МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ

МЕТОДИЧНІ ВКАЗІВКИ

ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ З ДИСЦИПЛІНИ

«ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ»

для студентів денної форми навчання

спеціальності 125 Кібербезпека

Луцьк - 2024

УДК 004.7-049.5](072)

М 54

Методичні вказівки до виконання лабораторних робіт з дисципліни «Захист комп'ютерних мереж» для студентів спеціальності 125 Кібербезпека денної форми навчання освітнього ступеню «бакалавр» [Електронний ресурс] / уклад. С.Я. Гільгурт. – Луцьк : ДонНТУ, 2024. – 160 с.

Наведено завдання до виконання лабораторних робіт з дисципліни «Захист комп'ютерних мереж». Для кожної роботи вказано мету, у стислій формі надано теоретичні відомості, сформульовано завдання, описано порядок виконання робіт, а також наведено контрольні питання, перелік літературних джерел, вимоги до оформлення звітів. Додано зразок титульної сторінки. Завдання лабораторних робіт складені з метою кращого засвоєння знань, отриманих студентами при вивченні лекційного матеріалу та придбання навичок розробки і використання технології захисту інформаційної та/або кібербезпеки в комп'ютерних мережах.

Укладач: С.Я. Гільгурт, професор кафедри ПМІ, д-р техн. наук, ст. наук. співр.

Рецензент: С.О.Ковалев, к.т.н., доцент, в.о.зав.каф. ЕТКІ

Відповідальний за випуск:
Н.О. Маслова, завідувач кафедри прикладної математики і інформатики

Затверджено на засіданні навчально-методичного відділу ДонНТУ,
протокол № 9 від 30.04.2024 р.

Ухвалено на засіданні кафедри прикладної математики і інформатики,
протокол № 4 від 09 квітня 2024 р.

ЗМІСТ

ВСТУП

Метою вивчення навчальної дисципліни «Захист комп'ютерних мереж» є опанування методами захисту комп`ютерних мереж, підготовка фахівців, здатних розробляти і використовувати технології захисту інформаційної та/або кібербезпеки. Лабораторний практикум є важливою складовою частиною навчального процесу, найефективнішою формою пізнавальної діяльності студентів, розвиває навички самостійної дослідницької роботи, унаочнює та поглиблює теоретичний курс предмета. Методичні вказівки включають пояснення та приклади до виконання лабораторних робіт, що в цілому повинно сприяти формуванню у студентів здатностей із захисту даних, оволодінню практичними навичками з проведення процедур захисту комп`ютерних мереж.

Всі лабораторні роботи мають певну мету, містять стислі теоретичні відомості, опис порядку виконання, вимоги до змісту звіту та питання для самоконтролю.

Навички, якими студент опановує під час виконання завдань лабораторних робіт, включених до методичних вказівок, можуть виявитися корисними під час його подальшої професійної діяльності, оскільки дозволяють використовувати певний напрацьований інструментарій володіння програмними та технічними засобами забезпечення кібербезпеки та захисту інформації в комп'ютерних мережах різного рівня.

ЛАБОРАТОРНА РОБОТА 1. НАЛАШТУВАННЯ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

Мета роботи: набуття навичок налаштування міжмережевих екранів у UNIX-подібних операційних системах.

1.1. Теоретичний матеріал до лабораторної роботи

1.1.1. Загальні теоретичні відомості

Міжмережевий екран можна визначити як певний засіб захисту інформації. Спеціальне поєднання в ньому апаратного та програмного забезпечення дозволяє здійснювати аналіз та фільтрацію мережевих пакетів, що проходять через нього. Залежно від встановлених правил, міжмережевий екран пропускає або знищує пакети і таким чином дозволяє або забороняє мережеві з'єднання. Встановлюють міжмережевий екран на межі між внутрішньою (захищеною) та зовнішньою (потенційно небезпечною) мережами. Це класичний засіб захисту периметра комп'ютерної мережі, який контролює з'єднання між вузлами цих мереж. Синонімами за визначенням міжмережевого екрану є фаєрвол або файрвол (від англ. терміну Firewall) та брандмауер (німецький термін brandmauer).

Фільтрація пакетів проводиться на підставі правил. Найбільш безпечним для формування правил міжмережевого екрану вважається підхід «заборонено все, що явно не дозволено». У цьому випадку мережевий пакет перевіряється на відповідність дозвільним правилам, а якщо таких не знайдеться, то пакет буде відкинуто. Але в деяких випадках застосовується і зворотний принцип: "дозволено все, що явно не заборонено". Тоді перевірка проводиться на відповідність заборонним правилам, і якщо таких не буде знайдено, пакет буде пропущено.

Фільтрацію можна проводити на різних рівнях еталонної моделі мережевої взаємодії OSI. За цією ознакою міжмережеві екрани можна умовно поділити на три основні класи:

- брандмауер екранного маршрутизатора (мережевий фільтр);

- екранувальний транспорт (шлюз сеансового рівня);
- екранувальний шлюз (посередник прикладного рівня).

Брандмауер екранного маршрутизатора також відомий як брандмауер мережевого рівня або брандмауер з фільтруванням пакетів. Пакетна фільтрація є однією із давно відомих та розповсюджених технологій управління доступом до мережі, тому, зазвичай, брандмауери мають таку функцію. Брандмауер з фільтрацією пакетів це або маршрутизатор, або виконувана на сервері програма, які відповідно до своєї конфігурації фільтрують вхідні та вихідні пакети. Брандмауер пропускає або відкидає пакети у відповідності до інформації, яка є у IP-заголовках пакетів. Наприклад, пакети можуть пропускатись або відхилятись на основі інформації, що дозволяє асоціювати цей пакет із конкретними відправником та отримувачем (повна асоціація), яка складається із наступних елементів:

- адреса відправника;
- адреса отримувача;
- інформація про додаток або протокол;
- номер порту джерела;
- номер порту отримувача.

Усі маршрутизатори (навіть ті, які не налаштовані для фільтрації пакетів), зазвичай перевіряють повну асоціацію пакета, щоб визначити, куди його потрібно направити. Брандмауер із фільтрацією пакетів перед відправленням пакета одержувачу порівнює його повну асоціацію з таблицею правил, відповідно до яких він повинен пропустити або відбракувати цей пакет. Якщо брандмауер отримав пакет, який не відповідає жодному табличному правилу, він застосовує правило, задане за замовчуванням, яке також має бути чітко визначене в таблиці брандмауера. З міркувань безпеки це правило зазвичай вказує на необхідність відбракування всіх пакетів, що не задовольняють жодному з інших правил.

Можна задати правила фільтрації пакетів, які «вказуватимуть» брандмауеру, які пакети повинні бути пропущені, а які відбраковані.

Наприклад, можна визначити правила таким чином, щоб брандмауер відбраковував пакети, що надходять від зовнішніх серверів, IP-адреси яких вказані в таблиці. Можна також задати правило, відповідно до якого буде дозволено пропускати лише вхідні повідомлення електронної пошти, адресовані поштовому серверу, або правило блокування всіх поштових повідомлень, що надходять від зовнішнього хоста, яке розсилало спам.

Також можна налаштувати брандмауер для фільтрації пакетів на основі номерів портів, що задаються в заголовках пакетів TCP та UDP (User Datagram Protocol). У цьому випадку можна буде пропускати окремі види пакетів (наприклад, Telnet або FTP), лише якщо вони надсилаються до певних серверів (відповідно до Telnet або FTP). Однак успішне виконання подібного правила залежить від того, які угоди прийняті в мережі, що функціонує на основі TCP/IP: для роботи додатків TCP/IP сервери та клієнти зазвичай використовують конкретні порти (які часто називають відомими, тобто наперед визначеними), однак це не є обов'язковою умовою.

Наприклад, програма Telnet на серверах мережі з TCP/IP зазвичай працює через порт 23. Щоб дозволити сеанси Telnet тільки з певним сервером, необхідно задати правила, одне з яких "змусить" брандмауер пропускати всі пакети, що запитують порт 23 за адресою 123.45.6.7 (приклад IP-адреси сервера Telnet), а інше – відбраковувати вхідні пакети, які вимагають цей порт за іншими адресами. Зазвичай, реальні правила є складнішими і передбачають виконання декількох умов одночасно.

Переваги брандмауерів з фільтруванням пакетів:

- відносна невисока вартість;
- невелика затримка під час проходження пакетів.

Недоліки брандмауерів із фільтрацією пакетів:

- локальна мережа маршрутизується із Інтернет;
- правила фільтрації складні в описанні, тому потребують певні знання технологій TCP та UDP;
- відсутня автентифікація на рівні користувача;

– аутентифікацію з використанням IP-адреси можна обійти за допомогою IP-спуфінгу, коли атакуюча система видає себе за іншу через підміну IP-адреси.

Шлюз сеансового рівня стежить за підтвердженням зв'язку (квитування) між авторизованим клієнтом і зовнішнім хостом (і навпаки), визначаючи, чи сеанс зв'язку, що запитується, допустимим. При фільтрації пакетів шлюз сеансового рівня полягає в інформації, що у заголовках IP-пакетів сеансового рівня протоколу TCP, тобто. функціонує на два рівні вище, ніж брандмауер із фільтрацією пакетів.

Щоб визначити, чи є запит на сеанс зв'язку допустимим, шлюз сеансового рівня виконує приблизно таку процедуру. Коли авторизований клієнт запитує деяку послугу, шлюз приймає цей запит, перевіряючи, чи задовольняє клієнт базовим критеріям фільтрації (наприклад, чи DNS-сервер може визначити IP-адресу клієнта та асоційоване з ним ім'я). Потім, діючи від імені клієнта, шлюз встановлює з'єднання із зовнішнім хостом і слідкує за виконанням процедури квитування зв'язку протоколу TCP.

Ця процедура складається з обміну TCP-пакетами, які позначаються прапорами SYN (синхронізувати) та ACK (підтвердити). Перший пакет сеансу TCP, позначений прапором SYN і містить довільне число, наприклад 1000, є запитом клієнта на відкриття сеансу. Зовнішній хост, який одержав цей пакет, посилає у відповідь пакет, позначений прапором ACK і містить число, на одиницю більше, ніж у прийнятому пакеті (у нашому випадку 1001), підтверджуючи таким чином прийом пакета SYN від клієнта. Після цього здійснюється зворотна процедура: хост посилає клієнту пакет SYN з вихідним числом (наприклад, 2000), а клієнт підтверджує отримання передачею пакета ACK, що містить число 2001.

У цьому процес квитування зв'язку завершується. Шлюз сеансового рівня "вважає" запитаний сеанс допустимим тільки в тому випадку, якщо при виконанні процедури квитування зв'язку прапори SYN і ACK, а також числа, що містяться в TCP-пакетах, логічно пов'язані між собою. Після того як шлюз «визначив», що довірений клієнт та зовнішній шлюз є авторизованими

учасниками сеансу TCP, та перевірив допустимість цього сеансу, він встановлює з'єднання.

Починаючи з цього моменту, шлюз просто копіює і перенаправляє пакети туди і назад, не проводячи жодної фільтрації. Він підтримує таблицю встановлених з'єднань, пропускаючи дані, які стосуються одному з сеансів зв'язку, які зафіксовані у цій таблиці. Коли сеанс завершується, шлюз видаляє відповідний елемент з таблиці та розриває ланцюг, що використовується в даному сеансі. Для копіювання та перенаправлення пакетів у шлюзах сеансового рівня використовуються спеціальні програми, які іноді називають канальними посередниками (pipe proxies), оскільки вони встановлюють між двома мережами віртуальний ланцюг, або канал, а потім дозволяють пакетам (що генеруються додатками TCP/IP) проходити по цьому каналу.

Шлюз сеансового рівня виконує ще одну важливу функцію захисту: він використовується як сервер-посередник (proxy server). І хоча цей термін передбачає наявність сервера, на якому працюють програми-посередники (що справедливо для шлюзу сеансового рівня), у цьому випадку він означає дещо інше. Сервером-посередником може бути брандмауер, який використовує процедуру трансляції адрес, при якій відбувається перетворення внутрішніх IP-адрес в одну «надійну» IP-адресу. Ця адреса асоціюється з брандмауером, з якого передаються всі вихідні пакети.

В результаті в мережі зі шлюзом сеансового рівня всі вихідні пакети виявляються відправленими з цього шлюзу, що виключає прямий контакт між внутрішньою (авторизованою) мережею і потенційно небезпечною зовнішньою мережею (у нашому випадку мережа Інтернет). IP-адреса шлюзу сеансового рівня стає єдиною активною IP-адресою, яка потрапляє до зовнішньої мережі. Таким чином, шлюз сеансового рівня та інші сервери-посередники захищають внутрішні мережі від нападів типу spoofing (імітація адрес або підміна адрес).

Шлюзи сеансового рівня немає «вроджених» вразливих місць, проте після встановлення зв'язку такі шлюзи фільтрують пакети лише з сеансовому рівні, тобто. не можуть перевіряти вміст пакетів, що передаються між внутрішньою

та зовнішньою мережею на рівні прикладних програм, тобто ця передача здійснюється «наосліп». Таким чином, хакер, що знаходиться в зовнішній мережі, може "протягнути" свої "шкідливі" пакети через шлюз і звернеться безпосередньо до внутрішнього веб-серверу, який сам по собі може не забезпечувати функції брандмауера. Іншими словами, якщо процедура квитування зв'язку успішно завершена, шлюз сеансового рівня встановить з'єднання і буде тупо копіювати і перенаправляти всі наступні пакети незалежно від їх вмісту.

Щоб фільтрувати пакети, що генеруються певними мережними службами відповідно до їх вмісту, потрібен шлюз прикладного рівня.

Так само як і шлюз сеансового рівня, шлюз прикладного рівня (посередник) перехоплює вхідні та вихідні пакети, використовує програми-посередники, які копіюють та перенаправляють інформацію через шлюз, а також функціонує як сервер-посередник, виключаючи прямі з'єднання між довіреним сервером або клієнтом та зовнішнім хостом . Однак посередники, що використовуються шлюзом прикладного рівня, мають важливі відмінності від канальних посередників шлюзів сеансового рівня: по-перше, вони пов'язані з програмами, а по-друге, можуть фільтрувати пакети на прикладному рівні. На відміну від канальних посередників, посередники прикладного рівня пропускають лише пакети, які їм доручено обслуговувати. Наприклад, програма-посередник служби Telnet може копіювати, перенаправляти та фільтрувати лише графік, який генерується цією службою.

Якщо в мережі працює лише шлюз прикладного рівня, то можуть передаватися вхідні та вихідні пакети лише тих служб, котрим є відповідні посередники. Так, якщо шлюз прикладного рівня використовує лише програми-посередники FTP і Telnet, він пропускатиме пакети цих служб, блокуючи у своїй пакети всіх інших служб. На відміну від шлюзів сеансового рівня, які копіюють і «сліпо» перенаправляють всі пакети, що надходять, посередники прикладного рівня перевіряють вміст кожного пакета, що проходить через шлюз.

Ці посередники можуть фільтрувати окремі види команд або інформації протоколах прикладного рівня, які їм доручено. Утиліти цих шлюзів дозволяють фільтрувати певні команди, що використовуються цими службами (FTP, Telnet, HTTP тощо). Наприклад, можна налаштувати шлюз таким чином, щоб він запобігав використанню клієнтами команди FTP Put, яка дає можливість користувачеві, підключеному до FTP-серверу, записувати на нього інформацію. Багато мережних адміністраторів воліють заборонити використання цієї команди, щоб зменшити ризик випадкового пошкодження інформації, що зберігається на FTP-сервері, і ймовірність заповнення його гігабайтами хакерських даних, що пересилаються на сервер для заповнення його дискової пам'яті і блокування роботи.

На додаток до фільтрації пакетів багато шлюзів прикладного рівня реєструють всі виконувані сервером дії і, що найважливіше, попереджають мережевого адміністратора про можливі порушення захисту, надсилаючи йому повідомлення електронною поштою або на мессенджер.

Переваги:

- локальна мережа невидима з Internet;
- захист на рівні додатків дозволяє здійснювати велику кількість додаткових перевірок, знижуючи цим ймовірність злому з використанням дірок у програмному забезпеченні;
- при організації автентифікації на рівні користувача може бути реалізована система негайного попередження про спробу злому.

Недоліки:

- вища, ніж для пакетних фільтрів вартість;
- продуктивність нижча, ніж для пакетних фільтрів.

Брандмауери експертного рівня поєднують у собі елементи всіх описаних вище категорій. Як і брандмауери з фільтрацією пакетів, вони працюють на мережному рівні, фільтруючи вхідні та вихідні пакети на основі перевірки IP-адрес та номерів портів. Брандмауери експертного рівня також виконують функції шлюзу сеансового рівня, визначаючи, чи пакети відносяться до

відповідного сеансу. І, нарешті, брандмауери експертного рівня беруть він функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета відповідно до політики безпеки, виробленої у конкретній організації. Як і шлюз прикладного рівня, брандмауер експертного рівня може бути налаштований для відбраковування пакетів, що містять певні команди, наприклад команди Put та Get служби FTP. Однак, на відміну від шлюзів прикладного рівня, при аналізі даних прикладного рівня такий брандмауер не порушує клієнт-серверної моделі взаємодії в мережі.

Шлюз прикладного рівня встановлює два з'єднання: одне – між авторизованим клієнтом та шлюзом, друге – між шлюзом та зовнішнім хостом. Після цього він просто пересилає інформацію між цими двома з'єднаннями. Незважаючи на високий рівень захисту, що забезпечується подібними шлюзами, така схема може позначитись на продуктивності роботи. На противагу цьому брандмауери експертного рівня допускають прямі з'єднання між клієнтами та зовнішніми хостами. Для забезпечення захисту такі брандмауери перехоплюють та аналізують кожен. Замість застосування пов'язаних із додатками програм-посередників, брандмауери експертного рівня використовують спеціальні алгоритми розпізнавання та обробки даних на рівні додатків.

За допомогою цих алгоритмів пакети порівнюються з відомими шаблонами даних, що теоретично має забезпечити більш ефективну фільтрацію пакетів. Оскільки брандмауери експертного рівня допускають пряме з'єднання між авторизованим клієнтом та зовнішнім хостом, деякі стверджують, що брандмауери цієї категорії забезпечують менш високий рівень захисту, ніж шлюзи прикладного рівня. Інші ж дотримуються протилежної думки. Проте брандмауери експертного рівня забезпечують один із найвищих на сьогоднішній день рівнів захисту корпоративних мереж, і, за твердженням фахівців, обдурити їх дуже не просто. Однак не варто забувати, що навіть ці надійні брандмауери не забезпечують 100% безпеки.

На рис. 1.1 представлено типові схеми підключення міжмережевих екранів. У першому випадку (рис. 1.1 а) міжмережевий екран встановлюється після маршрутизатору і захищає всю внутрішню мережу. Така схема застосовується, якщо вимоги у сфері захисту від несанкціонованого міжмережевого доступу приблизно однакові для всіх вузлів внутрішньої мережі. Наприклад, "дозволяти з'єднання, що встановлюються з внутрішньої мережі у зовнішню, і припиняти спроби підключення із зовнішньої мережі у внутрішню".

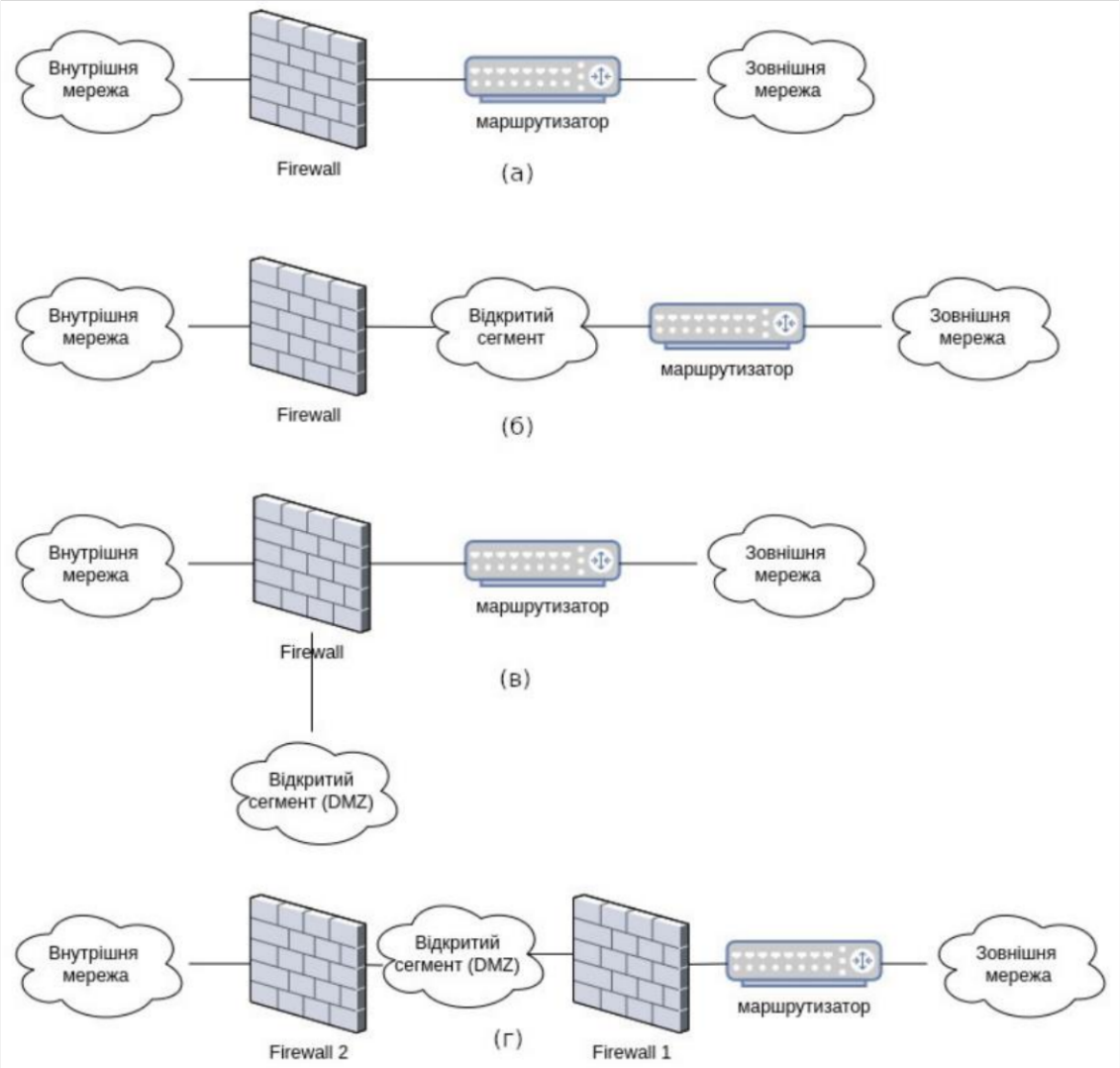


Рисунок 1.1 – Типові схеми підключення міжмережевих екранів:
а) підключення файрволу із двома мережевими інтерфейсами;
б) підключення файрволу з двома мережевими інтерфейсами при виділенні відкритого сегмента внутрішньої мережі;
в) підключення файрволу з трьома мережевими інтерфейсами;
г) підключення двох файрволів

Якщо вимоги для різних вузлів різні – наприклад, потрібно розмістити поштовий сервер, до якого можуть підключатися «ззовні», то подібна схема установки міжмережевого екрана не є достатньо безпечною. Наприклад, хакер у результаті реалізації мережевої атаки може отримати контроль над таким поштовим сервером і через нього вже отримає доступ до інших вузлів внутрішньої мережі. У подібних випадках іноді перед міжмережевим екраном створюється відкритий сегмент мережі підприємства (рис. 1.1, б), а мережевий екран захищає іншу внутрішню мережу. Недолік цієї схеми у тому, що підключення до вузлів відкритого сегмента міжмережевим екраном не контролюється.

Кращим у цьому випадку є використання міжмережевого екрану з трьома мережевими інтерфейсами (рис. 1.1, в). Міжмережевий екран з трьома мережними інтерфейсами конфігурується таким чином, щоб правила доступу у внутрішню мережу були більш суворими, ніж у відкритий сегмент. У той же час, і внутрішня мережа, і відкритий сегмент будуть контролюватись міжмережевим екраном. Такий відкритий сегмент часто зветься «демілітаризованою зоною» – DMZ.

Більш надійною для відкритого сегменту DMZ вважається схема, в якій для її захисту використовується два незалежних міжмережевих екрани (рис. 1.1, г). Другий файрвол реалізує набір правил фільтрації, що забезпечує захистом внутрішню мережу, які більш жорсткі проти правил першого файрволу, що контролює доступ до DMZ. Навіть успішна атака на перший файрвол не зробить внутрішню мережу беззахисною.

