на практиці. При цьому однією з рекомендацій при роботі з фірмами-постачальниками послуг в сфері інформаційної безпеки є правило – користуватися послугами кількох різних фірм і періодично міняти партнерів, які забезпечують вирішення тих чи інших проблем безпеки.

7.7.2. Особливості деяких видів послуг інформаційної безпеки

Кожен вид послуг в цій сфері має свої специфічні характеристики як з точки зору організації роботи компаній, що надають послуги, так і з точки зору структури ринку. Відповідно, для ефективної роботи необхідний індивідуальний підхід до організації надання таких послуг, а також організації взаємодії між споживачами і постачальниками послуг.

Послуги з реагування на інциденти (порушення інформаційної безпеки), є одним з найбільш характерних прикладів обґрунтованості та доцільності передачі сервісів безпеки на аутсорсинг. Зокрема, доцільність відмови від самостійного виконання функцій реагування на інциденти та їх (функцій) централізації в спеціалізується на таких завданнях компанії пов'язана з тим, що ця діяльність має наступні важливі особливості:

- вимагає постійного (цілодобового) чергування, що передбачає утримання в штаті як мінімум п'яти фахівців;
- передбачає наявність висококваліфікованих (а отже, високооплачуваних і затребуваних на ринку праці) фахівців, здатних швидко вжити ефективних заходів протидії загрозам (в тому числі і вжити контрзаходів до нападників в процесі триває атаки), а також самостійно прийняти необхідні рішення в процесі відображення триває атаки;
- завантаження чергових фахівців, що відповідають за реагування на інциденти, може бути вкрай нерівномірним.

Таким чином, ефект від централізації функцій, пов'язаних з реагуванням на інциденти, складається з декількох складових і надає можливості як для скорочення витрат і підвищення рівня захищеності підприємств-клієнтів, так і для отримання прибутку фірмами-постачальниками таких послуг. При цьому розмежування функцій між підприємством-клієнтом і компанією-постачальником послуг може залежати від таких факторів, як:

- рівень довіри підприємства-клієнта до фірми-постачальника послуг;
- усталена практика надання таких послуг і наявність у фірми-постачальника необхідних фахівців з певним рівнем кваліфікації;
- склад, характеристики та функціональність інформаційних систем підприємства-клієнта;
- рівень кваліфікації співробітників підприємства-клієнта (як користувачів інформаційних систем, так і співробітників департаменту інформаційної безпеки);
- оцінка існуючих ризиків (ймовірності нанесення збитку);
- оцінка (в тому числі і суб'єктивна) того, наскільки значущим є знання

внутрішнього середовища підприємства співробітниками служби інформаційної безпеки і їх здатність "зсередини" координувати дії і вирішувати проблеми в разі будь-яких інцидентів.

Крім того, в деяких випадках можуть існувати певні законодавчі обмеження на аутсорсинг процесів безпеки (зокрема, для державних підприємств).

Основні питання проведення аудитів інформаційної безпеки (і, зокрема, зовнішніх аудитів). Крім уже зазначених факторів, які зумовлюють необхідність проведення саме зовнішніх аудитів, а не внутрішніх (більш висока кваліфікація фахівців, право робити висновки про відповідність міжнародним стандартам і т.п.), важливим є також і та обставина, що зовнішні аудитори, як правило, не зацікавлені в поданні необ'єктивної інформації (на відміну від внутрішньої служби інформаційної безпеки). У разі ж, якщо підприємство захоче створити власну незалежну службу для проведення аудитів інформаційної безпеки (окремо від департаменту інформаційної безпеки та інших підрозділів підприємства), результатом можуть виявитися дуже великі витрати, тим більше що частота проведення таких аудитів, як правило, є не дуже великий .

Необхідність вдаватися до послуг спеціалізованих фірм, пов'язаних з перевіркою захищеності і надійності окремих елементів інформаційної інфраструктури (серверів, мереж, міжмережевих екранів і т.п.), обумовлена, як правило, наявністю у цих фірм спеціалізованих програмних і апаратних засобів, необхідних для проведення таких перевірок (наприклад, спеціалізованих сканерів вразливостей), а також наявність спеціальних знань і навичок і різнобічного досвіду, накопиченого в процесі практичної роботи при проведенні подібних перевірок на різних підприємствах. Придбання подібного досвіду в рамках одного підприємства, нехай навіть і дуже великого, практично неможливо. Одним з найбільш ефективних прийомів при проведенні такого роду перевірок є пробне (тестове) подолання захисту, коли перевіряючий імітує певний напад з метою здійснити порушення (зруйнувати базу даних, викрасти конфіденційну інформацію і т.п.). Основними завданнями перевірок такого роду є:

- оцінка ефективності використовуваних технічних (програмних і апаратних) засобів захисту інформації;
- оцінка ефективності роботи фахівців, відповідальних за реагування на інциденти;
- контроль дотримання співробітниками підприємства вимог політики безпеки.

Для отримання найбільш достовірних результатів бажано, щоб на самому підприємстві про проведення такого тесту знали тільки кілька керівників,

відповідальних за його організацію.Також важливою умовою проведення такої перевірки є чітка домовленість про те, наскільки далеко має зайти атака і який рівень проникнення і руйнівних дій є достатнім, для того щоб достовірно продемонструвати, що атакована (перевіряється) система є вразливою. У будь-якому випадку вся відповідальність за шкоду, завдану в результаті здійснення такої перевірки, повністю лягає на підприємство, яке замовило таку послугу.

Консультаційні послуги, пов'язані з первинної постановкою системи управління інформаційною безпекою (первинним аналізом, формуванням та використанням політики безпеки), зазвичай бувають необхідні в тій ситуації, коли підприємство вперше ставить для себе завдання цілеспрямованого систематичного комплексного забезпечення інформаційної безпеки. У цих умовах залучення сторонніх консультантів є практично єдиним способом сформувати досить адекватну і ефективну політику безпеки в досить стислі терміни, так як саме підприємство в такій ситуації зазвичай не має необхідних фахівців і керівників, які могли б вирішити весь комплекс завдань, пов'язаних з оцінкою ризиків, інвентаризацією інформаційних активів, виробленням стратегії, формуванням політики та організаційної структури департаменту інформаційної безпеки.

Залучена для вирішення всіх цих завдань консультаційна компанія повинна буде провести аналіз діяльності підприємства в декількох розрізах: з точки зору основних бізнес-процесів, з точки зору наявної інформаційно-технологічної та комунікаційної інфраструктури, а також з точки зору використовуваних додатків (програмного забезпечення та баз даних). Таким чином, необхідна якість роботи щодо забезпечення комплексної захищеності інформаційних ресурсів підприємства може бути досягнуто тільки в тому випадку, якщо у консалтинговій компанії є необхідні фахівці, а також досвід роботи як на подібних підприємствах, так і з подібними програмними і апаратними платформами. Високі вимоги до кваліфікації фахівців, що працюють в консалтингових компаніях, пояснюються необхідністю не просто зрозуміти особливості функціонування тих чи інших бізнес-процесів та інформаційних систем, але і досить швидко оцінити їх слабкі місця, існуючі ризики і найбільш ймовірні сценарії нанесення збитку інформаційних ресурсів.

Послуги з адміністрування інформаційних систем і засобів захисту інформації можуть надаватися як в комплексі з послугами з реагування на інциденти, так і незалежно від них. Фірми-постачальники послуг можуть здійснювати адміністрування таких систем, як:

- електронна пошта (захист від вірусів, спаму, порушення конфіденційності та інших порушень політики безпеки);
- мережеве обладнання (збір і аналіз інформації про функціонування

маршрутизаторів, серверів та інших пристроїв);

- брандмауери (конфігурація та виконати установку до мережі, а також забезпечення своєчасного реагування на різні порушення);
- системи виявлення вторгнень (відстеження всіх "підозрілих" дій щодо мереж, серверів, додатків і баз даних).

При цьому підприємство-покупець може вдаватися до послуг інших фірм для контролю за тим, наскільки ефективно здійснюється адміністрування засобів захисту інформації, або самостійно здійснювати такий контроль за допомогою спеціальних сканерів.