Типовим стало встановлення програмного файрволу на персональні комп'ютери або інші комп’ютери, що захищаються. Іноді такий файрвол називають "персональним". Подібна схема дозволяє захиститися від загроз, що надходять не тільки із зовнішньої мережі, а й із внутрішньої. Особливо актуальним є застосування персональних файрволів при безпосередньому підключенні комп'ютера до потенційно небезпечної мережі. Наприклад, при

підключенні домашнього комп'ютера до Інтернету або ноутбуку до загально доступної мережі кафе, вокзалу, транспорту, тощо.

1.1.2. Налаштування міжмережевого екрану в ОС Linux

Файрвол в UNIX-подібних операційних системах, зокрема в Linux, керується та налаштовується за допомогою утиліти ***iptables*** (або ***ip6tables*** – для протоколу IP версії IPv6). Для її використання необхідні привілеї суперкористувача (root). Налаштування даної утиліти доволі складне. Але в Інтернеті доступно багато довідкової інформації. Нижче наведено короткі відомості стосовно цієї утиліти.

Основними поняттями iptables є:

1. ***Правило***, яке складається з критерію, дії та лічильника. Якщо пакет відповідає критерію, то до нього застосовується дія, і він враховується лічильником. Якщо критерій відсутній, то неявно передбачається критерій "усі пакети". Якщо відсутня дія, то правило працюватиме лише як лічильник. Критерієм є логічний вираз, що аналізує властивості пакета та/або з'єднання і визначає, чи підпадає даний конкретний пакет під дію поточного правила. Дія описує те, що потрібно зробити із пакетом і/або з'єднанням, якщо вони відповідають правилу. Лічильник забезпечує облік кількості пакетів, які потрапили під критерій правила. Він враховує сумарний обсяг таких пакетів у байтах.

2. ***Ланцюжок*** – це упорядкована послідовність правил. Ланцюжки можна розділити на власні та базові. Базовий ланцюжок створюється за замовчуванням при ініціалізації таблиці. Кожен пакет, залежно від того, чи призначений він самому хосту, згенерований ним або є транзитним, повинен пройти набір базових ланцюжків різних таблиць. Крім того, базовий ланцюжок відрізняється від користувальницького наявністю «за замовчуванням дії» (default policy). Ця дія застосовується до тих пакетів, які було оброблено іншими правилами цього ланцюжка і викликаних з нього ланцюжків. Імена базових ланцюжків завжди записуються у верхньому регістрі (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING). Ланцюжок, що створюється користувачем може

використовуватись лише в межах своєї таблиці. Рекомендується не використовувати для таких ланцюжків імена у верхньому регістрі, щоб уникнути плутанини із базовими ланцюжками та вбудованими діями.

3. ***Таблицею*** є сукупність базових і користувальницьких ланцюжків, об'єднаних загальним функціональним призначенням. Імена таблиць (як і модулів критеріїв) записуються в нижньому регістрі, тому що в принципі не можуть конфліктувати з іменами ланцюжків користувача. При виклику команди iptables таблиця вказується у форматі -t ім'я_таблиці. У разі відсутності явної вказівки, використовується таблиця filter.

Усі пакети пропускаються через певні послідовності ланцюжків. При проходженні пакетом ланцюжка до нього послідовно застосовуються всі правила цього ланцюжка у порядку їх розташування. Під застосуванням правила розуміється перевірка пакета на відповідність критерію і, якщо пакет цьому критерію відповідає, застосовується до нього зазначена дія. Дією може бути як елементарна операція (наприклад, ACCEPT, MARK), так і перехід до одного із ланцюжків користувача. Дії можуть бути термінальними та нетермінальними. Термінальні дії припиняють обробку пакета в рамках даного базового ланцюжка, наприклад, ACCEPT, REJECT. Нетермінальні дії не переривають процес обробки пакета, наприклад, MARK, TOS. Якщо пакет пройшов через весь базовий ланцюжок і до нього не було застосовано жодної термінальної дії, то до нього застосовується стандартна дія для даного ланцюжка, яка є обов'язково термінальною.

Наступна команда дозволяє вивести список правил, що діють:

```
# iptables -L -n -v
```

Для виведення списку правил для пакетів, що приймаються (INPUT) або відправляються (OUTPUT) застосовуються наступні команди:

```
# iptables -L INPUT -n -v
# iptables -L OUTPUT -n -v
```

За допомогою наступних команд можна видалити усі або певні правила та ланцюжки:

```
# iptables -F
```

```
# iptables -X
# iptables -t nat -F
# iptables -t nat -X
# iptables -t mangle -F
# iptables -t mangle -X
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD ACCEPT
```

де -F – директива видалити (flush) усі правила;

-X – директива видалити ланцюжок;

-t table_name –вибрати таблицю(nat або mangle) і видалити усі правила;

-P –вибрати дії за замовчуванням (такі, як DROP, REJECT або ACCEPT).

До усіх пакетів, які відносяться до вже встановлених з'єднань, застосовується термінальна дія ACCEPT – пропустити:

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

В якості дії для пакетів, що надходять, за замовчуванням встановлюється DROP – блокування пакету:

```
iptables -P INPUT DROP
```

Наступне правило дозволяє прохід усіх пакетів, що виходять:

```
iptables -P OUTPUT ACCEPT
```

Тепер ланцюжок INPUT таблиці filter містить єдине правило, яке пропускає всі пакети, що стосуються вже встановлених з'єднань. До всіх інших вхідних пакетів буде застосовано стандартну дію – DROP. Ланцюжок OUTPUT взагалі не містить правил, тому до всіх вихідних пакетів застосовуватиметься дія за замовчуванням ACCEPT. Таким чином, хост, налаштований згідно з цим прикладом і підключений до Інтернету, буде недоступний ззовні (всі спроби встановити з'єднання зовні блокуються), проте з самого хоста доступ до Інтернету буде вільний (вихідні пакети дозволені, а відповіді на них уже відносяться до встановлених з'єднань).

У наступному прикладі показано, як заблокувати всі з'єднання з конкретної IP-адреси, а саме 10.10.10.10:

```
iptables -A INPUT -s 10.10.10.10 -j DROP
```

Якщо потрібно заблокувати всі IP-адреси в мережі 10.10.10.0/24 (тобто з маскою 255.255.255.0), можна використовувати маску мережі або стандартну косу риску для позначення діапазону IP-адрес:

```
iptables -A INPUT -s 10.10.10.0/255.255.255.0 -j DROP
iptables -A INPUT -s 10.10.10.0/24 -j DROP
```

Можливо також керувати підключенням до певного порту. в наступному прикладі показано, як заблокувати з'єднання SSH з адреси 10.10.10.10:

```
iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP
```

Елемент "ssh" можна замінити на інший номер протоколу або порту. Тут вираз "- tcp" повідомляє утиліті iptables, який протокол використовує з'єднання. Якщо замість TCP потрібно блокувати протокол UDP, цей вираз потрібно замінити на "-p udp".

У наступному прикладі показано, як заблокувати з'єднання SSH з будь-якої IP-адреси:

```
iptables -A INPUT -p tcp --dport ssh -j DROP
```

При короткочасовому підвищені навантаження на web-сервер з боку зовнішньої мережі дієвими є наступні правила.

– обмеження кількості з’єднань з однієї IP адреси:

```
iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 30 -j DROP
```

– блокування IP, наприклад, після 10 підключень до порту 80 на протязі 30 секунд:

```
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent -- set
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j DROP
```

Різке збільшення вхідного UDP трафіку та виявлення вихідного трафіку з усіх відкритих UDP-портів може вказувати на так званий UDP-Flood. Необхідно виставити обмеження на кількість підключень до відкритих портів і закрити порти, що не використовуються. Для цього додаються наступні правила.

– обмеження кількості підключень:

```
# iptables -I INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1
```

– дозволити підключення тільки перевіреним IP-адресам, наприклад, хосту з IP-адресою 1.2.3.4:

```
# iptables -A OUTPUT -p udp --dport 53 -d 1.2.3.4 -j ACCEPT
```

– блокування інших портів:

```
# iptables -A OUTPUT -p udp -j DROP
```

1.2. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи та виконати наступне завдання.

1.2.1. Опис задачі

Уявимо мережу яка задана IP-адресою 192.168.1.0 та маскою 255.255.255.0 і складається з трьох комп'ютерів, що мають наступні IP-адреси (рис. 1.2):

– PC1: 129.168.1.1/24;

– PC2: 129.168.1.2/24;

– PC3: 129.168.1.3/24.

Припустимо. що на комп'ютері PC1 встановлено та функціонує веб-сервер, наприклад, Apache.

Здійснімо уявно з обох комп'ютерів PC1 та PC2 flood-атаку на цей веб-сервер командою:

```
ping -f -c 100000 192.168.1.3
```

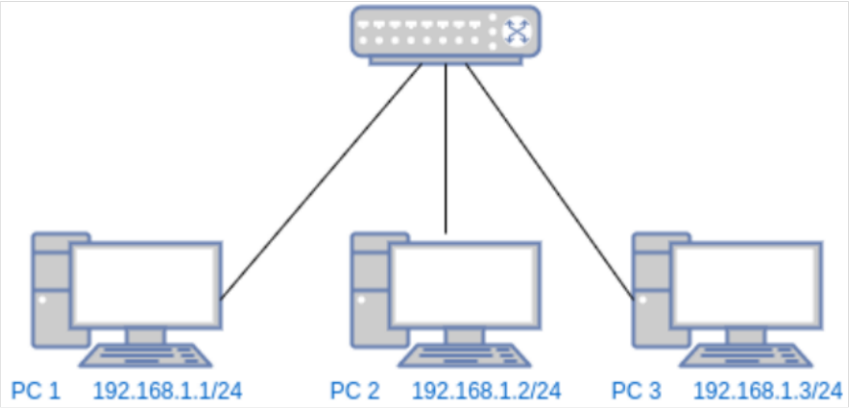


Рисунок 1.2 – Приклад мережі, що складається з трьох комп'ютерів

1.2.2. Завдання

Для свого варіанта (табл. 1.1) створіть правило (правила) для утиліти iptables на комп'ютері PC3, яке заблокує таку flood-атаку. Запропонуйте кілька різних варіантів. Поясніть, в чому різниця між ними, в яких ситуаціях які з них доцільно використовувати?

Таблиця 1.1 – Варіанти завдань до Лабораторної роботи 1

№ з/п	IP-адреси комп'ютерів	Маска підмережі
1.	PC1:192.168.3.28; PC2:192.168.3.29; PC3:192.168.3.30	255.255.255.0
2.	PC1:172.16.56.12; PC2:172.16.56.13; PC3:172.16.56.14	255.255.0.0
3.	PC1:10.4.0.34; PC2:10.4.0.34; PC3:10.4.0.34	255.0.0.0
4.	PC1:192.168.10.2; PC2:192.168.11.2; PC3:192.168.12.2	255.255.255.0
5.	PC1:172.16.16.17; PC2:172.16.16.18; PC3:172.16.16.19	255.255.0.0
6.	PC1:10.11.5.200; PC2:10.11.5.201; PC3:10.11.5.202	255.0.0.0
7.	PC1:192.168.1.23; PC2:192.168.1.24; PC3:192.168.1.25	255.255.255.0
8.	PC1:172.16.0.19; PC2:172.16.0.20; PC3:172.16.0.21	255.255.0.0
9.	PC1:10.13.128.21; PC2:10.13.128.22; PC3:10.13.128.23	255.0.0.0
10.	PC1:192.168.12.4; PC2:192.168.12.5; PC3:192.168.12.6	255.255.255.0

1.3. Питання до самоконтролю

1. Який сенс має поняття «правило» для утиліти iptables?
2. Який сенс має поняття «ланцюжок» для утиліти iptables?
3. Який сенс має поняття «таблиця» для утиліти iptables?
4. Назвіть базові ланцюжки та їх налаштування.
5. Яке правило виконується останнім?
6. В яких випадках є неприйнятною схема підключення файрволу згідно рис. 1.1, б? Чому?
7. Назвіть особливості та переваги схеми підключення файрволів згідно рис. 1.1, г.

1.4. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

1.5. Література до Лабораторної роботи 1

Рекомендовані літературні джерела до виконання Лабораторної роботи 1: [1-3]

ЛАБОРАТОРНА РОБОТА 2. МІЖМЕРЕЖЕВІ ЕКРАНИ ОС WINDOWS

Мета роботи: набуття навичок налаштування міжмережевих екранів у операційних системах сімейства Windows.

2.1. Теоретичний матеріал до лабораторної роботи

2.1.1. Загальні теоретичні відомості

Брандмауер Windows – вбудований в операційні системи сімейства Microsoft Windows міжмережевий екран. Вперше з'явився у версії Windows XP Service Pack 2. Потім був також вбудований у версії ОС:

- Windows Server 2003;
- Windows Vista;
- Windows Server 2008;
- Windows 7;
- Windows Server 2008 R2;
- Windows 8;
- Windows Server 2012;
- Windows RT;
- Windows 10;
- Windows 11.

Однією з відмінностей від попередника – Internet Connection Firewall – контроль доступу в мережу Інтернет окремих програм. Брандмауер Windows є частиною Центру забезпечення безпеки Windows.

За допомогою брандмауера можна запобігти атакам зовнішніх кіберзлочинців та проникненню на комп'ютер шкідливих програм через мережу або Інтернет. Крім того, брандмауер запобігатиме надсиланню зловмисних програм із вашого комп'ютера на інші.

Спочатку Windows XP включала «Брандмауер підключення до інтернету» («Internet Connection Firewall»), який (за умовчанням) був вимкнений через проблеми сумісності. Налаштування «Internet Connection Firewall» знаходилися

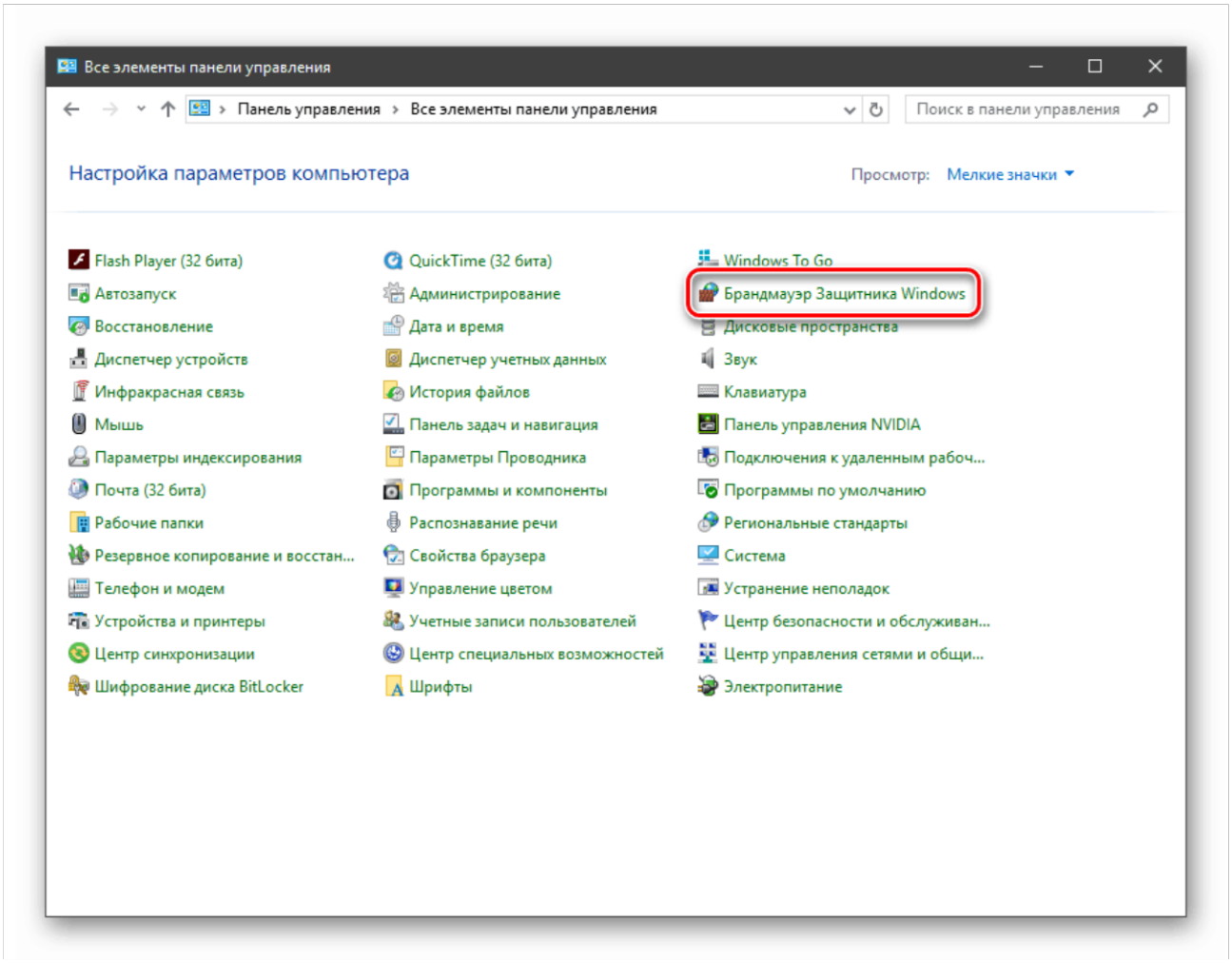
в конфігурації мережі, тому багато користувачів не знаходили їх. В результаті в середині 2003 року комп'ютерний хробак Blaster атакував велику кількість комп'ютерів під управлінням ОС Windows, використовуючи уразливість в службі Віддалений виклик процедур. Через декілька місяців хробак Sasser провів аналогічну атаку. Протягом 2004 року поширення цих хробаків продовжувалося, внаслідок чого комп’ютери з не оновленими вчасно ОС заражалися протягом кількох хвилин. Компанія Microsoft отримала критичні зауваження і тому булла вимушена поліпшити функціональність та інтерфейс міжмережевого екрану Internet Connection Firewall. Тоді ж він був перейменований в «Брандмауер Windows».

В брандмауер Windows вбудований журнал безпеки, який дозволяє фіксувати IP-адреси та інші дані, що відносяться до з'єднань в домашніх і офісних мережах або в мережі Інтернет. Можна організувати реєстрацію як успішних підключень, так і пропущених пакетів.

Брандмауер Windows дозволяє певним чином підвищити рівень безпеки персонально комп’ютера за відсутністю інших встановлених міжмережевих екранів. На відміну від продуктів сторонніх виробників цей засіб відносно простий в управлінні та має дружній інтерфейс, звичний для користувачів ОС Windows.

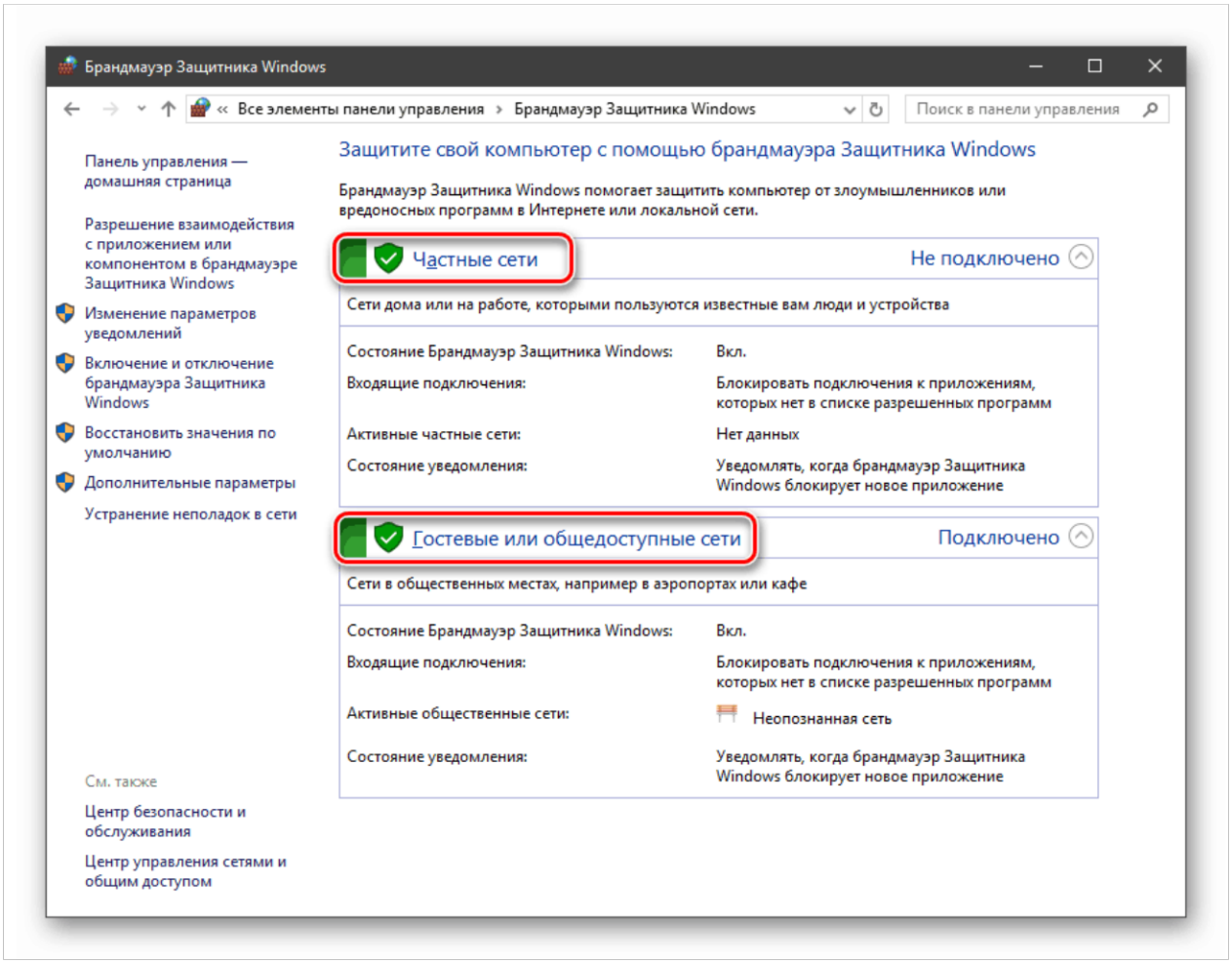
2.1.2. Налаштування брандмауера Windows

Відкрити брандмауер Windows можна в різний спосіб. Зокрема – з *«Панелі управління»* Windows. Перемикаємось на режим перегляду *«Дрібні піктограми»*, знаходимо та запускаємо аплет *«Брандмауер для захисника Windows»*:



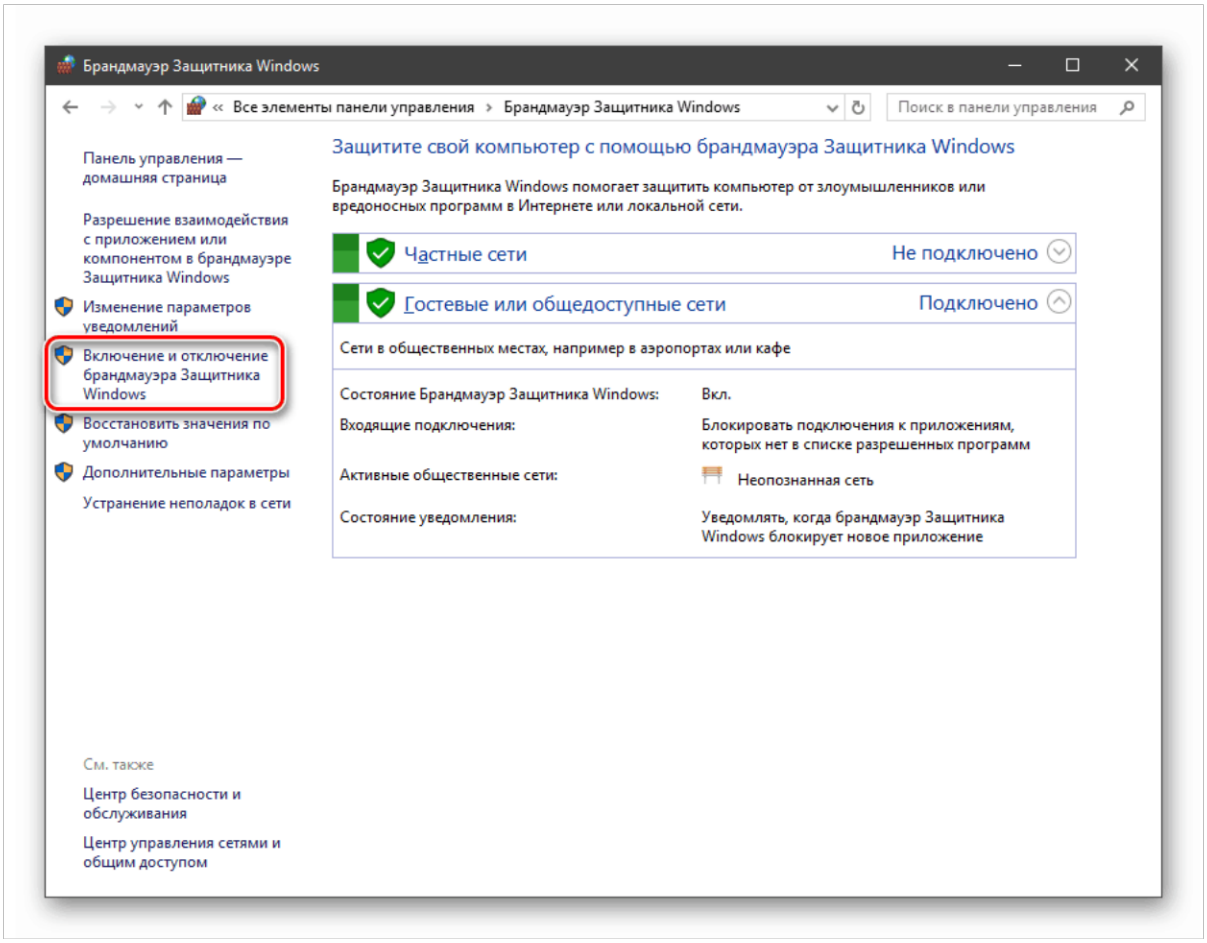
2.1.3. Типи мереж на персональному комп’ютері

Розрізняють два типи мереж: приватні та спільного використання. Першими вважаються довірені підключення до пристроїв, наприклад, вдома або в офісі, коли всі вузли відомі і безпечні. Другими – з'єднання з зовнішніми джерелами через дротові або бездротові мережеві адаптери. За замовчуванням спільні мережі вважаються небезпечними, і до них застосовуються більш суворі правила:

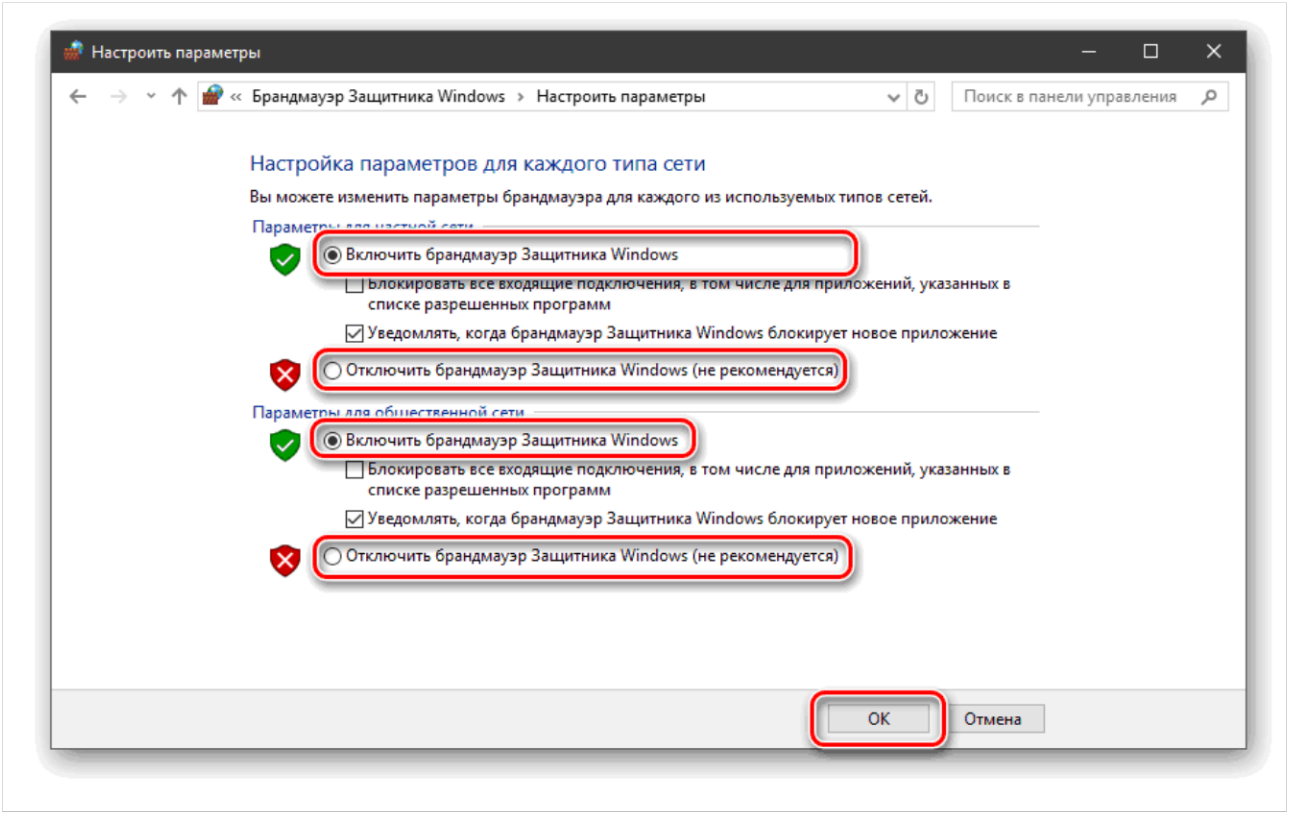


2.1.4. Вмикання та вимикання, блокування, повідомлення

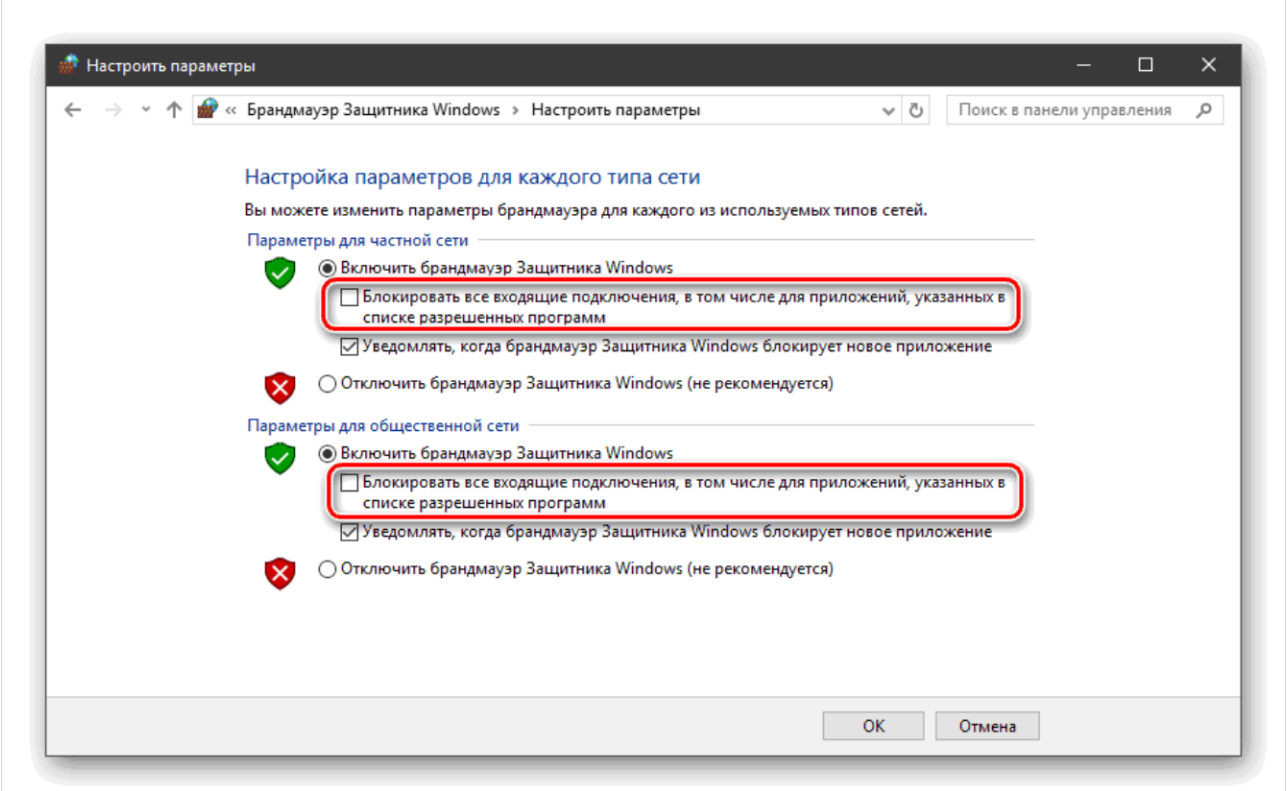
2.1.4.1. **Вмикання.** Активувати брандмауер або вимкнути його можна за відповідним посиланням в розділі налаштувань:



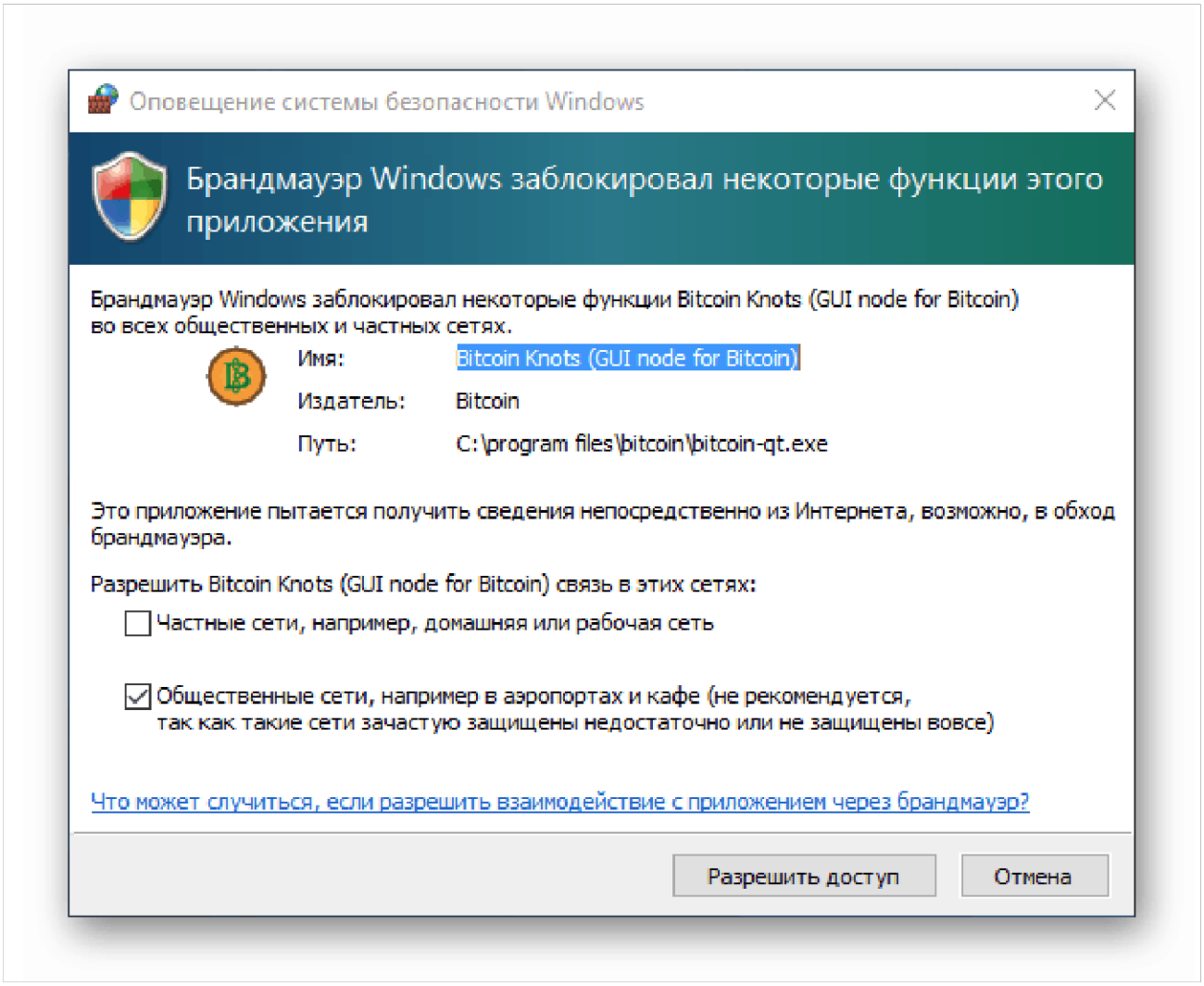
Тут досить поставити перемикач в потрібне положення і натиснути ОК:



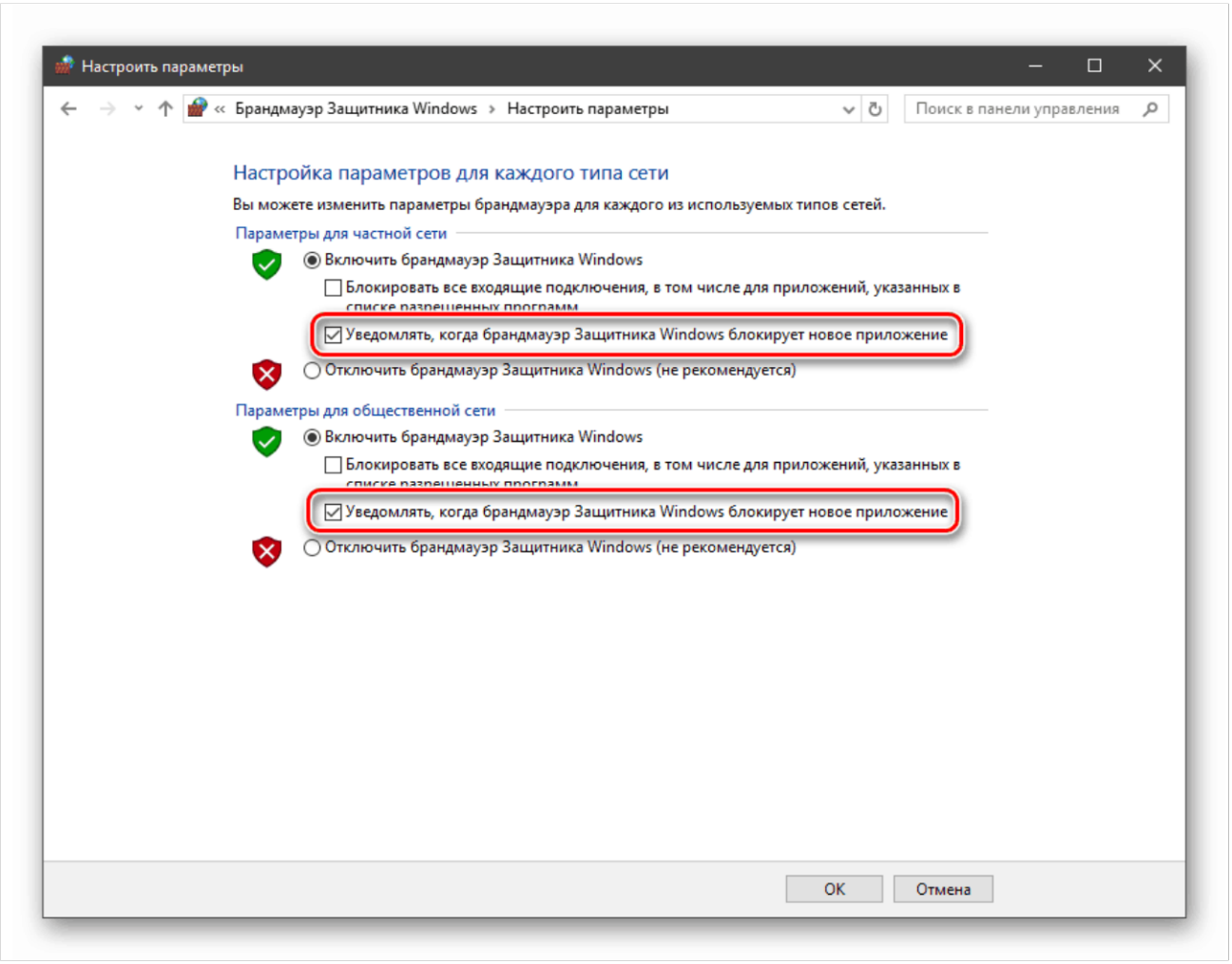
2.1.4.2. **Блокування** забороняє всі вхідні підключення! Будь-які додатки, в тому числі браузери, не зможуть завантажувати дані з мережі:



2.1.4.3. **Повідомлення** – це особливі вікна, що виникають при спробах підозрілих програм вийти в інтернет або увійти в локальну мережу:

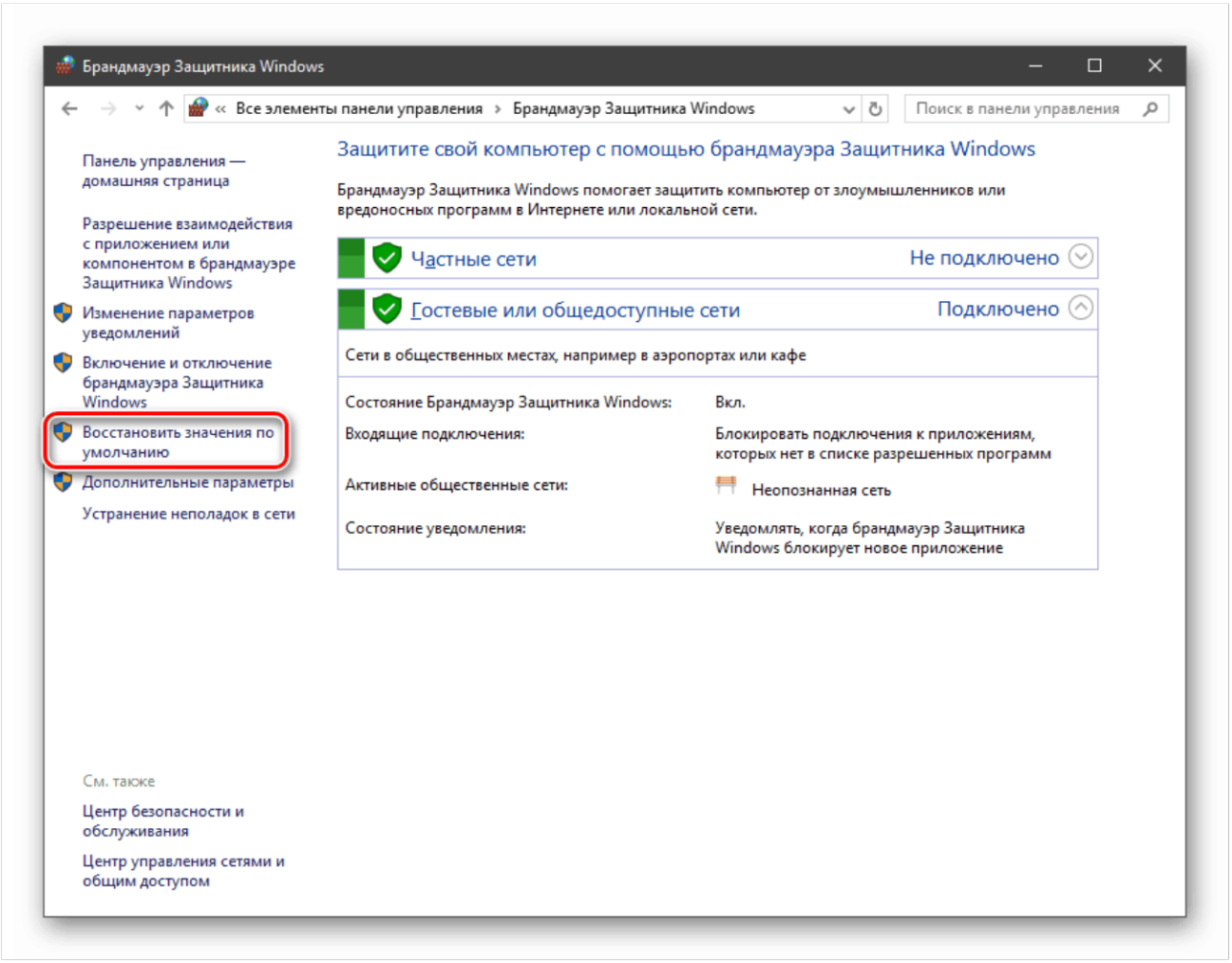


Повідомлення можна вимкнути зняттям прапорців в зазначених чекбоксах:

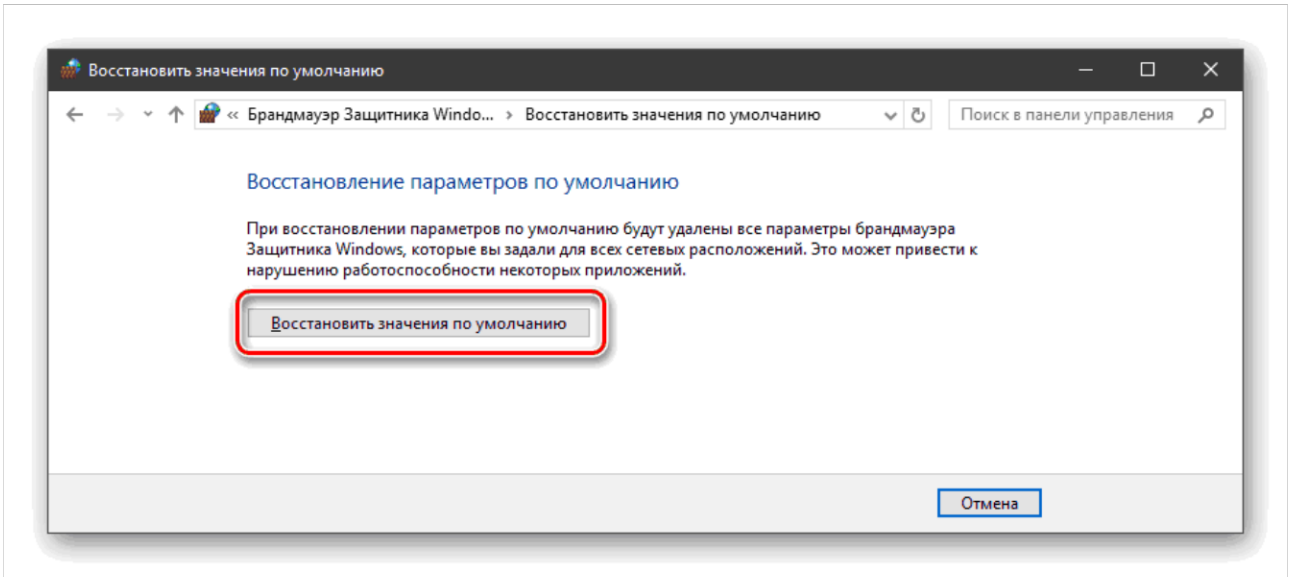


2.1.5. Скидання налаштувань

Дана процедура видаляє всі призначені для користувача правила і призводить параметри до значень за замовчуванням:

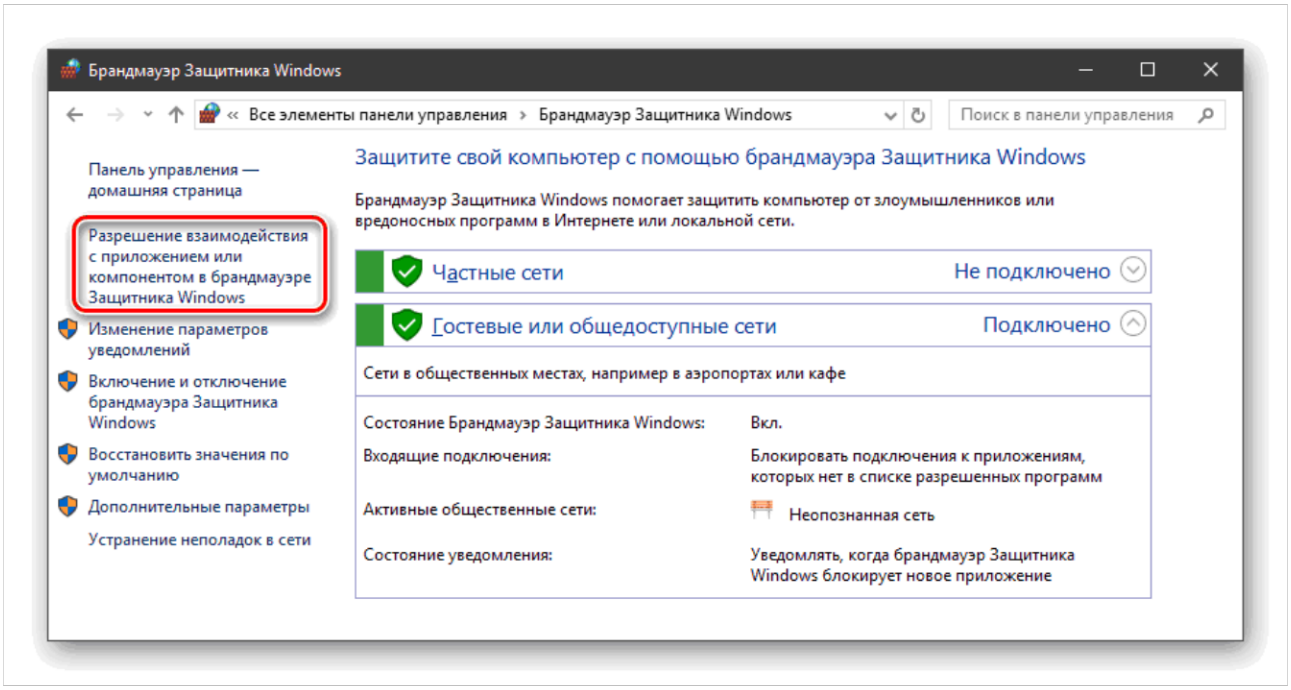


Скидання налаштувань зазвичай виконується при збоях в роботі брандмауера за різних причин, а також після невдалих експериментів з настройками безпеки. Слід розуміти, що «правильно налаштовані» опції також будуть скинуті, що може привести до непрацездатності додатків, які вимагають підключення до мережі:

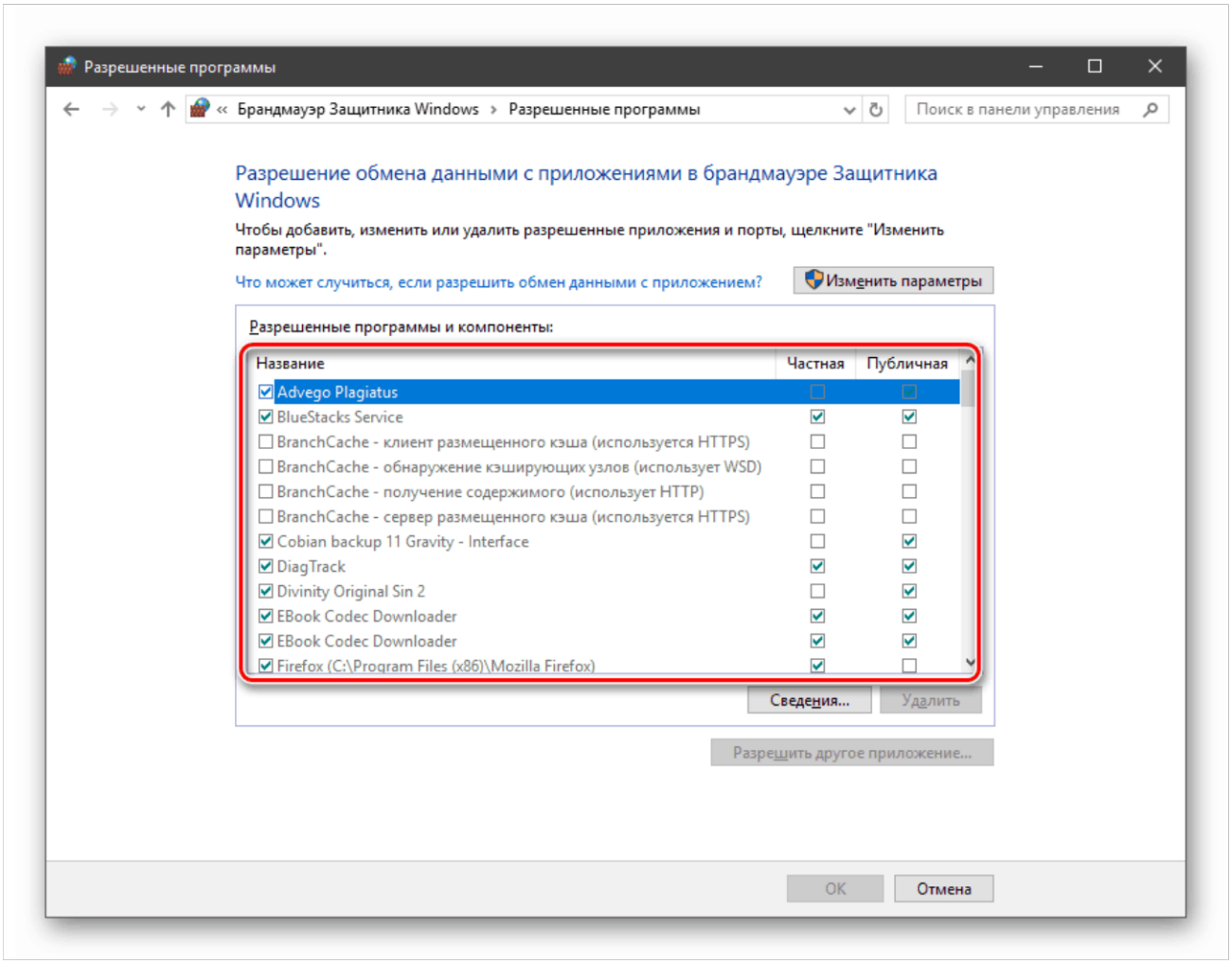


2.1.6. Взаємодія з програмами

Ця функція дозволяє налаштувати підключення до мережі для окремих програм:

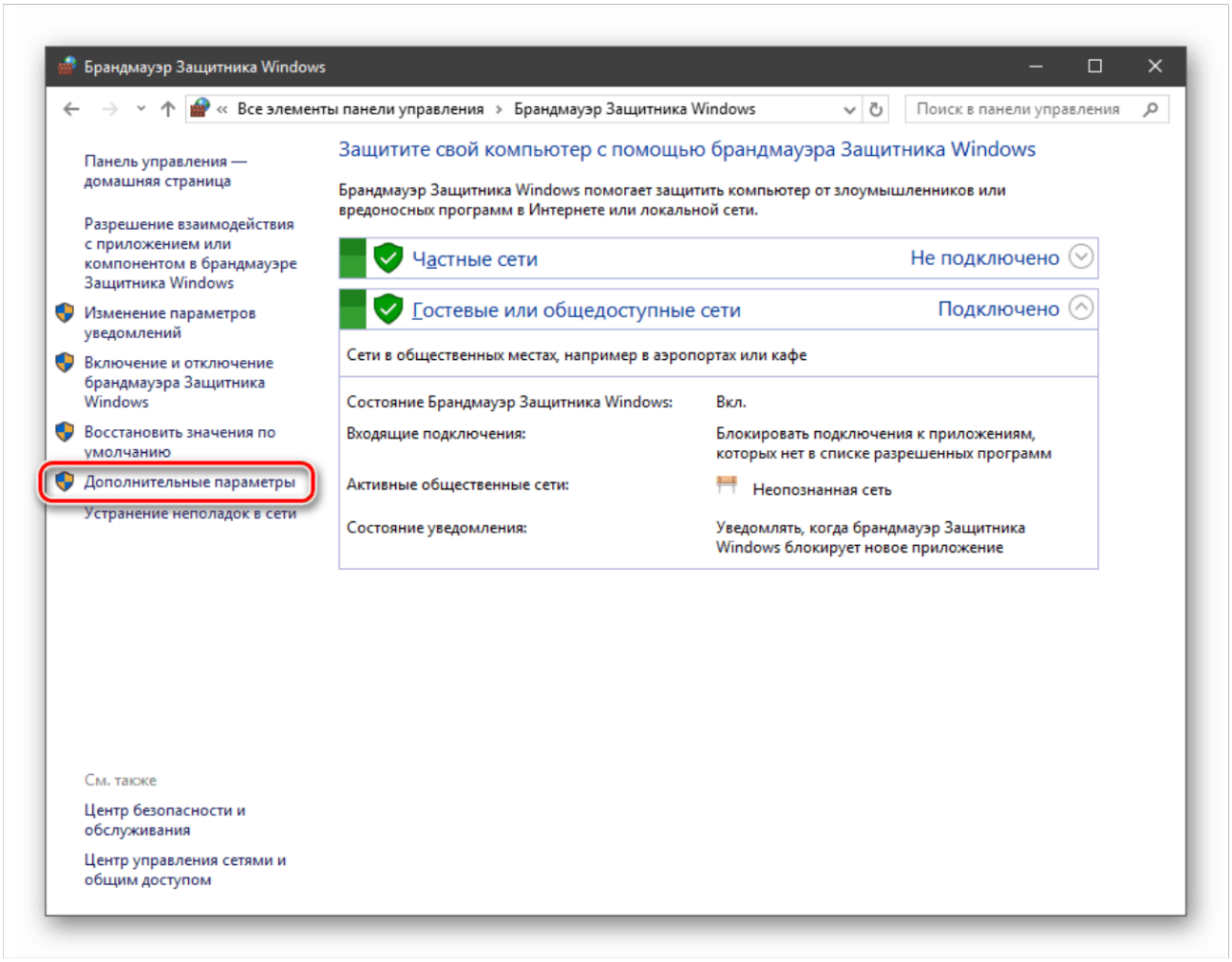


Відповідний перелік програм називають «винятками»:

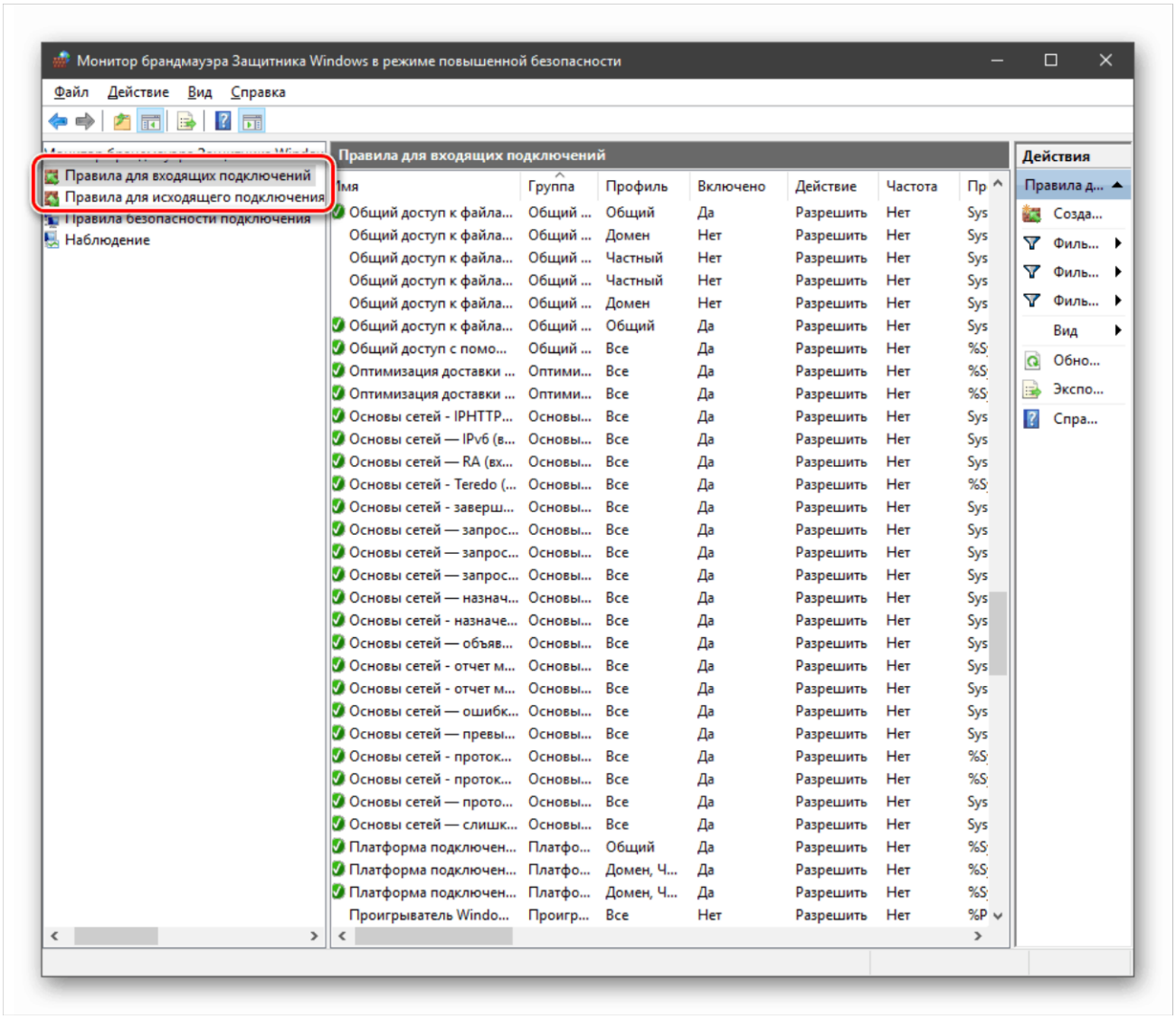


2.1.7. Правила

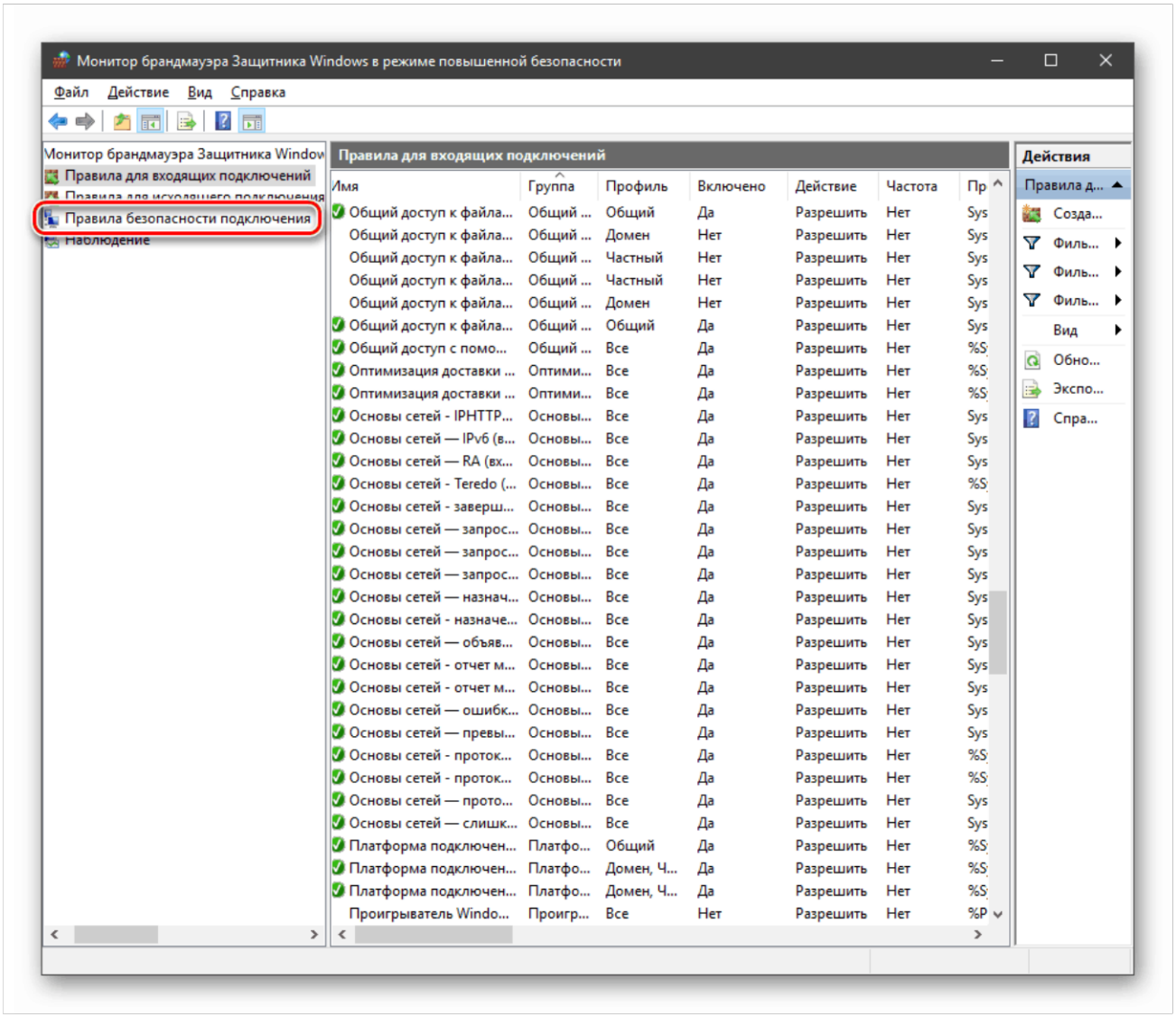
Правила – це основний інструмент брандмауера для керування безпекою. За допомогою правил можна забороняти або дозволяти мережеві підключення за певними ознаками. Цей функціонал налаштовується в розділі Додаткових параметрів:



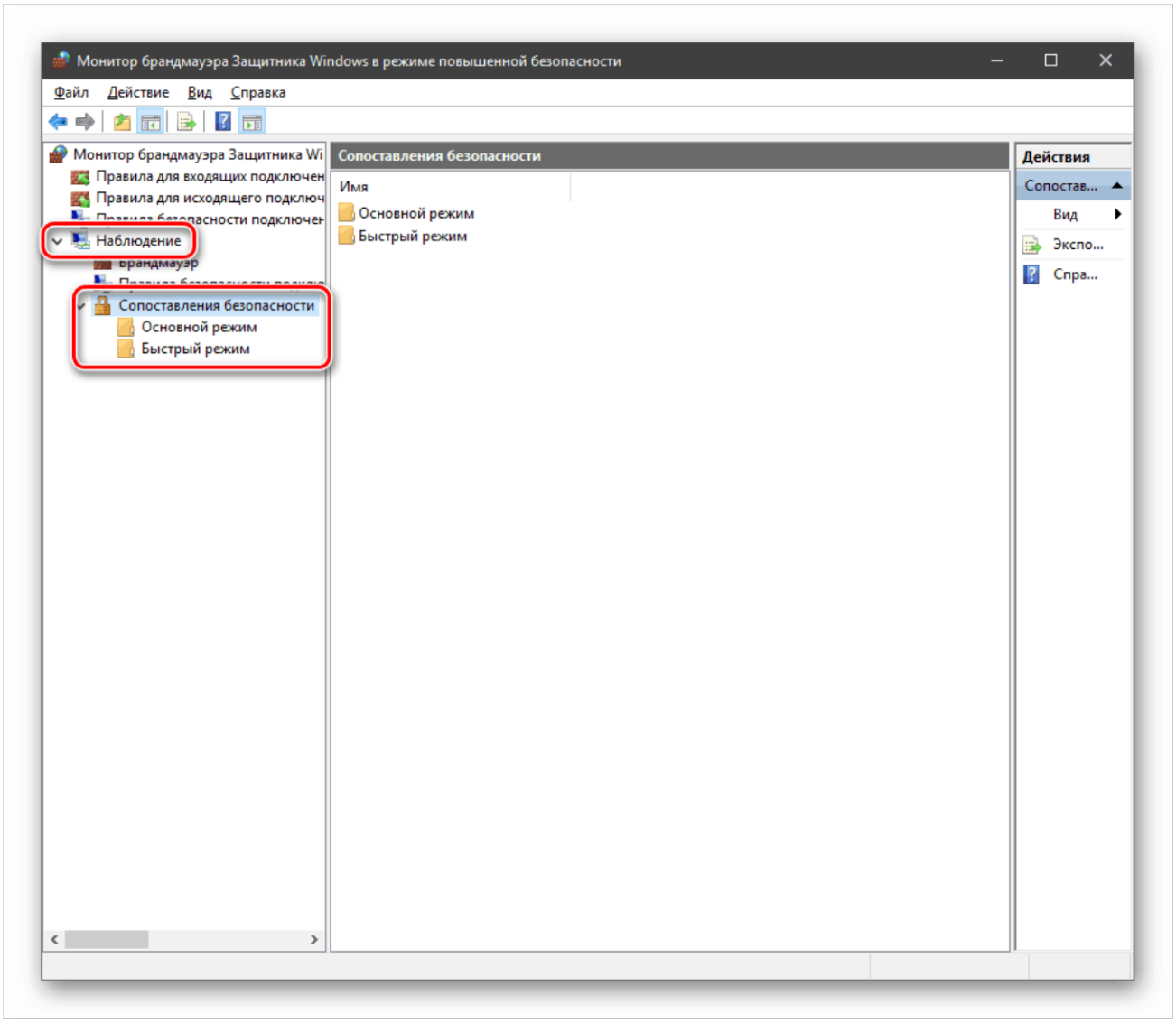
Вхідні правила містять умови для отримання даних ззовні, тобто потрапляння інформації з мережі всередину системи. Правила можна створювати для будь-яких програм, компонентів системи, протоколів або портів. Налаштування ***вихідних правил*** впливає на заборону або дозвіл відправки запитів на зовнішні сервери й контролюють процес видачі інформації назовні:



Правила безпеки під'єднання дозволяють здійснювати підключення з використанням набору спеціальних протоколів IPSec, згідно з якими проводиться автентифікація, отримання і перевірка цілісності отриманих даних та їх шифрування, а також захищена передача ключів через глобальну мережу:

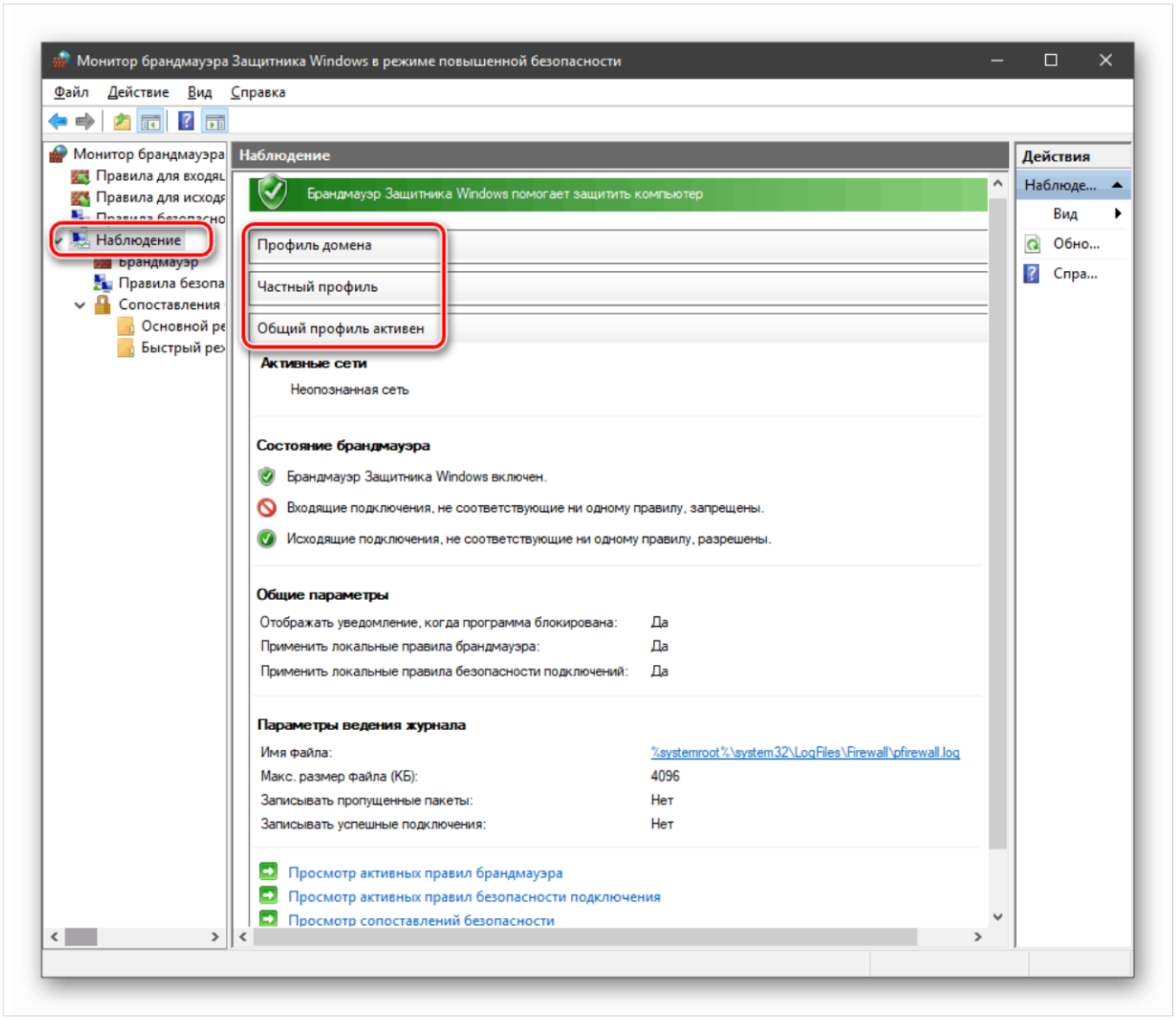


У гілці ***Спостереження***, в розділі ***зіставлення безпеки***, можна переглядати інформацію про підключення, для яких налаштовані правила безпеки:



2.1.8. Профілі

Профілі представляють собою набір параметрів для різних типів підключень. Існують профілі трьох типів (в порядку зростання «суворості», тобто рівня захисту): «Профіль домену», «Приватний» та «Загальний»:

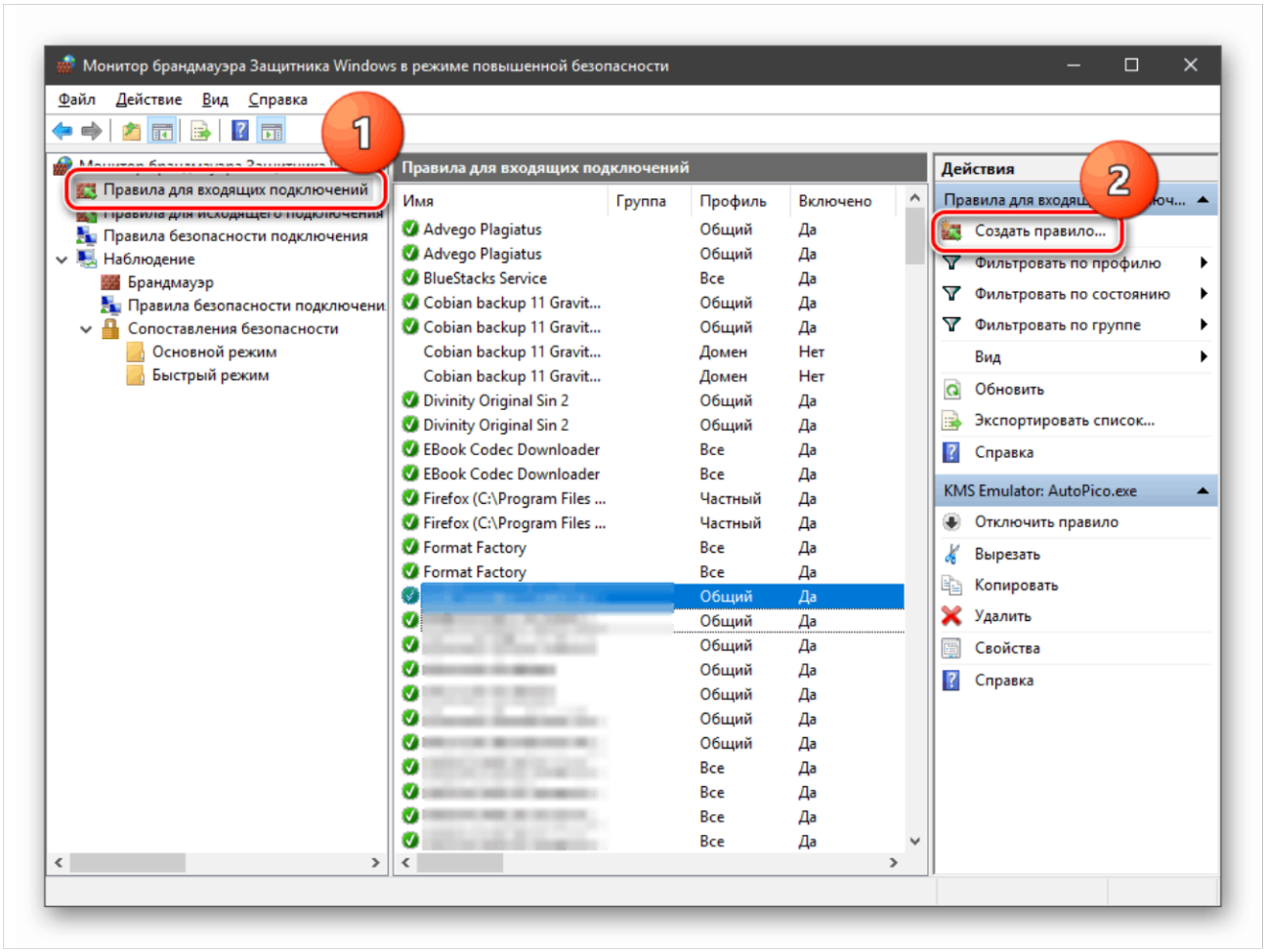


При звичайній роботі ці набори активуються автоматично при з'єднанні з певним типом мережі (обирається при створенні нового підключення або підключенні мережевого адаптера).

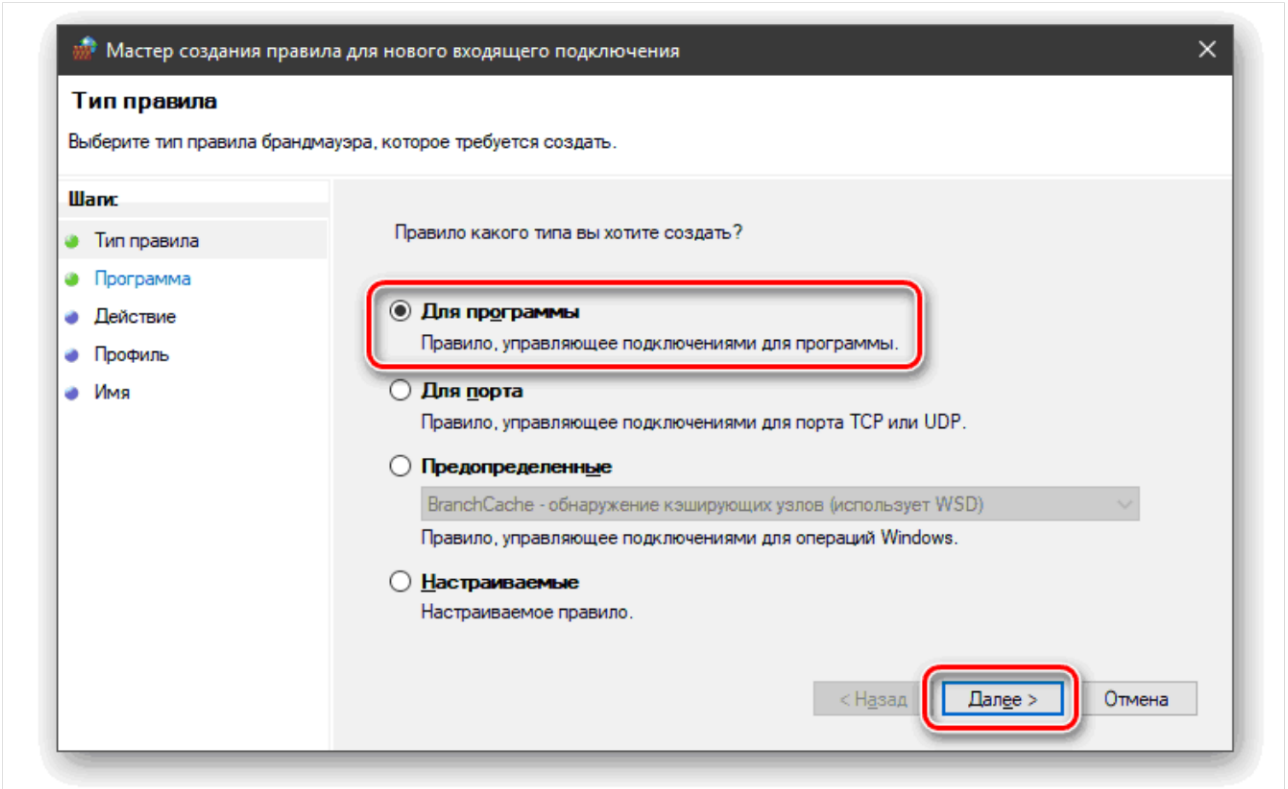
2.1.9. Створення правил для програм

Як згадувалося вище, правила бувають вхідні та вихідні. За допомогою перших налаштовуються умови отримання трафіку певними програмами, другі визначають, чи зможуть програми передавати дані в мережу.

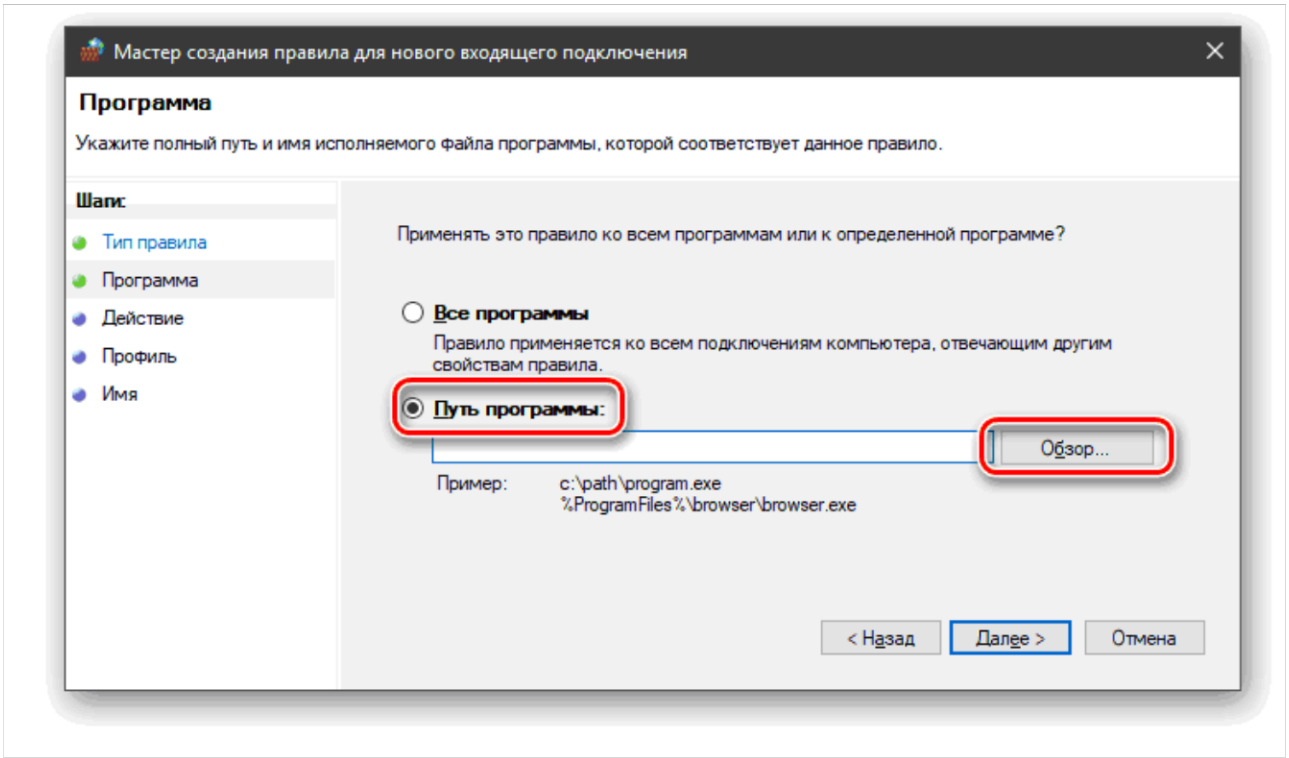
У вікні «Монітор брандмауера для Захисника Windows» (в розділі «Додаткові параметри») обираємо пункт «Правила для вхідних підключень» і на панелі праворуч обираємо «Створити правило»:



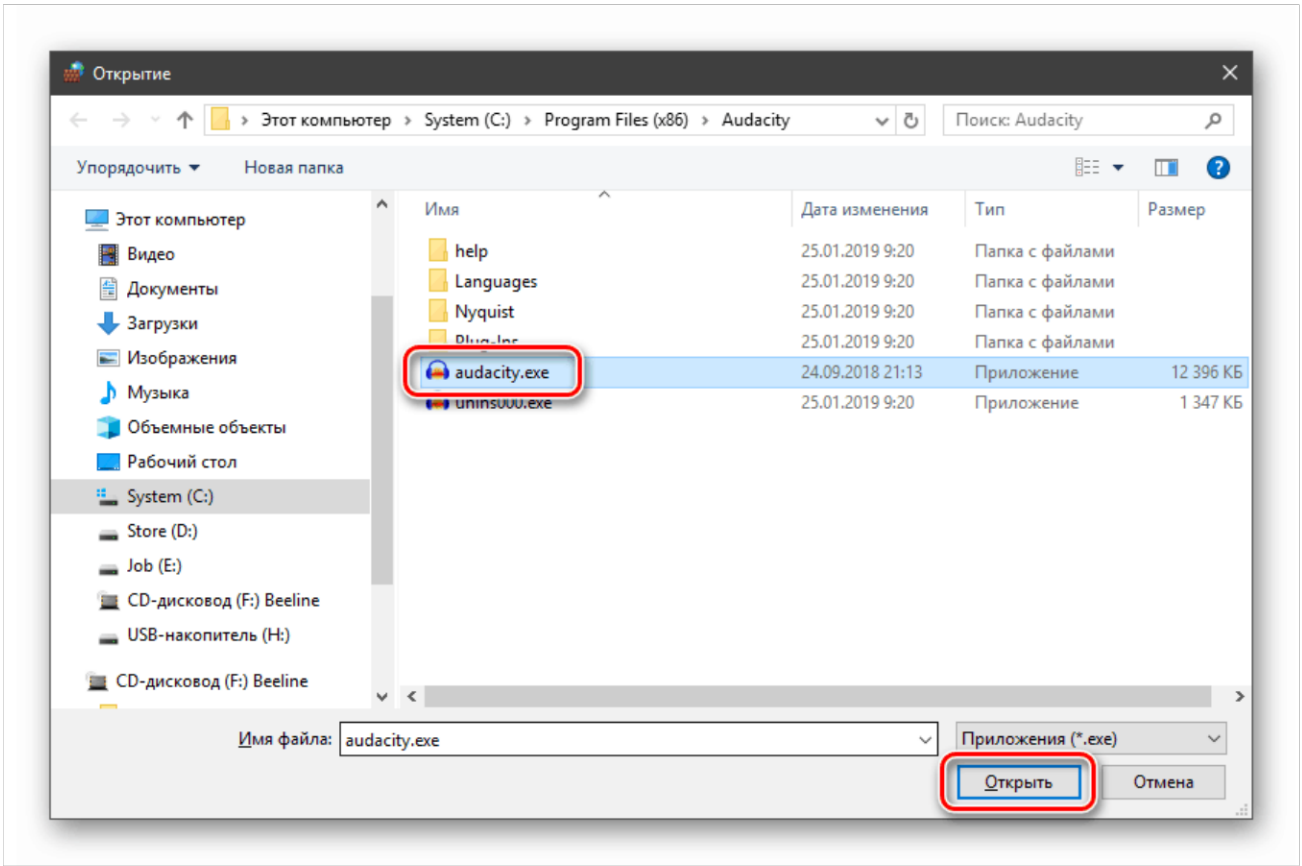
Обираємо опцію «Для програми» і тиснемо «Далі»:



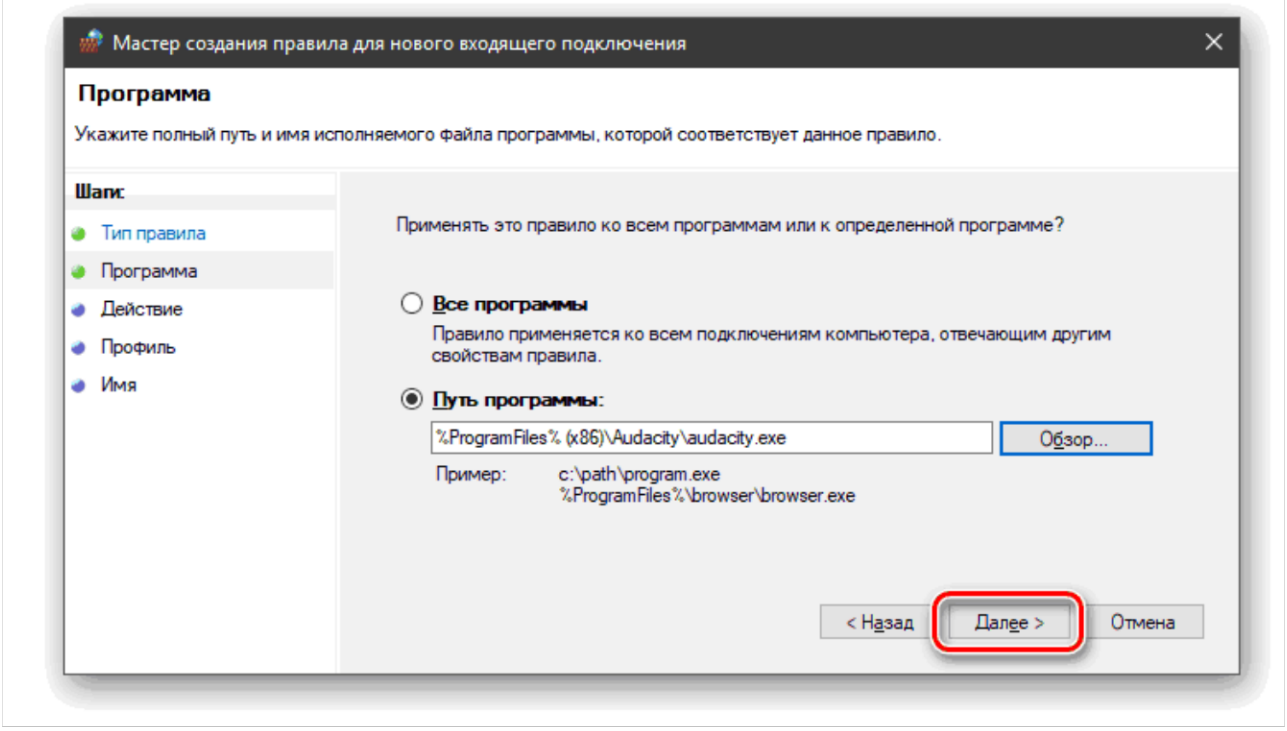
Перемикаємось на опцію «Шлях до програми» і тиснемо кнопку «Огляд»:



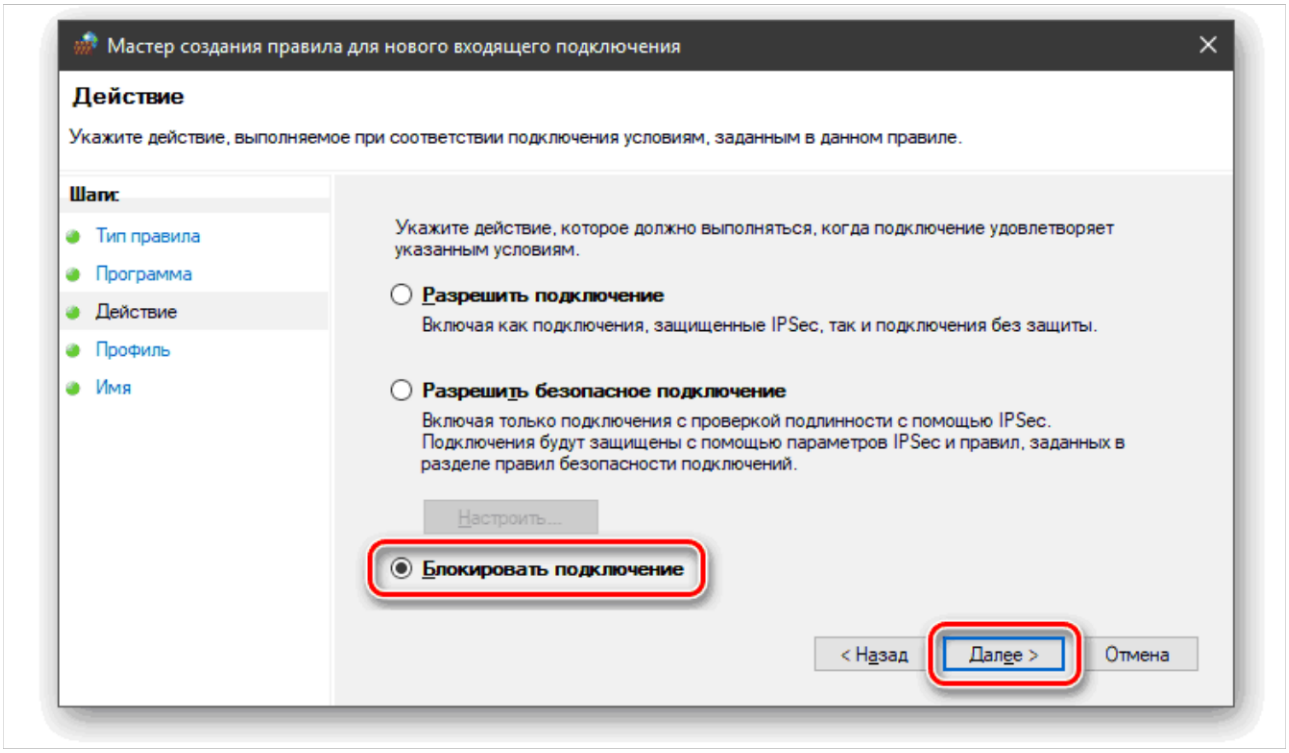
За допомогою «Провідника» шукаємо виконуваний файл питомої програми (в даному прикладі – ***audacity.exe***), клікаємо по ньому і натискаємо «Відкрити»:



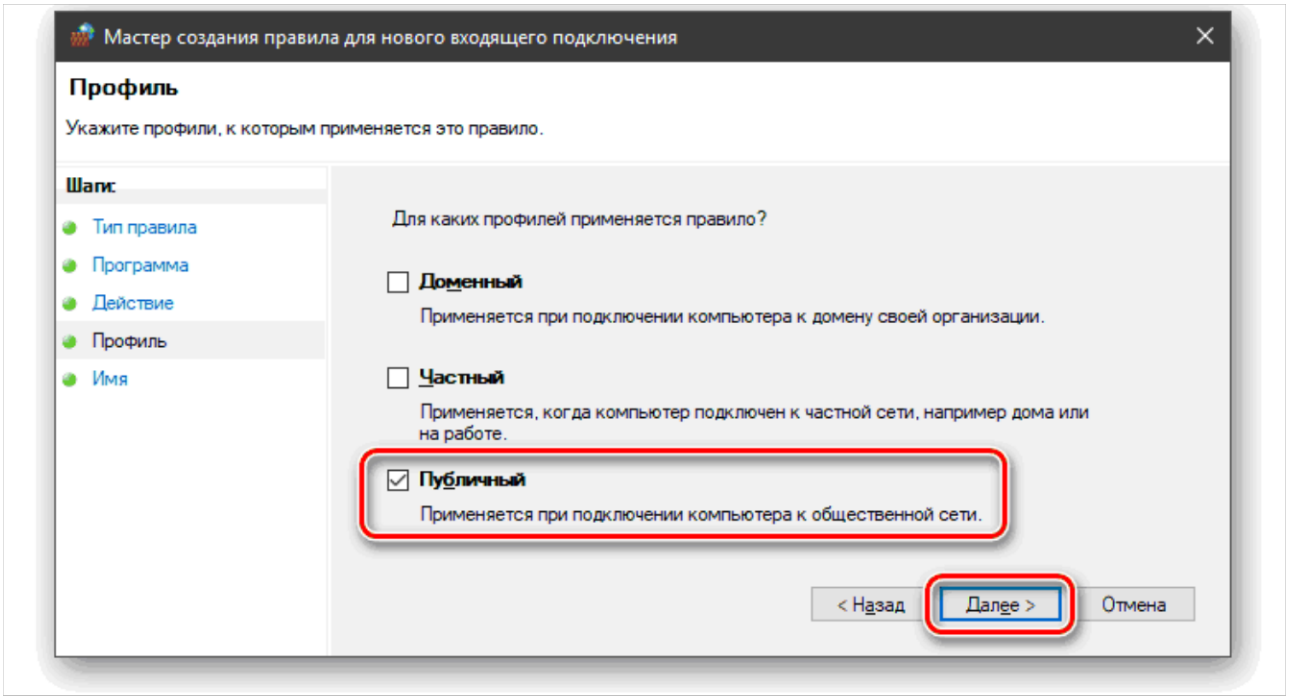
Йдемо далі:



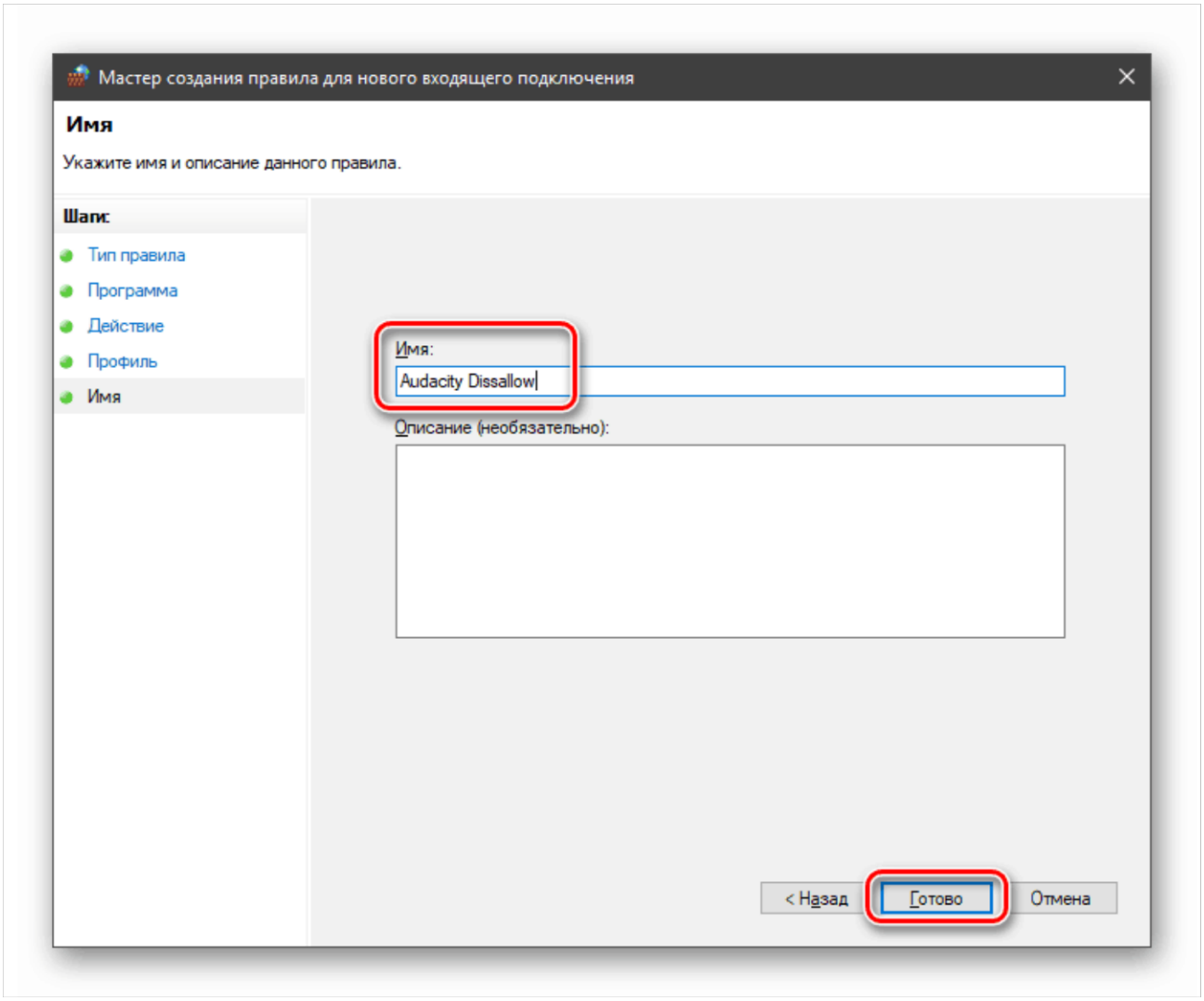
У наступному вікні бачимо варіанти дії. Тут можна або дозволити, або надати доступ через IPSec, або заборонити підключення. Виберемо третій пункт:



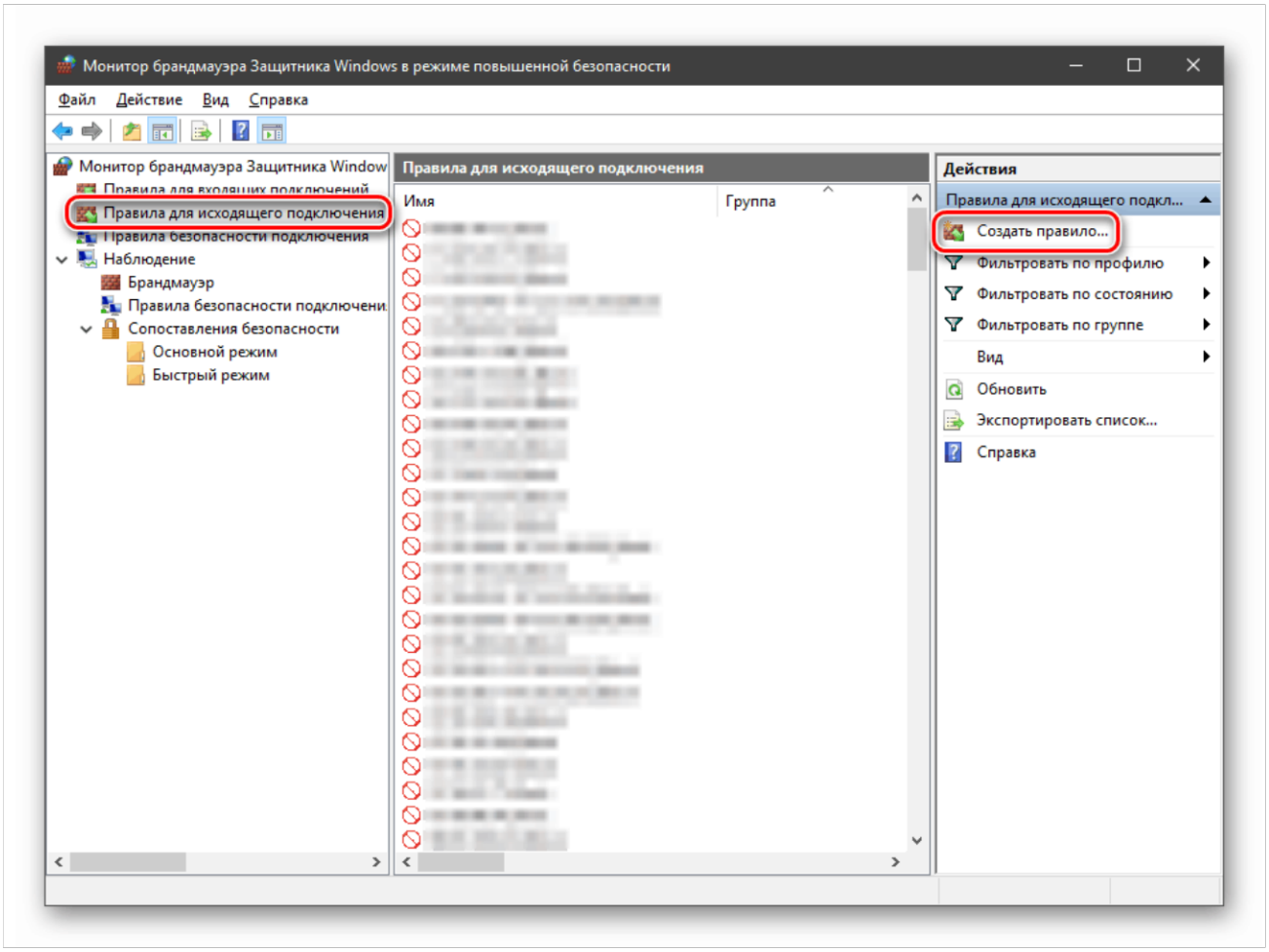
Визначаємо, для яких профілів буде працювати нове правило. Зробимо так, щоб програма не могла підключатися тільки до мереж спільного використання (безпосередньо до інтернету), а в домашньому оточенні працювала в штатному режимі:



Надаємо правилу ім'я, під яким воно буде відображатися в списку. За бажанням створюємо опис цього правила для кращого розуміння. Після натискання кнопки «Готово» правило буде створено і одразу застосовано:

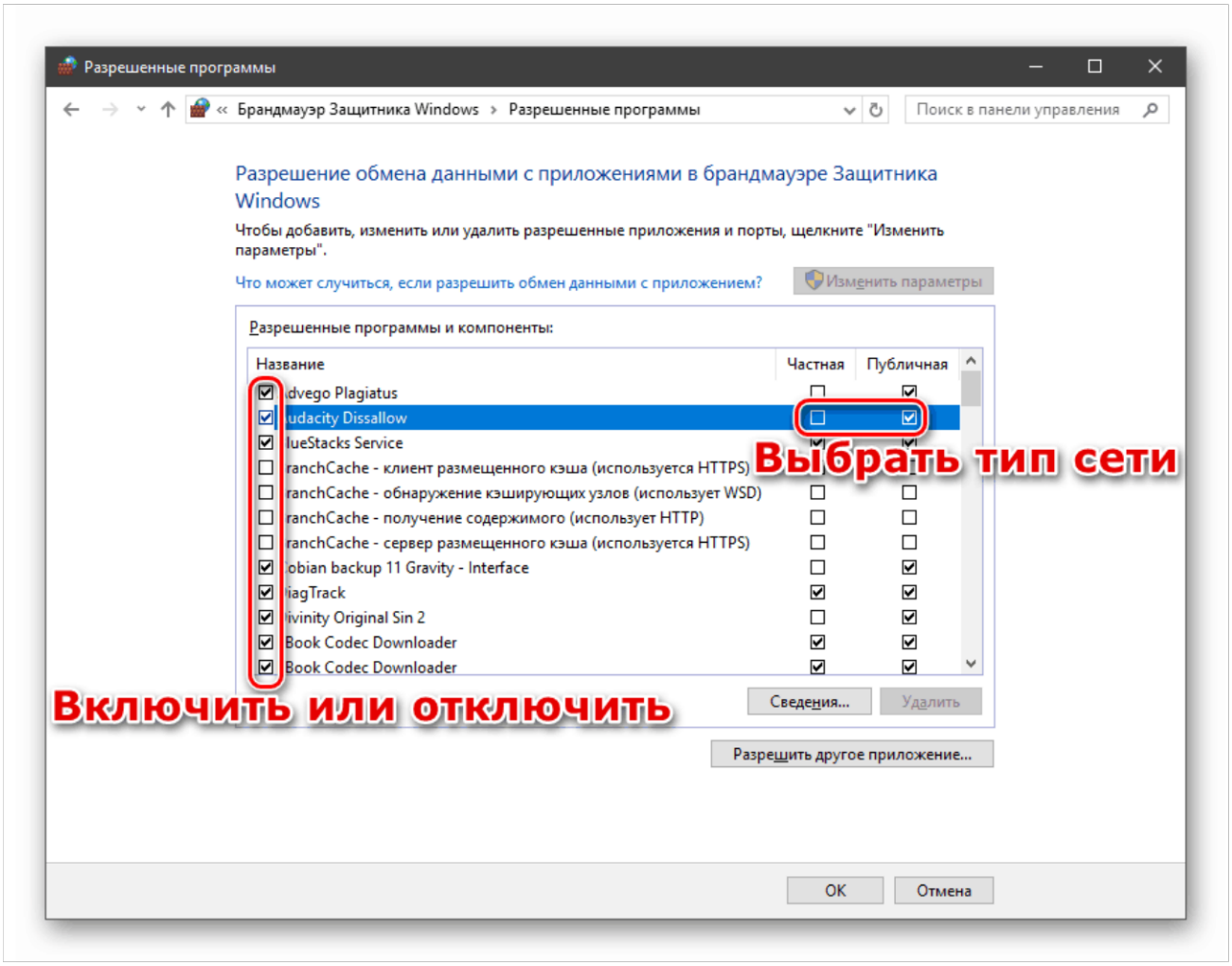


Вихідні правила створюються аналогічним чином на відповідній вкладці:



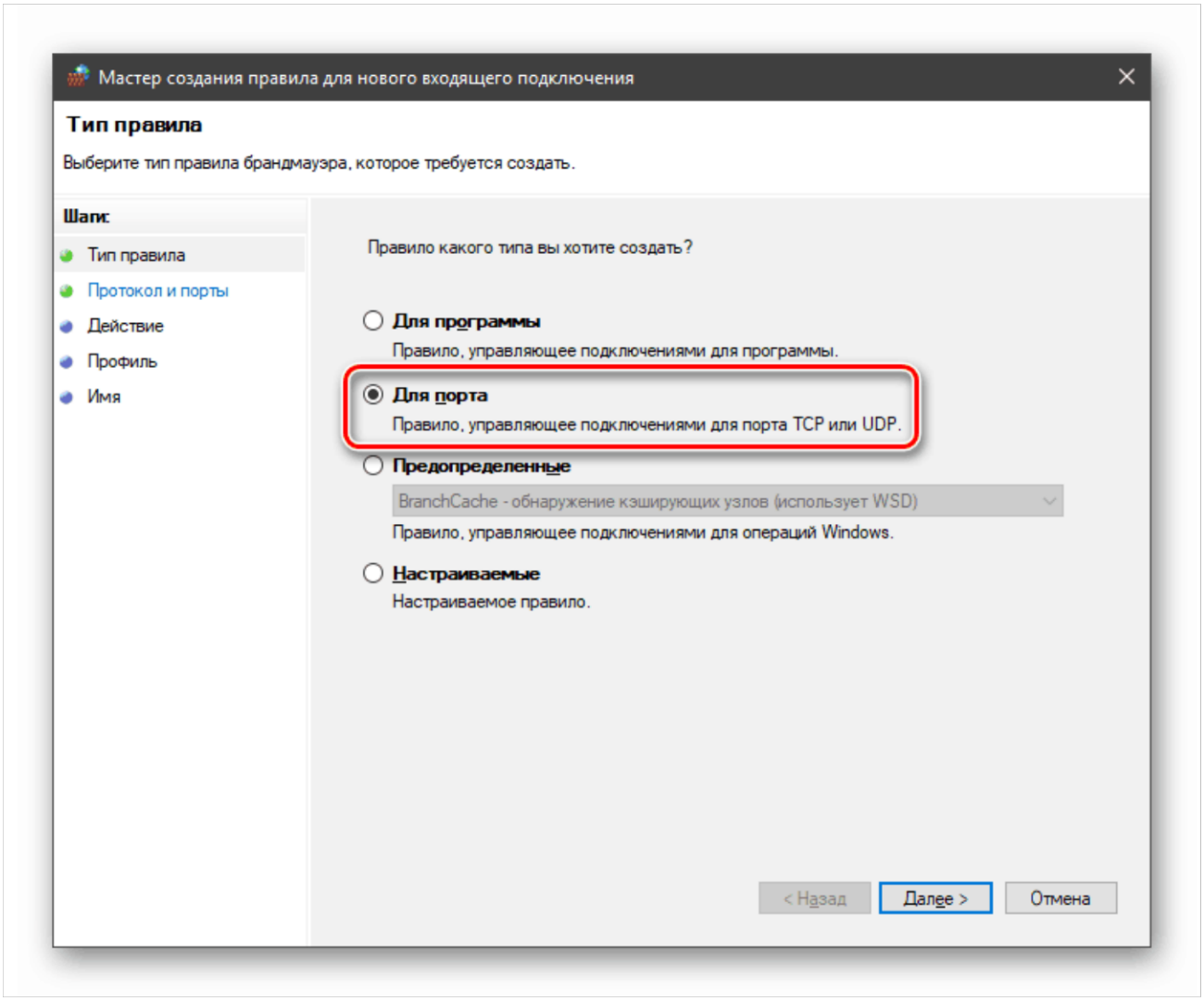
2.1.10. Робота з винятками

Додавання програми в перелік виключень брандмауера дозволяє швидко створити для неї дозволяюче правило. Також в цьому списку можна налаштувати деякі параметри – увімкнути або вимкнути позицію і вибрати тип мережі, в якій вона діє:



2.1.11. Правила для портів

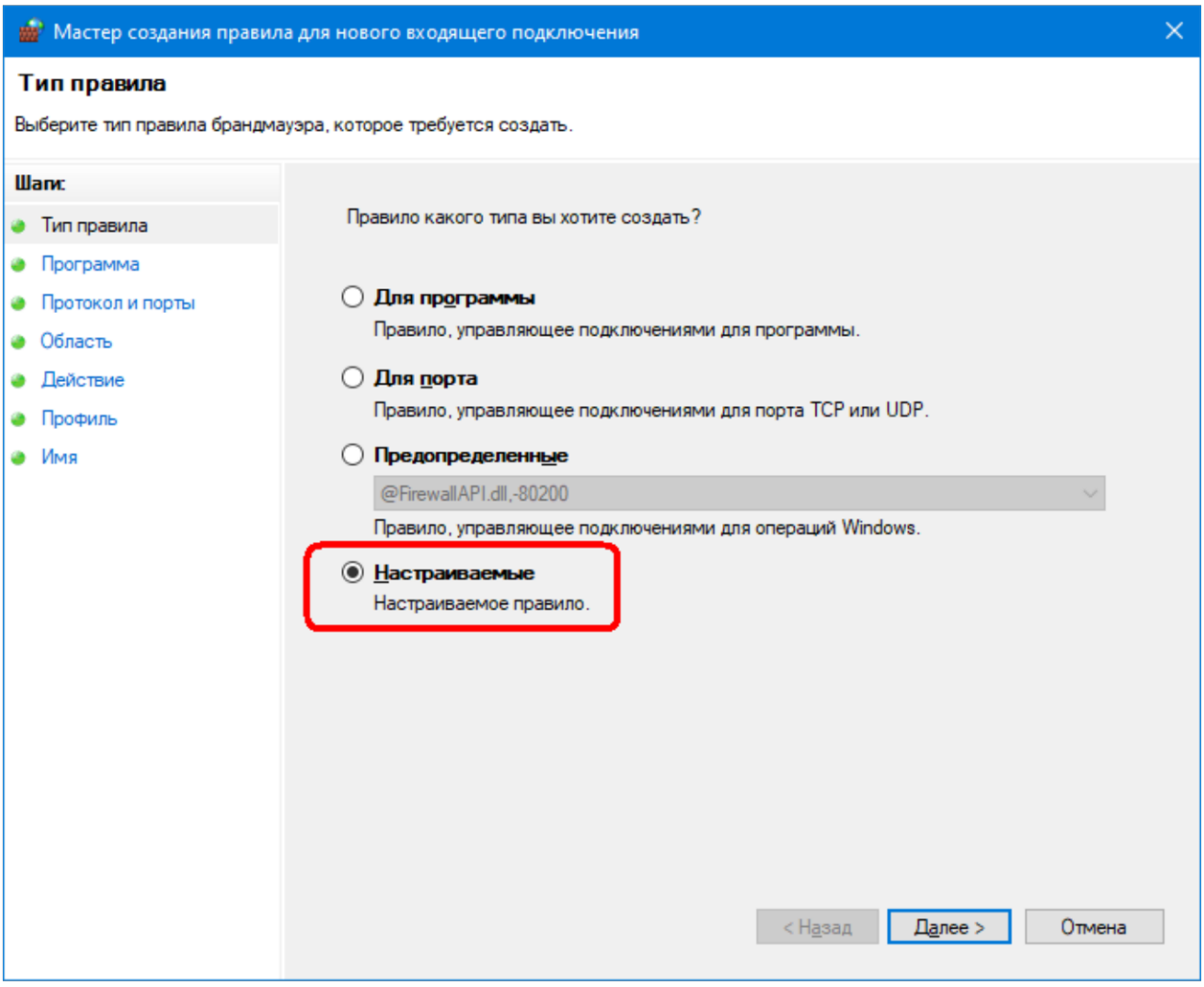
Такі правила створюються таким же чином, як правила для програм (вхідні та вихідні) за відмінністю, що на етапі визначення типу правила обирається пункт «Для порту»:



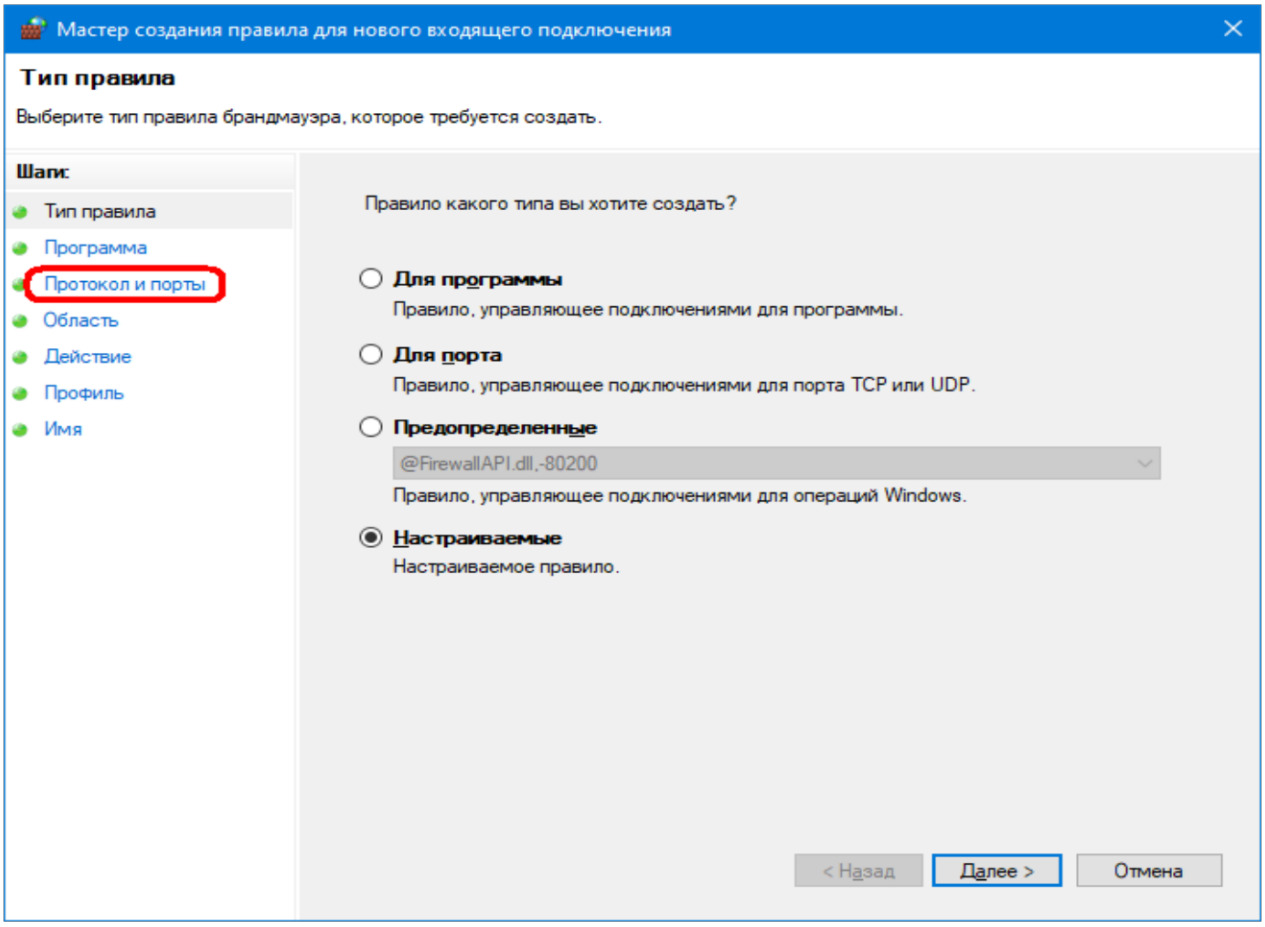
Типові варіанти застосування правил для портів – налаштування взаємодії з поштовими клієнтами, месенджерами або ігровими серверами.