При наданні послуг з адміністрування фірма-постачальник, як правило, не може взяти на себе повну відповідальність за збереження інформації (так само як і при наданні послуг з реагування на інциденти), проте для встановлення формальних відносин підприємство-клієнт і фірма-постачальник можуть розробити Угоду про рівень обслуговування, яке повинно передбачати основні параметри функціонування інформаційних систем і їх захищеності (гарантований час надійної роботи систем, гарантовані строки відновлення працездатності при порушеннях і т.п.).

7.7.3. Інфраструктура публічних ключів

Інфраструктура публічних ключів (Public Key Infrastructure, PKI) являє собою складну організаційно-технічну систему, засновану на сучасних технологіях і розвинених організаційних стандартах, яка дозволяє ефективно вирішувати деякі ключові проблеми інформаційної безпеки і, зокрема, проблеми захисту даних, що передаються по мережі (як локальним, так і глобальним), і ідентифікації сторін, що беруть участь в інформаційному обміні (користувачів, інформаційних систем, програмних процесів). Технологія PKI є основним інструментом, за допомогою якого на основі законодавчої бази може бути створений юридично значущий документообіг, який, в свою чергу, може стати основою для активного розвитку електронної торгівлі, надання фінансових, інформаційних та інших послуг, а також здійснення електронних платежів через інформаційні мережі загального користування. Можливість використання цієї технології для здійснення платежів і господарських операцій пов'язана з тим, що її найважливішим елементом є так званий цифровий сертифікат, що видається третьою стороною, яка фактично є гарантом того, що операції, що здійснюються з використанням певного цифрового сертифікату, відбуваються від імені певної особи . Таким чином, одним з ключових елементів інфраструктури публічних ключів є організаційні структури, що здійснюють ідентифікацію осіб (якщо мова йде про видачу сертифіката для однієї людини) і видачу електронного

сертифіката встановленого зразка, однозначно і достовірно представляє цю людину.Також ці центри вирішують безліч додаткових завдань, пов'язаних із забезпеченням ефективної роботи інфраструктури публічних ключів: ведуть списки анульованих сертифікатів, оновлюють минулі сертифікати і т.п. В цілому вся сукупність використовуваних технічних і організаційних рішень, а також діюча юридична база дають можливість однозначно пов'язувати цифровий сертифікат (цифровий підпис) з певною фізичною особою і також гарантувати, що не відбувається порушення цілісності переданих повідомлень.

В даний час досить добре розроблені базові технічні стандарти та інформаційні технології (засоби криптографії, алгоритми, що реалізують хеш-функції і т.п.), необхідні для побудови засобів захисту на основі PKI.Подальші перспективи розвитку в цій сфері пов'язані, головним чином, з вдосконаленням ринку послуг і організаційних механізмів.

Ідеологія роботи PKI передбачає створення мереж і взаємопов'язаних структур безлічі різнихзасвідчуюючих центрів, що працюють в рамках єдиної узгодженої політики і спираються на загальний "кореневий" засвідчуючий центр. На практиці ж найбільш поширене створення самостійних розрізнених засвідчувальних центрів, створюваних окремими підприємствами (наприклад, комерційними банками) на основі тиражованих програмних і апаратних рішень для забезпечення захищеності і надання юридичної значимості створюваних документів і транзакцій, що здійснюються в корпоративних інформаційних системах (таким як, наприклад, платіжні доручення) службовцями, клієнтами та бізнес-партнерами підприємства. У разі якщо підприємство самостійно розгортає PKI в рамках власної інформаційної системи, всі взаємовідносини між адміністрацією і користувачами регулюються внутрішньою політикою.

При цьому одним з можливих підходів до впровадження технології PKI є передача функцій, пов'язаних з видачею і подальшим зверненням цифрових сертифікатів, на аутсорсинг. Передача функцій засвідчувального центру сторонньої спеціалізованої компанії, як правило, вирішує для підприємства два важливих завдання:

- дозволяє уникнути значних витрат, пов'язаних із закупівлею та підтриманням програмних і апаратних засобів, а також найманням і навчанням персоналу;
- дає можливість застосовувати цифрові сертифікати за межами свого підприємства, а також використовувати на підприємстві сертифікати співробітників інших підприємств.

У свою чергу, компанія, що виконує функції засвідчувального центру, може передати частину робіт, які пов'язані з перевіркою документів осіб, які претендують на отримання сертифіката, і їх консультуванням, своїм партнерам -

так званим "реєстраційним центрам". Їх основна функція полягає в спрощенні і прискоренні процедури перевірки документівта ідентифікації особистості при видачі сертифіката для осіб, які не можуть особисто з'явитися в засвідчуючий центр.

Саме на основі мереж реєстраційних центрів, а також взаємодії різних центрів, що засвідчують (їх об'єднання в єдину мережу) має відбуватися побудова універсальної загальнодоступної інфраструктури публічних ключів. Передбачається, що основними користувачами – клієнтами центрів, що засвідчують, що бажають отримати цифрові сертифікати, – повинні бути особи, зацікавлені в доступі до різних спеціалізованих електронних сервісів, що полегшує взаємодію як з різними комерційними структурами (наприклад, банками), так і з державними органами

7.8 Надання страхових послуг у сфері інформаційної безпеки

Світова практика страхування інформаційних ризиків почала складатися в дев'яностих роках і отримала свій розвиток після 2000-го року, коли ризики інформаційної безпеки стали більш серйозними. Розглянемо організаційні питання надання різних послуг, пов'язаних із забезпеченням інформаційної безпеки: аудиторських, консультаційних, послуг з впровадження технічних засобів захисту, а також послуг зі страхування інформаційних ризиків.

7.8.1. Страхування інформаційних ризиків.

Хоча страхування ризиків, пов'язаних з інформаційною безпекою, само по собі не є організаційним засобом захисту інформації (бо факт наявності або відсутності такої страховки не впливає на ймовірність нанесення шкоди інформаційних ресурсів), все ж воно є важливим і перспективним інструментом управління інформаційними ризиками на підприємстві.

З погляду ризик-менеджменту, страхування є головним інструментом так званої "передачі ризиків". Основним чинником, що обумовлює зацікавленість підприємств у страхуванні своїх інформаційних ресурсів, є те, що в разі будь-яких серйозних порушень в роботі інформаційних систем підприємство отримує можливість за рахунок страхових виплат відносно швидко відновити їх роботу, а також основні бізнес-процеси і компенсувати (хоча б частково) збиток від вимушеного простою і втрати інформаційних активів.

Згідно із законодавством об'єктом страхування можуть бути не суперечать законодавству майнові інтереси, пов'язані з володінням, користуванням, розпорядженням майном, а також пов'язані з відшкодуванням страхувальником

заподіяної ним шкоди особі або майну фізичної особи, а також шкоди, заподіяної юридичній особі (страхування відповідальності). Таким чином, на практиці об'єктами страхування можуть бути:

- інформаційні ресурси (в будь-якому їх вигляді: бази даних, бібліотеки електронних документів тощо);
- програмне забезпечення (як уже використовувані програмні власні та покупні продукти, так і ті, що знаходяться в розробці);
- апаратне забезпечення інформаційних систем (мережеве обладнання, сервери, робочі станції, телекомунікаційне обладнання, периферія, джерела безперебійного живлення тощо);
- фінансові активи (грошові кошти, бездокументарні цінні папери) в електронній формі (у тому числі кошти на рахунках, керованих за допомогою систем "клієнт-банк").