2.1.12. Правила для протоколів

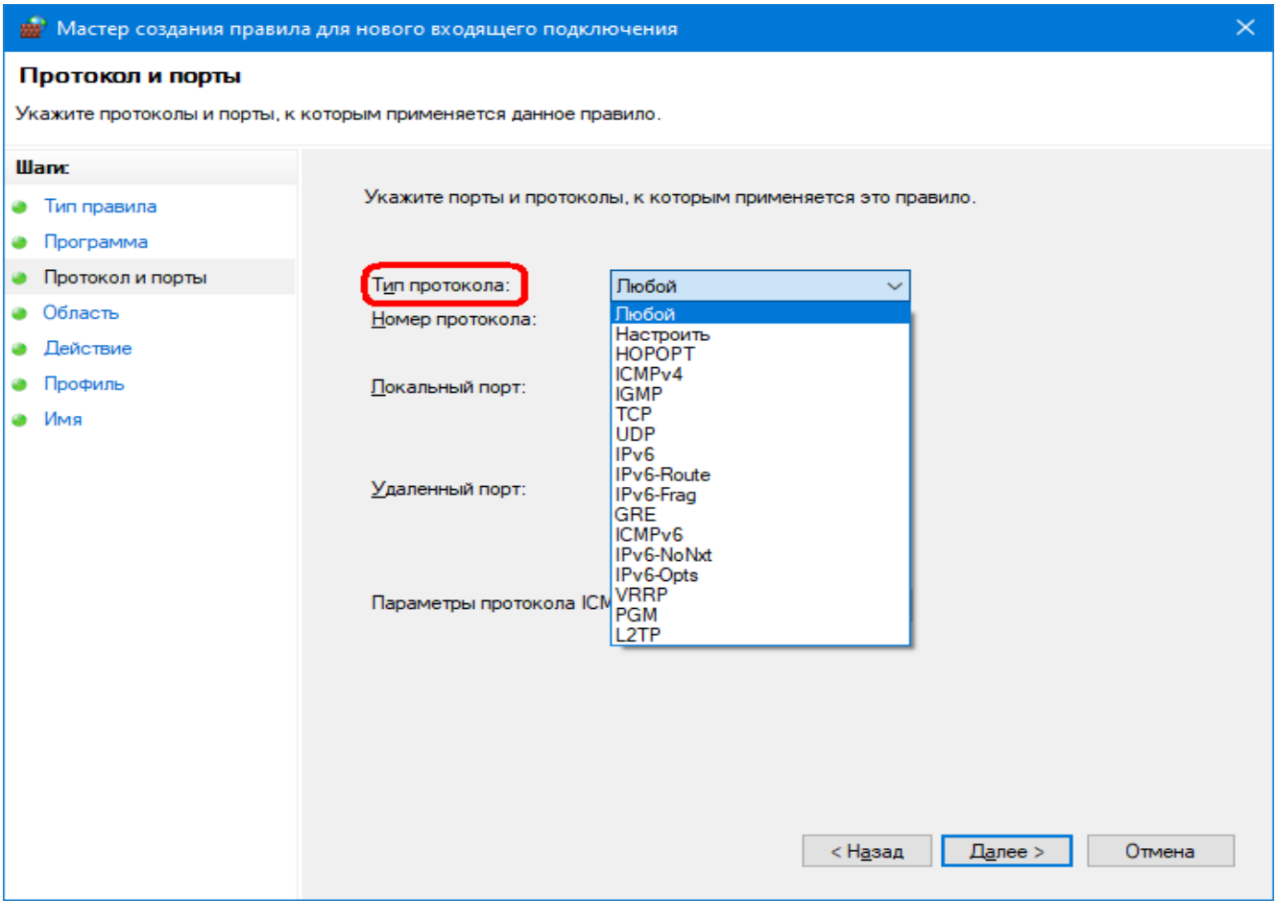
Такі правила є більш складними в створенні та налаштуванні. На етапі визначення типу правила обирається пункт «Налаштовувані»:



А потім – пункт «Протокол і порти»:



Після чого обирається тип протоколу:



Якщо вказано протокол рівня вище за мережевий, можливо також обрати потрібні порти / діапазони портів. У випадку обрання протоколу ICMP також доступні його окремі налаштування.

2.1.13. Прикінцеве зауваження

Під час налаштування брандмауера Windows слід пам'ятати, що зміни правил, встановлених в ньому за замовчуванням, як при роботі з будь-яким міжмережевим екраном можуть привести або до зниження рівня безпеки системи, або до порушення нормальної роботи деяких додатків і компонентів, функціонування яких пов’язане з доступом до мережі.

2.1.14. Службова утиліта Ping

2.1.14.1. **Призначення та принцип дії утиліти Ping.** Службова утиліта Ping призначена для перевірки з'єднань в TCP/IP- мережах. Вона відправляє запити (Echo-Request) зазначеному вузлу мережі й фіксує відповіді (Echo-Reply), використовуючи протокол ICMP. Вчасне не отримання відповіді означає відсутність з'єднання з зазначеним вузлом мережі. Недосяжність питомого вузла, яку здатна виявити утиліта Ping, може бути обумовлена непрацездатністю будь-якого компонента стеку протоколів TCP/IP на рівнях від фізичного до мережевого.

Повна відсутність ICMP-відповідей може також свідчити, що віддалений вузол (або якийсь із проміжних маршрутизаторів) блокує ICMP-відповіді або ігнорує ICMP- запити.

Утиліта Ping є одним з основних діагностичних засобів у мережах TCP/IP і входить до складу всіх сучасних мережевих операційних систем. Функціональність ping також реалізована в деяких вбудованих операційних системах маршрутизаторів та інших мережевих пристроїв.

2.1.14.2. **Параметри запуску утиліти Ping:**

Утиліта Ping може бути використана з наступними параметрами:

-t – відправка пакетів на вказаний вузол до команди переривання;

-a – встановлення адрес по іменах вузлів;

-n – число запитів, що відсилаються;

-l – розмір буферу відсилання;

-f – встановлення прапорця, що забороняє фрагментацію пакета;

-i – встановлення терміну життя пакету <"Time To Live">;

-v – встановлення типу служби <"Type Of Service">;

-r – запис маршруту для вказаного числа переходів;

-s – штамп часу для вказаного числа переходів;

-j – вільний вибір маршруту по списку вузлів;

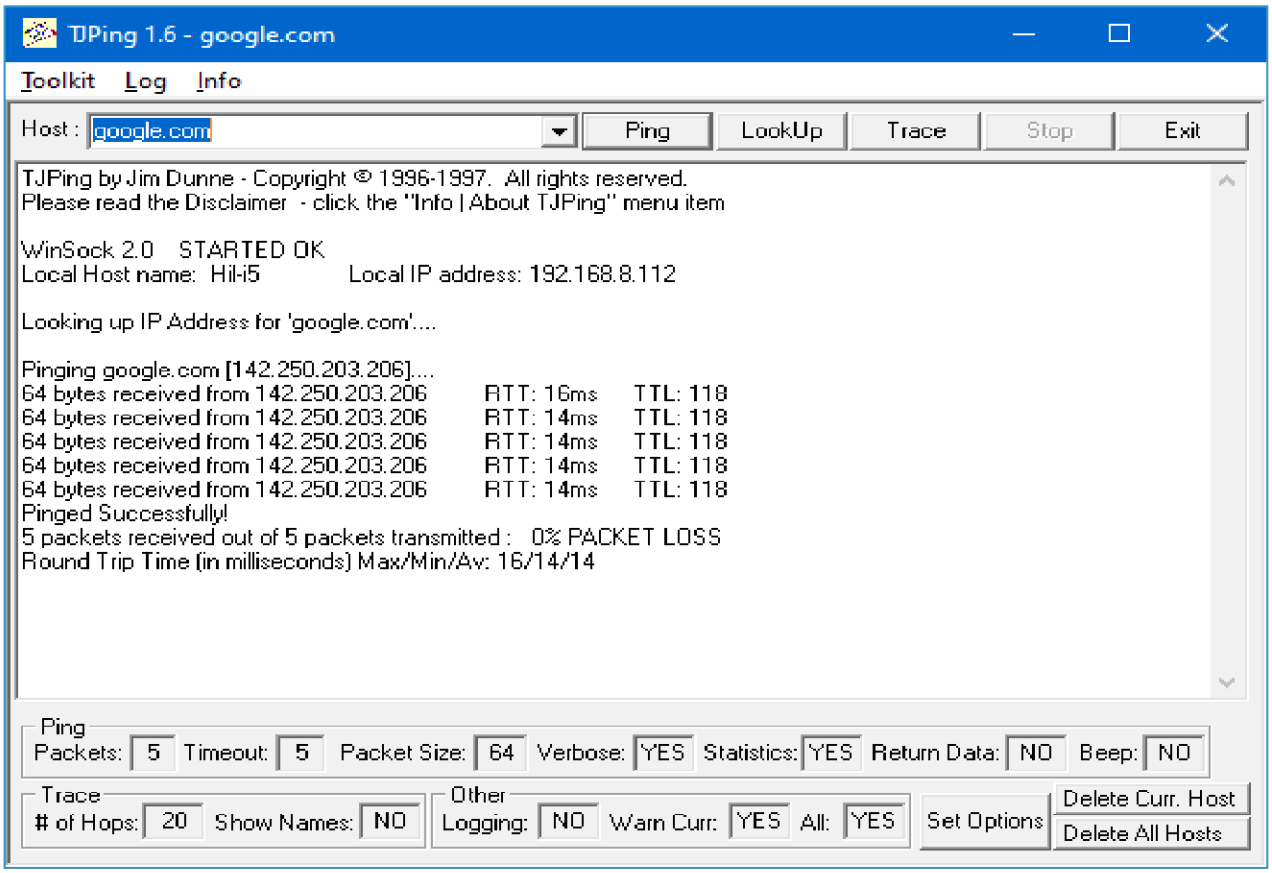
-k – жорсткий вибір маршруту по списку вузлів;

-w – таймаут кожної відповіді в мілісекундах;

-4 – примусове використання протоколу IPv4;

-6 – примусове використання протоколу IPv6.

2.1.14.3. **Утиліта TJPing з графічним інтерфейсом.** Дана безкоштовна утиліта є одним з не багатьох додатків, в якому команда ping виконується у звичному для користувачів ОС Windows оточенні:



Крім власне перевірки з’єднання з питомим вузлом мережі (режим Ping), заданим IP-адресою або доменним ім’ям, утиліта TJPing дозволяє:

- дізнатися IP-адресу по доменному імені (режим LookUp);
- виконати трасування з’єднання до питомого вузла (режим Trace);
- визначити, чи є на поточному комп'ютері проблеми з налаштуванням DNS (виконуючі команду ping спочатку для IP-адреси, а потім для відповідного доменного імені);
- приблизно оцінити якість каналу зв’язку (за кількістю втрачених пакетів або часом відклику).

2.2. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи та виконати наступне завдання.

2.2.1. Завдання

1. Завантажте програму TJPing.exe з папки завдань для лабораторних робіт (Teams ЗК / Файли / Документи / General / Навчальні матеріали / 2. Завдання для лабораторних робот / TJPing.exe) на свій комп’ютер, наприклад в папку "C:\TJPing\".

2. Для зручного використання створіть ярлик для цієї програми (для цього: клікніть додатковою (правою) кнопкою миши на поверхні робочого столу; у вікні, що відкрилося, оберіть пункти Створити/Ярлик; вкажіть розташування програми – C:\TJPing\TJping.exe; введіть ім’я для ярлика (наприклад, TJPing); натисніть "Готово").

3. Запустіть програму TJPing.exe.

4. У полі "Host:" введіть ім'я веб-сайту за своїм варіантом (табл. 2.1).

5. Натисніть кнопку "Ping", переконайтеся, що команда перевірки з’єднання виконалася вдало (від питомого хоста надійшло всі 5 відкликів на надіслані 5 запитів).

6. За допомогою Брандмауера Windows спробуйте перешкодити нормальній роботі програми TJPing кожним з наступних чотирьох способів:

6.1. Шляхом повного блокування доступу в Інтернет для всього комп’ютера (див. підпункт 2.1.4.2);

6.2. Шляхом створення правила для програми (див. пункт 2.1.10);

6.3. Шляхом створення правила для порту (див. пункт 2.1.11);

6.4. Шляхом створення правила для протоколу (див. пункт 2.1.12).

Таблиця 2.1 – Варіанти завдань до Лабораторної роботи 2

№ з/п	Ім'я веб-сайту
1.	www.ukr.net
2.	www.i.ua
3.	www.mon.gov.ua
4.	www.nas.gov.ua
5.	www.ipme.kiev.ua
6.	www.donntu.edu.ua
7.	www.nau.edu.ua
8.	www.knu.ua
9.	www.kpi.kharkov.ua
10.	www.lntu.edu.ua

7. Для кожного з пунктів 6.1-6.4 практичної частини запишіть свої дії у вигляді повного переліку обраних пунктів вікон / полів / кнопок (наприклад: "*Панель управління / Брандмауер для захисника Windows / Додаткові параметри / Правила для вхідних підключень / Створити правило / Налаштоване / Протокол і порти / Тип протоколу: ICMPv4 / Далі / Локальні IP-адреси: Довільна IP-адреса / Віддалені IP-адреси: Довільна IP-адреса / Далі /* ...") та опишіть результат, якого вдалося здобути.

2.3. Питання до самоконтролю

1. В яких версіях ОС Windows є вбудованим брандмауер Windows?

2. Для мереж якого типу потрібно встановлювати більш суворі правила захисту – приватних чи спільного використання? Чому?

3. Для випадку, коли в результаті невдалого налаштування брандмауера Windows якась з програм непередбачувано втратила доступ до мережі Інтернет, який існує механізм швидко усунути проблему саме для цієї програми?

4. Чи є принципово неможливим виконання якогось з пунктів 6.1-6.4 практичної частини лабораторної роботи? Чому?

2.4. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

2.5. Література до Лабораторної роботи 2

Рекомендовані літературні джерела до виконання Лабораторної роботи 2: [1, 2, 4-6].

ЛАБОРАТОРНА РОБОТА 3. СЕГМЕНТАЦІЯ МЕРЕЖІ (VLAN)

Мета роботи: набуття навичок побудови, налаштування та моніторингу віртуальних локальних мереж.

3.1. Теоретичний матеріал до лабораторної роботи

3.1.1. Потреба у віртуальних локальних мережах

Для підвищення захищеності локальної комп'ютерної мережі та зменшення впливу на її продуктивність широкомовних кадрів (комутаторами канального рівня) використовують механізм організації так званих віртуальних локальних мереж (Virtual Local Area Network – VLAN).

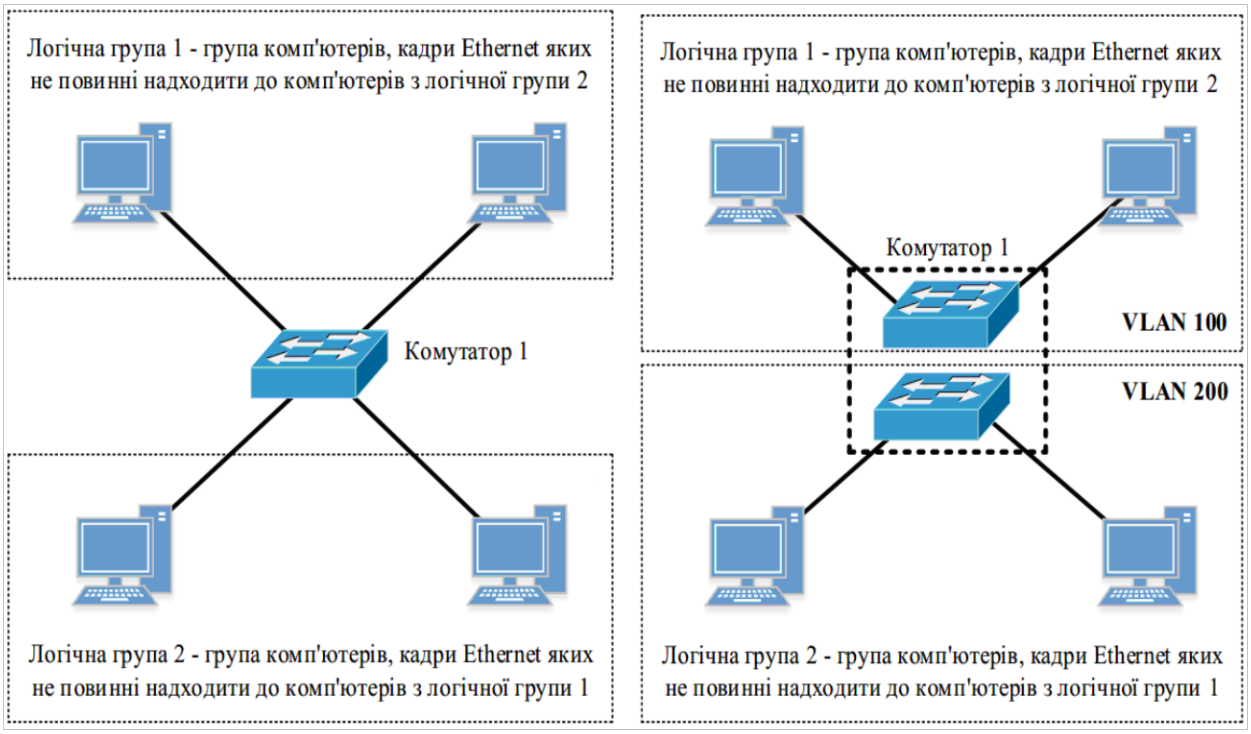
Застосування віртуальних локальних мереж надає можливість за рахунок відповідного конфігурування комутаторів розділити на канальному рівні фізично єдину локальну мережу на кілька логічно незалежних сегментів. Такі сегменти потім можуть бути об'єднані в складну мережеву ієрархію шляхом використання маршрутизаторів вже на мережевому рівні. Програмний спосіб керування процесом розділенням мережі на віртуальні локальних мережі суттєво зніжує трудомісткість реорганізації структури такої мережевої ієрархії, якщо виникне потреба внести зміни в цю структуру.

3.1.2. Принципи логічної сегментації мережі Ethernet на основі VLAN

3.1.2.1. Властивості віртуальних локальних мереж

Віртуальною локальною мережею VLAN будемо називати логічну групу вузлів мережі, кадри яких, у тому числі й широкомовні, на канальному рівні повністю ізольовані від інших вузлів мережі, що не входять до даної групи. Із цього випливає, що передача кадрів між різними VLAN на підставі MAC-адреси неможлива незалежно від типу адреси (одиночної, групової або широкомовної). У той же час усередині VLAN кадри передаються відповідно до технології канального рівня. Тому така логічна сегментація дозволяє логічну

структуру мережі Ethernet зробити незалежною від її фізичної структури (рис. 3.1).



а) б)

Рисунок 3.1 – Приклад сегментації мережі з використанням VLAN: а) фізична структура мережі; б) логічна структура мережі (один фізичний комутатор поділяється на два окремі умовні комутатори, які знаходяться у різних VLAN)

Треба також відмітити, що вузли, які належать до однієї логічної групи можуть бути фізично приєднані до різних комутаторів.

Таким чином, застосування VLAN призводить до обмеження розповсюдження широкомовних кадрів, а також кадрів, які розсилає комутатор по всіх своїх портах у випадку відсутності MAC-адреси отримувача кадру в його MAC-таблиці, тільки в межах однієї VLAN. Це в свою чергу дає можливість зменшити частку широкомовних кадрів у мережі й імовірність виникнення широкомовних штормів, що можуть суттєво погіршити характеристики продуктивності мережі.

Застосування VLAN забезпечує можливість гнучкого розділення користувачів на ізольовані групи, тобто кінцеві вузли користувачів (наприклад,

персональні комп’ютери) будуть ізольовані один від одного на канальному рівні. Також VLAN дозволяє покращити характеристики безпеки мережі за рахунок обмеження області розповсюдження кадрів другого рівня і реалізації необхідної політики взаємодії користувачів з різних VLAN за допомогою обладнання комутації третього рівня. Крім того, VLAN надає можливість спрямування за необхідними трактами передачі у випадку, якщо їх декілька, кадрів другого рівня, що дозволяє встановити необхідний розподіл потоків кадрів у певному сегменті мережі.

3.1.2.2. **Віртуальні локальні мережі на основі портів.** При використанні VLAN на основі портів кожен порт призначається у певну VLAN. Це означає, що всі користувачі, приєднані до цього порту, будуть членами однієї VLAN. Конфігурація портів статична й може бути змінена тільки вручну (рис. 3.2).

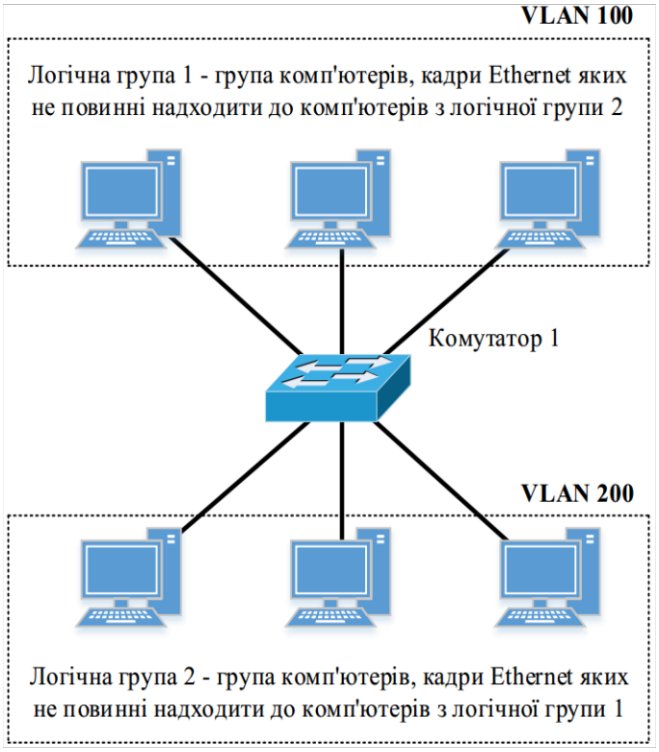


Рисунок 3.2 – VLAN на основі портів

Якщо вузли якої-небудь віртуальної мережі приєднані до різних комутаторів, то для з'єднання комутаторів між собою для кожної VLAN має бути виділено по одному порту (рис. 3.3).

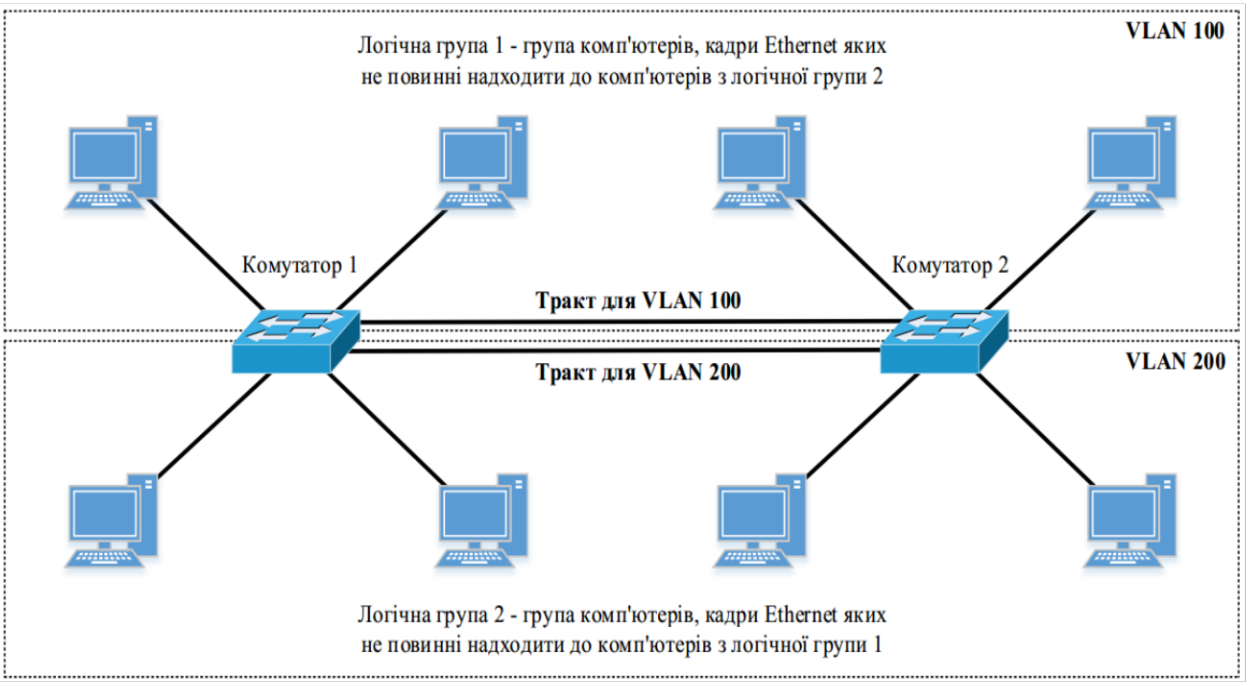


Рисунок 3.3 – VLAN на основі портів у мережі з декількома комутаторами

Передача інформації між користувачами з різних віртуальних мереж можлива тільки через мережевий рівень (на канальному рівні віртуальні мережі повністю незалежні). Для цього один з портів, що належить кожній VLAN, приєднується до окремого порту маршрутизатора, який забезпечує пересилання IP-пакетів між користувачами, що перебувають у різних віртуальних мережах (рис. 3.4). При цьому слід зазначити, що IP-адреси користувачів з різних віртуальних мереж повинні знаходиться урізних IP-мережах (підмережах), тобто префікси IP-мереж мають відрізнятися (це необхідно для того, щоб порти маршрутизатора перебували в різних IP-мережах).