Договір страхування (страховий поліс) може передбачати відшкодування прямих збитків у разі настання різних страхових випадків, таких як:

- вихід з ладу (збої в роботі) інформаційних систем, обумовлені недостатньою якістю використовуваних програмних і апаратних засобів, помилками при їх проектуванні, розробці, виробництві, установки, настройки, обслуговуванні або експлуатації;
- навмисні протиправні дії співробітників підприємства, вчинені з метою завдати шкоди підприємству або отримати певну вигоду;
- напади (атаки) на інформаційні системи підприємства , які здійснені третіми особами з метою завдати шкоди інформаційних ресурсів підприємства і його інформаційним системам (пошкодити або знищити інформацію, що зберігається в електронному вигляді, отримати конфіденційні відомості, вивести з ладу програмні і апаратні засоби з метою припинити або призупинити функціонування певних сервісів і т.п.);
- впливу шкідливих програм і макросів (вірусів, хробаків і т.п.), що спричинили порушення роботи інформаційних систем, втрату інформації або розголошення конфіденційної інформації;
- розкрадання фінансових активів (грошових коштів, бездокументарних цінних паперів), вчинене шляхом здійснення різних неправомірних дій: крадіжки паролів і ключів, присвоєння особистості, внесення змін в програмне забезпечення і т.п.

На додаток до основних ризиків, безпосередньо пов'язаних з інформаційними активами, також можуть бути застраховані:

- збитки від припинення основної господарської діяльності підприємства в результаті порушення роботи інформаційних систем;

- додаткові витрати, пов'язані з підтриманням поточної господарської діяльності в період відновлення роботи пошкоджених інформаційних систем;
- додаткові витрати, пов'язані з терміновим відновленням роботи інформаційних систем, а також терміновим відновленням основної господарської діяльності підприємства;
- додаткові витрати на відновлення ділової репутації після того, як їй було завдано збитків у результаті атаки на інформаційні ресурси та інформаційні системи.

Збитки від призупинення основної господарської діяльності підприємства можуть включати в себе упущену вигоду, зумовлену простоєм інформаційних систем (тобто той прибуток, який підприємство могло б отримати, але не отримало внаслідок виходу з ладу інформаційних систем), а також витрати на підтримку інфраструктури підприємства в період вимушеного простою (як правило, це деякі постійні витрати, які не залежать від обсягу випуску продукції та інтенсивності господарської діяльності). Додаткові витрати, пов'язані з підтриманням поточної господарської діяльності в період відновлення роботи пошкоджених інформаційних систем, можуть виникати в тому випадку, якщо існують деякі альтернативні способи обробки та зберігання інформації та здійснення бізнес-процесів (наприклад, на базі програмних і апаратних засобів, а також телекомунікаційних каналів, тимчасово орендованих у спеціалізованих компаній) і підприємство визнає потрібним і можливим скористатися цими альтернативними способами. При цьому задіяння таких резервних ресурсів, як правило, має бути узгоджене зі страховою компанією, покриває ці витрати. Додаткові витрати, пов'язані з терміновим відновленням роботи інформаційних систем, можуть виникати в тому випадку якщо, наприклад, у сторонніх постачальників існують деякі альтернативні (більше оперативні в порівнянні із звичайними) умови поставок обладнання та програмного забезпечення, а також надання послуг по введенню в дію інформаційних систем.

Всі ці видатки, очевидно, також можуть бути об'єктами страхування. При цьому в кожній ситуації страховику і страхувальнику необхідно детально проаналізувати різні альтернативи виходу з кризової ситуації і вибирати найбільш доцільні варіанти. Так, наприклад, страхова компанія може відмовитися компенсувати додаткові витрати, пов'язані з терміновим відновленням інформаційних систем, якщо більш вигідною є компенсація упущеної вигоди за період більш тривалого вимушеного простою.

Процедура страхування (життєвий цикл договору страхування) включає в себе кілька основних етапів (рисунок 16.1).

1. Попереднє обстеження підприємства, аналіз існуючих ризиків для інформаційної безпеки.
2. Формулювання рекомендацій щодо зменшення ризиків та реалізація підприємством відповідних заходів.
3. Узгодження умов страхування і укладення договору.
4. Аналіз збитку і його розрахунок у грошовому еквіваленті в разі реалізації застрахованих ризиків.
5. Узгодження і подальше здійснення страхових виплат, що покривають збитки.

Попереднє обстеження підприємства до укладення договору страхування в багато чому аналогічно проведенню зовнішнього аудиту і також може здійснюватися незалежною спеціалізованою компанією. Після закінчення такої перевірки можуть бути сформовані два основних документи:

- звіт (висновок) про стан інформаційної безпеки на підприємстві;
- рекомендації щодо підвищення рівня захищеності інформаційних ресурсів і зменшення ризиків.

Таке обстеження в подальшому створює передумови для прийняття рішення про можливість і доцільність страхування інформаційних ризиків даного підприємства, а також для обґрунтованого кількісного аналізу ризиків та визначення основних параметрів договору страхування.

На основі оцінок ризиків (з урахуванням реалізації рекомендованих заходів щодо їх зменшення) визначається одне з найбільш істотних умов договору страхування – ставка страхування. Як правило, її розмір не перевищує п'яти відсотків, однак на практиці він може варіюватися в діапазоні від декількох десятих часток відсотка до п'яти і більше відсотків. На розмір ставки у кожному конкретному випадку можуть вплинути декілька факторів:

- статистичні дані, що стосуються порушень інформаційної безпеки на аналогічних підприємствах;
- рівень захищеності інформаційних ресурсів даного підприємства (якість використовуваних технічних засобів, рівень організаційного забезпечення інформаційної безпеки на підприємстві і т.п.);
- інтенсивність поточної господарської діяльності (виконання поточних бізнес-операцій);
- страхова сума – вартість інформаційних активів, що підлягають страхуванню (як правило, чим більша вартість страхування ресурсів, тим нижче питома ставка страхування).

Крім ставки страхування в процесі узгодження умов договору також визначається інший важливий параметр – ліміт відповідальності страхової компанії (максимальна величина коштів, які можуть бути виплачені страховиком

страхувальнику протягом усього терміну дії договору страхування). Як правило, страхова сума повинна бути досить великою, щоб у страхової компанії була можливість компенсувати накладні витрати (зокрема, витрати на попереднє обстеження підприємства), пов'язані з укладанням договору страхування.

У разі реалізації ризику (виникнення страхового випадку) застраховані інформаційні ресурси можуть бути повністю втрачені. При цьому страхова компанія повинна буде зробити страхові виплати в повному обсязі (в межах встановленого ліміту відповідальності). У випадку, якщо пошкоджена тільки частина інформаційних ресурсів, для підприємства і страхової компанії починається складний процес визначення суми збитку, яка повинна бути компенсована. Така оцінка також може бути проведена незалежною третьою стороною. Крім того, предметом аналізу в цій ситуації можуть бути всі обставини, пов'язані зі страховим випадком. Зокрема, договором страхування може бути передбачений обов'язок підприємства-клієнта вжити низку заходів в рамках певного плану аварійних заходів з метою мінімізувати збиток. Таким чином, страхова компанія, перш ніж зробити виплати, повинна буде переконатися в тому, що підприємством-клієнтом були зроблені певні запобіжні заходи.

Та обставина, що взаємодія страховика і страхувальника при визначенні розміру страхових виплат є одним з найбільш проблемних питань, змушує передові компанії шукати нові форми організації процесу страхування. Так, наприклад, для вирішення проблем при реалізації деяких страхових ризиків та зменшення збитків третьою стороною в договорі страхування може виступати компанія – постачальник інформаційних систем і комплексних рішень, яка при настанні страхового випадку може на деякий час (на період відновлювальних робіт) надати резервні програмні та апаратні засоби для забезпечення безперервності основної діяльності підприємства-страхувальника, а також організувати самі відновлювальні роботи. У цьому випадку страхова компанія може скоротити розмір страхових виплат на компенсацію упущеної вигоди підприємства-страхувальника і уникнути деяких зайвих виплат на відновлення втрачених інформаційних ресурсів.

Крім страхування власне інформаційних ризиків, також важливе значення має страхування цивільної відповідальності компаній, що надають інформаційні послуги та послуги із захисту інформації великій кількості користувачів:

- страхування цивільної відповідальності засвідчувальних центрів, що працюють в інфраструктурі публічних ключів;
- страхування відповідальності фондових бірж та інших електронних торговельних майданчиків по відшкодуванню майнової шкоди третім особам;

- страхування цивільної відповідальності розробників і постачальників засобів захисту інформації.

Необхідність страхування цивільної відповідальності компаній-постачальників продуктів і послуг перед споживачами в цьому випадку обумовлена тим, що їх послугами (продуктами) користується велика кількість клієнтів, кожен з яких з використанням цих продуктів і послуг управляє дорогими інформаційними активами (фінансовими засобами, конфіденційними відомостями, розголошення яких може призвести до величезних збитків, і т.п.). Таким чином, у компаній-постачальників таких продуктів і послуг виникають ризики того, що до них будуть пред'явлені позови про відшкодування збитку, понесеного клієнтами внаслідок того, що зловмисники скористалися уразливими в поставляються продуктах. Очевидно, що власні активи і доступні засоби, наявні у компаній-постачальників, як правило, набагато менше потенційно можливого збитку, який може виникнути у їхніх клієнтів. В результаті цього страхування виявляється єдиним засобом забезпечення відповідальності і, отже, побудови цивілізованих взаємовідносин на ринку засобів захисту інформації, а також послуг із захисту інформації.

7.8.2. Ринок страхових послуг

Світова практика страхування інформаційних ризиків почала складатися в дев'яностих роках і отримала свій розвиток після 2000-го року, коли, з одного боку, ризики інформаційної безпеки стали більш серйозними, ніж будь-коли, а з іншого – в західних країнах остаточно склалася практика не включати інформаційні ризики в універсальні страхові поліси, якими зазвичай покривалися основні бізнес-ризики. Таким чином, до теперішнього часу найбільшими світовими компаніями, що надають послуги зі страхування інформаційних ризиків, є:

- Британська страхова компанія "Lloyds of London";
- американська компанія "AIG";
- Zurich North America ("The E-Risk Edge solution");
- страхова група "Chubb";
- страхова компанія "Marsh".

Страхування інформаційних ризиків компанією Lloyds of London здійснюється спільно з відомою компанією Counterpane, що надає послуги з оцінки стану захищеності інформаційних ресурсів і за поточною підтримки інформаційної безпеки. Також в цій роботі беруть участь компанії Frank Crystal & Co. і SafeOnline Ltd. Ці фірми пропонують два основних спільних страхових продукту:

- Internet Asset and Income Protection Coverage ("Покриття ризиків, пов'язаних з інформаційними активами і інформаційною діяльністю") – програма страхування інформаційних ресурсів окремих компаній;
- Internet Asset and Income Protection Warranty Plan ("План гарантування інформаційних активів та інформаційної діяльності") – заснований на страхуванні план гарантування надійності роботи постачальників послуг Інтернет.

Американська страхова компанія American International Group, Inc. (AIG), що діє в 130 країнах світу, в особі свого підрозділу AIG eBusiness Risk Solutions (AIG eBRS) пропонує програму страхування інформаційних ризиків netAdvantage (AIG netAdvantage Suite). У рамках своєї комплексної програми страхування ця компанія пропонує знижки клієнтам, які користуються певними засобами захисту інформації. Для забезпечення ефективності та комплексності послуг зі страхування AIG eBRS організовує технологічні альянси з компаніями, які постачають засоби захисту інформації, а також провідними аудити безпеки.

В рамках програми netAdvantage пропонується кілька варіантів страхового захисту:

- захист від збитків у разі неправомірного розголошення приватних даних;
- захист від знищення (втрати) даних або програмного забезпечення;
- захист від збитків у разі порушення операційної діяльності (упущена вигода і додаткові витрати) у разі порушень інформаційної безпеки;
- страхова компенсація витрат на нейтралізацію вразливостей;
- страхова компенсація витрат на відновлення ділової репутації (PR) у разі реалізації ризиків.

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, «Магнолія 2006», 2013. – 256 с.
2. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) - Львів, «Магнолія 2006», 2014. – 312 с.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологи, протоколы: Ученик для вузов. 5-е узд.– СПб.: Питер, 2016. – 992 с.
4. Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.
5. Жуков І.А., Дрововозов В.І., Махновський Б.Г.Експлуатація комп'ютерних систем та мереж. – К.: НАУ , 2007.-361с.
6. Антонов, В.М. Сучасні комп'ютерні мережі. - К. : МК-Прес, 2005. – 478 с.
7. В.П. Бабак, О.Г. Корченко. Інформаційна безпека та сучасні мережеві технології. – К. : НАУ, 2003. – 670 с.
8. Буров Є.В. Комп'ютерні мережі: підручник.– Львів: Магнолія 2006, 2010. – 262 с.
9. Мельник І.В. За ред. Л.С. Глоби. Інформаційні комп'ютерні мережі: Навч. посіб. для дистанційного навч. – К.: Ун- т "Україна", 2006. – 250с.
10. Ю.С. Рамський, В.П. Олексюк, А.В. Балик. Адміністрування комп'ютерних мереж і систем: навчальний посібник. – Тернопіль: Навч. кн. - Богдан, 2010. – 196 с.
11. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley. 20th Anniversary edition. 2015. 784 p..
12. В. Олексюк, Н. Балик, А. Балик. Організація комп'ютерної локальної мережі. – К.: Підручники та посібники, 2006.-80с.
13. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 6th Edition. 2016. 464 p.
14. Stallings W., Brown L., Computer Security: Principles and Practice. Pearson, 2017. 800 p.
15. Keith W. Ross. Computer Networking: A Top-Down Approach. Pearson, 7th Edition. 2016. 864 p.
16. Остапов С. Е. Основи криптографії: навчальний посібник / С. Е. Остапов, Л. О. Валь. – Чернівці: Книги–ХХІ, 2008. – 188 с.
17. Єфіменко А. А. Порівняльний аналіз алгоритму симетричного блокового перетворення «Калина» (ДСТУ 7624:2014) з іншими міжнародними

стандартами шифрування даних / А.А. Єфіменко, Є. М. Байлюк, О. А. Покотило //Збірник наукових праць ЖВІ. Випуск 15, С. 156-162.
18. Грайворонський М. В. Безпека інформаційно-комунікаційних систем /М. В. Грайворонський, О. М. Новіков – К.: Видавнича група BHV, 2009. – 608 с.
19. Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів. БаК, 2003. –168 с.
20. Яковина В.С., Федасюк Д.В. Основи безпеки комп’ютерних мереж: Навчальний посібник / За ред. Д.В. Федасюка. – Львів: НВФ «Українські технології», 2008. – 396 с..
21. Струтинська О. В. Інформаційні системи та мережеві технології / О. В. Струтинська., 2008. – 211 с.
22. Величко О. М. Інтелектуальні інформаційні системи: структура і застосування / О. М. Величко, Т. Б. Гордієнко., 2022. – 728 с..
23. Лунтовський А. О. Проектування та дослідження комп'ютерних мереж / А. О. Лунтовський, І. В. Мельник. – Київ: Університет "Україна", 2010. – 362 с.
24. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видавничій Центр, 2002. – 520 с.
25. Буров Є. Комп’ютерні мережі. 2-ге оновлене і доповн. Вид. Львів: Бак, 2003. – 584 с.
26. О. В. Тимошенко. Комп'ютерна безпека. Захист від хакерів та вірусів. Київ: КМ-Букс, 2018 – 432с.
27. Ю. М. Єфремов, В. І. Захарченко, В. В. Рибак. Комп'ютерні мережі. Київ: Кондор, 2019. – 624с.
28. М. В. Семикіна. Комп'ютерні мережі та інтернет. Харків: Техніка, 2018. – 528с..
29. О. О. Єфремов. Захист комп'ютерних мереж. Київ: Папірус, 2020. – 400с.
30. Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / І. В. Горбатий, А. П. Бондарєв. – Львів: Львівська політехніка, 2016. – 336 с.
31. Олифер В. Г., Олифер Н. А. Новые технологии и оборудование IP-сетей. - СПб.: БХВ-Санкт-Петербург, 2010.
32. Новиков О.М. , Гайворонський М.В. Захист інформації в комп’ютерних системах і мережах. – К.: «Издательская группа bhv», 2006. – 496 с.
33. Gary A. Donahue. Network Warrior. O'Reilly Media; 1st edition. 2007. 913 p.