Таким чином, спосіб утворення VLAN на основі портів у мережі з декількома комутаторами, а також при забезпечення можливості обміну інформацією між користувачами, що перебувають у різних віртуальних мережах, вимагає для своєї реалізації додаткового виділення такої кількості портів, скільки віртуальних мереж підтримується. Це є істотним недоліком даного способу при великій кількості віртуальних мереж.

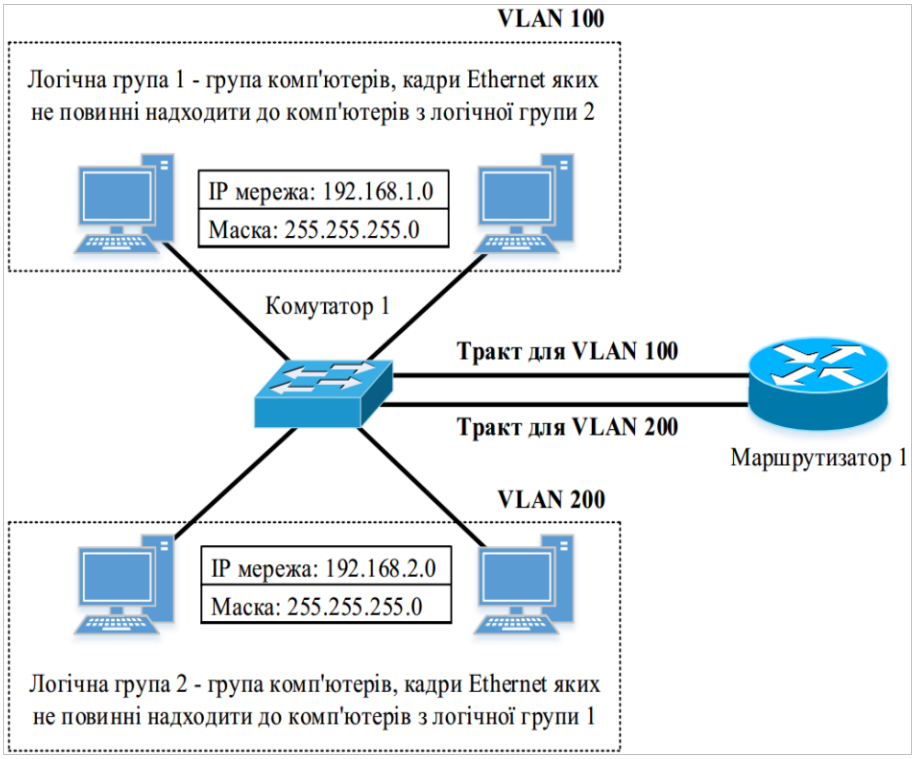


Рисунок 3.4 – Приклад організації можливості обміну інформацією між користувачами з різних VLAN на основі портів (IP-адреси користувачів з різних віртуальних мереж повинні знаходитись у різних IP-мережах)

3.1.2.3. **Віртуальні локальні мережі на основі стандарту IEEE 802.1Q**. Побудова VLAN на основі портів заснована тільки на додаванні додаткової інформації до таблиці комутації комутатора й не використовує можливості вбудовування інформації про приналежність до віртуальної мережі в кадри, що передаються.

Спосіб організації VLAN основі стандарту IEEE 802.1Q передбачає розміщення всередині кадру Ethernet додаткового службового поля розміром 4 байти, що дозволяє передавати таку інформацію (рис. 3.5):

1) Tag Protocol Identifier (TPID) − ідентифікатор протоколу розміром 16 біт − 0x8100, який відповідає стандарту 802.1Q, що вказує на використання у кадрі другого рівня цього стандарту;

2) Tag Control Information (TCI) – поле керування розміром 16 біт, що містить в собі такі поля:

– Priority – пріоритет кадру розміром 3 біти відповідно до стандарту IEEE 802.1p;

– Canonical Format Indicator (CFI) – індикатор канонічного формату розміром 1 біт, який вказує на формат MAC-адреси (0 – канонічний, 1 – неканонічний), що забезпечує сумісність між мережами Ethernet та Token Ring;

– VLAN Identifier (VID або VLAN ID) – ідентифікатор VLAN розміром 12 біт (діапазон можливих значень ідентифікатора в десятковому форматі становить від 0 до 4095, що надає можливість утворення 4095 віртуальних мереж).

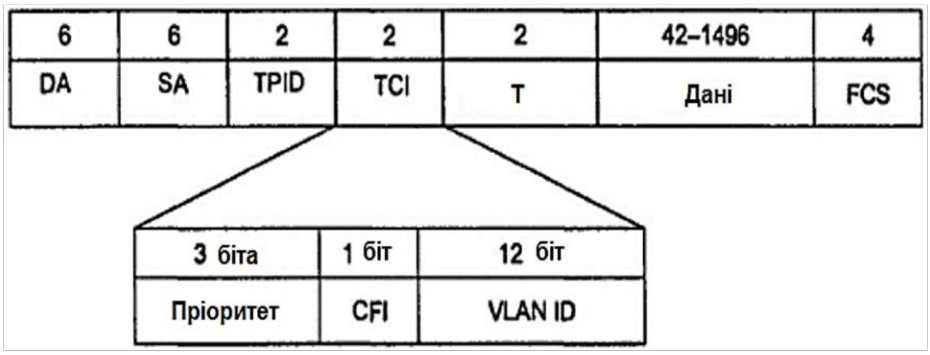


Рисунок 3.5 – Структура мережевого кадру Ethernet відповідно до стандарту 802.1Q

Відмітимо, що мінімальний та максимальний розміри поля даних кадру Ethernet зменшується на величину службових полів стандарту 802.1Q, тобто на 4 байти, а контрольна сума FCS обчислюється знову з урахуванням цих полів.

Порти комутаторів, які використовуються для організації VLAN на основі стандарту 802.1Q, мають тип Trunk (tagged, маркований порт). Ці порти можуть передавати кадри Ethernet, які містять службове поле відповідно до стандарту IEEE 802.1Q, від декількох VLAN, що дозволяє здійснювати з'єднання комутаторів мережі тільки одним трактом передачі (рис. 3.6), на відміну від VLAN на основі портів.

Для роботи комутатора з обладнанням, що є несумісним з стандартом IEEE 802.1Q, передбачаються порти типу Access (untagged, немарковані порти). З рис. 3.6 видно, що порти комутаторів, до яких приєднані персональні

комп’ютери (тут вважається, що мережеві адаптери комп’ютерів не мають підтримки стандарту IEEE 802.1Q), мають тип Access. Відмітимо, що порти типу Access можуть бути використані для організації VLAN на основі портів.

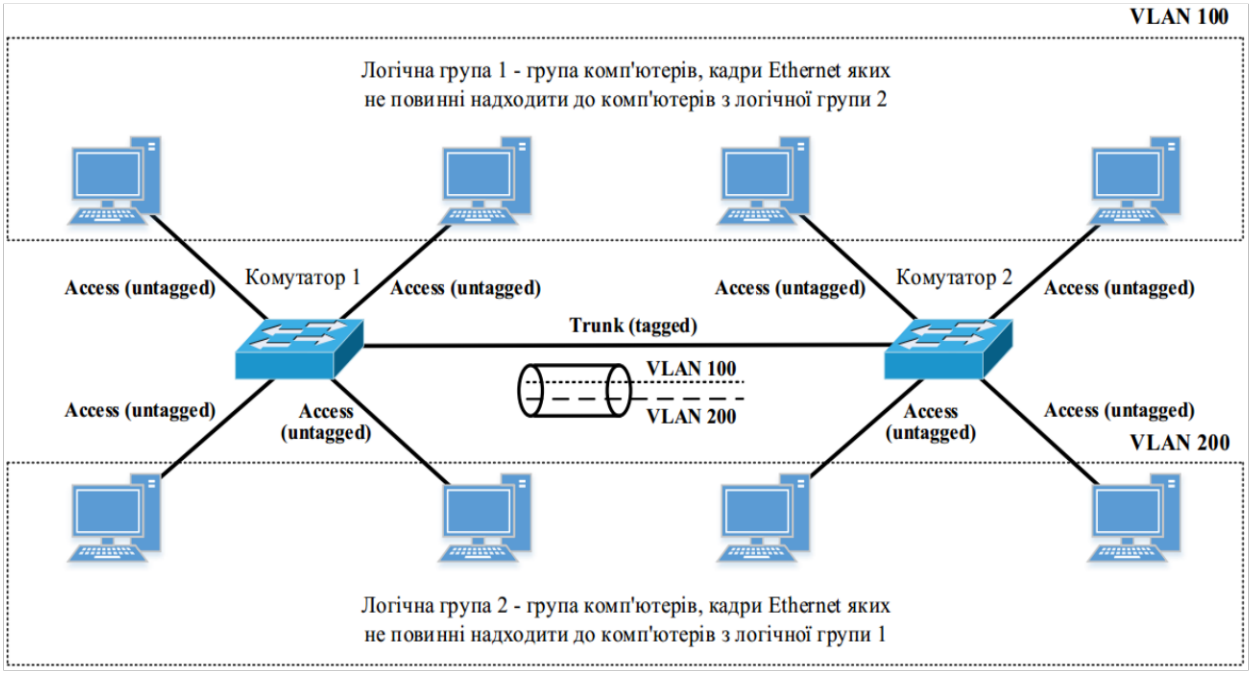


Рисунок 3.6 – VLAN на основі стандарту 802.1Q в мережі з декількома комутаторами (комутатори з’єднані між собою тільки одним трактом, утвореним портами типу Trunk)

Приклад організації можливості обміну інформацією між користувачами із різних VLAN на основі стандарту 802.1Q за допомогою маршрутизатора показаний на рис. 3.7, з якого видно, що комутатор з маршрутизатором з’єднуються тільки одним трактом, утвореним портами типу Trunk (марковані), на відміну від застосування VLAN на основі портів.

Таким чином, можна зробити висновок, що з погляду зручності й гнучкості настроювань, VLAN стандарту IEEE 802.1Q є кращим рішенням у порівнянні з VLAN на основі портів. Крім того, VLAN стандарту IEEE 802.1Q дозволяє на канальному рівні в мережі Ethernet застосовувати механізми забезпечення якості обслуговування QoS відповідно до стандарту IEEE 802.1p за рахунок поля Priority, передбаченого стандартом IEEE 802.1Q. Без застосування стандартів IEEE 802.1Q/P забезпечення якості обслуговування

QoS на канальному рівні в мережі Ethernet неможливо, оскільки кадр Ethernet відповідно до стандарту IEEE 802.3 не містить службового поля для цих цілей.

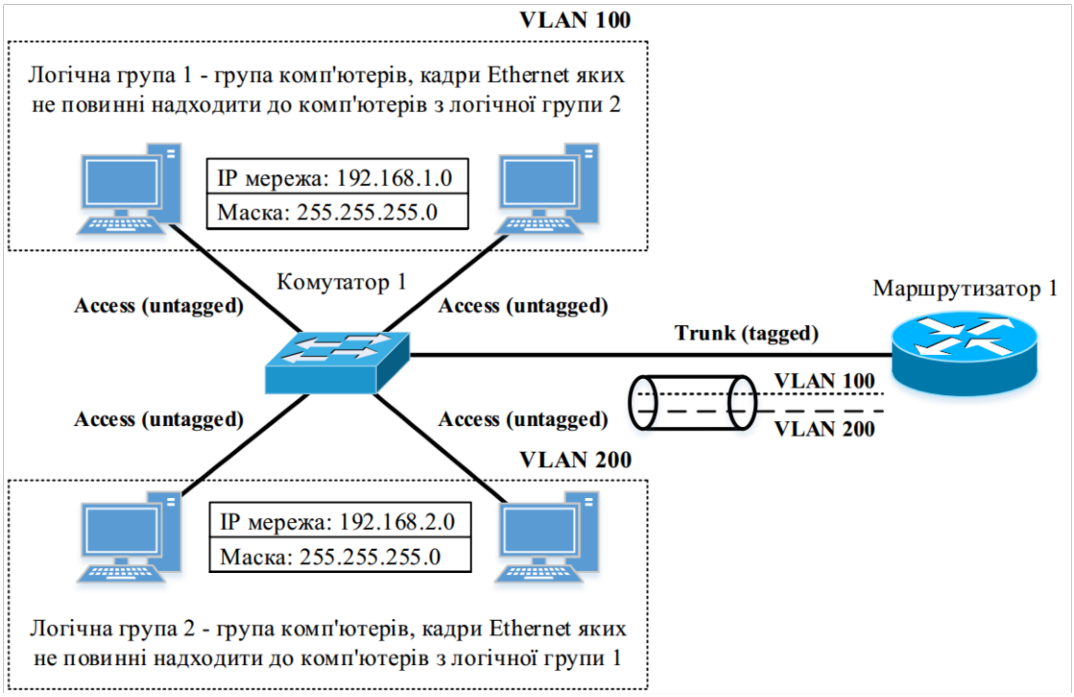


Рисунок 3.7 – Приклад організації можливості обміну інформацією між користувачами із різних VLAN на основі стандарту 802.1Q (комутатор з маршрутизатором з'єднані тільки одним трактом, утвореним портами типу Trunk; IP-адреси користувачів із різних віртуальних мереж повинні знаходитися у різних IP-мережах)

3.1.3. Схема мережі Ethernet з логічною сегментацією на основі VLAN

Схема мережі Ethernet з логічною сегментацією на основі VLAN та вихідні дані, необхідні для конфігурування обладнання, показані на рис. 3.8. До складу імені кожного з комп'ютерів на рис. 3.8 включена його IP-адреса.

З рис. 3.8 видно, що 12 комп'ютерів у мережі розділені на дві логічні групи незалежно від того, до якого з комутаторів вони приєднані. У даному випадку застосовуються два способи організації VLAN − на основі портів і на основі стандарту IEEE 802.1Q.

Комп'ютери логічної групи 1 підключені до портів, які належать до VLAN з ідентифікатором VLAN ID (VLAN Identifier) 100, а комп'ютери логічної групи 2 − до портів, які належать до VLAN з ідентифікатором VLAN

ID 200, що відповідає способу утворення VLAN на основі портів. Відмітимо, що такий спосіб організації VLAN не дозволяє з'єднати комутатор 1 і 2 лише одним трактом передачі, оскільки для кожної з VLAN необхідно використовувати окремий тракт, порти якого належать тільки до однієї VLAN, що не є раціональним.

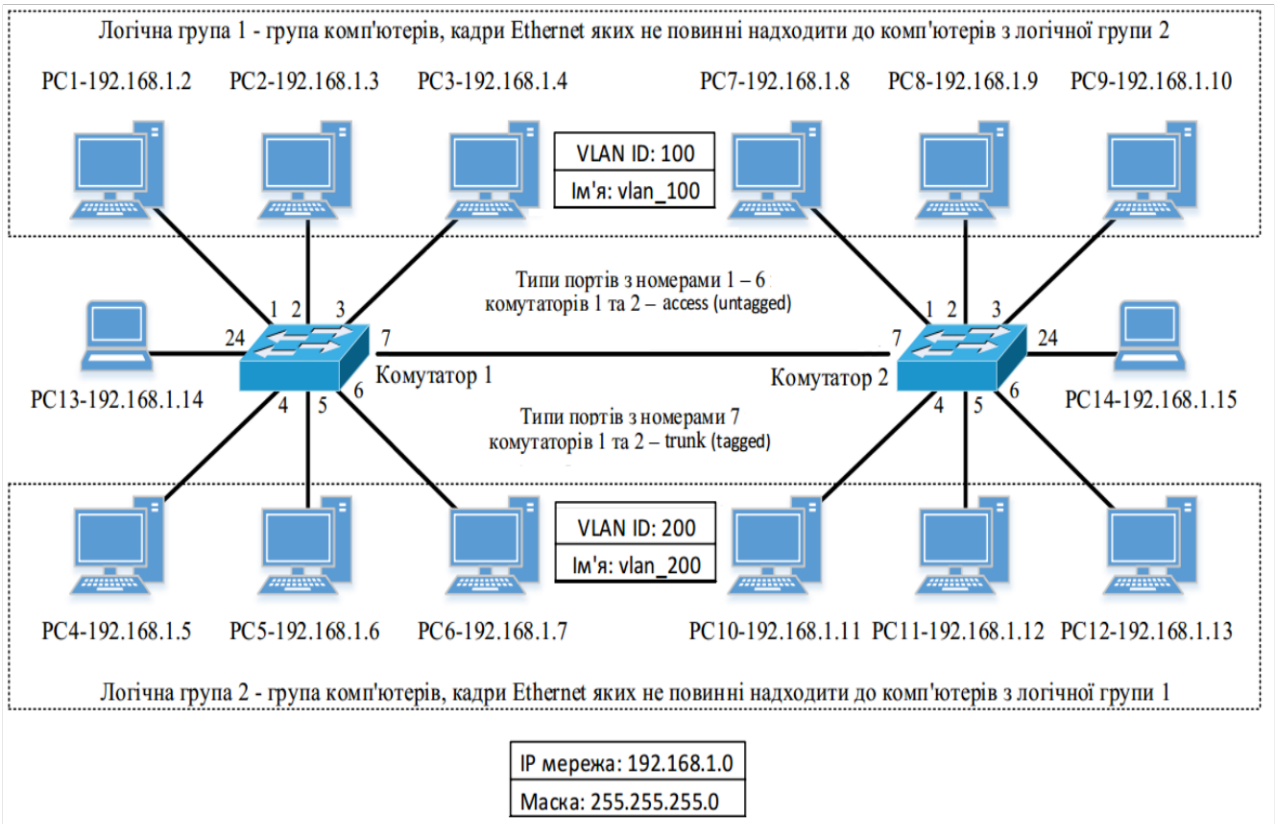


Рисунок 3.8 – Схема мережі на основі комутаторів другого рівня з логічною сегментацією на основі VLAN (якщо не передбачається обмін між користувачами з різних віртуальних мереж, IP-адреси комп'ютерів можуть знаходитись в однакових мережах)

Тому з метою з'єднання комутаторів розглядуваної мережі тільки одним трактом передачі у цьому тракті використано спосіб організації VLAN основі стандарту IEEE 802.1Q. Порти комутаторів, які використовуються для організації VLAN на основі портів мають тип Access (untagged – немарковані), а порти комутаторів, які використовуються для організації VLAN на основі стандарту 802.1Q, − тип Trunk (tagged – марковані).

Нагадаємо, що стандарт IEEE 802.1Q передає кадри від портів, які не включено до будь-якої VLAN, через тракт передачі з маркованими (tagged) портами, і ці кадри автоматично включаються до так званої Native VLAN, ідентифікатор якої за замовчуванням дорівнює 1. На рис. 3.8 два комп'ютери не належать до жодної з віртуальних мереж, тому їх кадри при передачі через тракт між комутатором 1 і комутатором 2 будуть автоматично включені до Native VLAN з ідентифікатором 1 за замовчуванням.

Розподіл портів комутаторів за номерами VLAN наведено в табл. 3.1. Відмітимо, що у розглядуваному прикладі порти комутаторів, які мають тип Trunk (марковані), застосовуються для передачі кадрів з усіх VLAN, але існує можливість передавати по тракту кадри тільки від VLAN з визначеними VLAN ID.

Таблиця 3.1 – Розподіл портів комутаторів за номерами VLAN

Умовна назва комутатора	Номери портів комутаторів	VLAN ID	Тип порту
Комутатор 1	1 – 3	100	Access
	4 – 6	200	Access
	7	–	Trunk
Комутатор 2	1 – 3	100	Access
	4 – 6	200	Access
	7	–	Trunk

3.1.4. Дослідження роботи мережі Ethernet з логічною сегментацію на основі VLAN з використанням широкомовної IP-адреси

Для проведення дослідження треба ввести в командному рядку на одному з комп'ютерів віртуальної мережі команду ***ping*** з використанням широкомовної IP-адреси:

```
ping -n 1 192.168.1.255
```

Тут команда ***ping*** застосовується з параметром [-n count], де count – кількість ехо-запитів, що буде надіслана отримувачу ехо-запиту.

Результати застосування команди **ping -n 1 192.168.1.255** на комп'ютерах PC1-192.168.1.2 (VLAN ID 100), PC4-192.168.1.5 (VLAN ID 200) та PC13-192.168.1.14 (не належить до жодної з VLAN) показані на рис. 3.9 – рис. 3.11.

```
PC>ping -n 1 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.4: bytes=32 time=11ms TTL=128
Reply from 192.168.1.8: bytes=32 time=11ms TTL=128
Reply from 192.168.1.9: bytes=32 time=11ms TTL=128
Reply from 192.168.1.10: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 1, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms
```

Рисунок 3.9 – Результати застосування команди **ping -n 1 192.168.1.255** на комп'ютері PC1-192.168.1.2 (VLAN ID 100)

```
PC>ping -n 1 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.7: bytes=32 time=0ms TTL=128
Reply from 192.168.1.11: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.13: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 1, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.10 – Результати застосування команди **ping -n 1 192.168.1.255** на комп'ютері PC4-192.168.1.5 (VLAN ID 200)

```
PC>ping -n 1 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.15: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.11 – Результати застосування команди **ping -n 1 192.168.1.255** на комп'ютері PC13-192.168.1.14 (належить до Native VLAN)

З результатів дослідження видно, що широкомовні ехо-запити отримують тільки комп'ютери, які належать до тієї ж самої віртуальної підмережі, що і комп'ютер, з якого здійснювався широкомовний запит.

3.2. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи та виконати наступне завдання.

3.2.1. Завдання

Уявно (тобто без використання реального обладнання або програм емуляції) виконайте наступні кроки.

1. Спроєктуйте мережу (призначте IP-адреси та назви комп'ютерів), що складається з двох VLAN подібно до рис. 3.8, але з параметрами згідно свого варіанту (табл. 3.2)

2. Маючи за приклади рис. 3.9 – рис. 3.11, відтворить реакцію мережевої системи на успішне виконання команди ***ping*** широкомовного ехо-запиту з параметром ***–n 1*** (по одному відгуку від кожного комп'ютера VLAN), тобто запишіть у текстовому вигляді повний зміст скріншотів (подібних до рис. 3.9 – рис. 3.11), які повинні бути отриманими на комп'ютерах уявної мережі для кожної з наведених нижче ситуацій:

2.1. Якщо виконати цю команду на одному з ПК у VLAN "vlan_100".

2.2. Якщо виконати цю команду на одному з ПК у VLAN "vlan_200".

2.3. Якщо виконати цю команду на кожному з ПК у Native VLAN.

Для кожного з трьох уявних "скріншотів" вкажіть назву та IP-адресу комп'ютера, з якого уявно виконувалася команда. Вважайте, що затримка отримання ехо-відповідей має випадкове значення в діапазоні 0 – 12 мс.

Таблиця 3.2 – Варіанти завдань до Лабораторної роботи 3

№ з/п	Кіль-кість комута-торів	Простір IP-адрес в кожній мережі	Кількість ПК у VLAN "vlan_100"	Кількість ПК у VLAN "vlan_200"	Кількість ПК у Native VLAN
1.	2	172.16.6.0/24	4	5	3
2.	2	192.168.3.28/24	5	7	2
3.	2	172.16.56.12/24	6	3	3
4.	2	192.168.10.2/24	4	4	4
5.	2	172.16.12.4/24	5	5	2
6.	2	192.168.12.4/24	6	6	3
7.	2	172.16.10.2/24	7	7	2
8.	2	192.168.1.23/24	4	3	4
9.	2	172.16.3.28/24	5	4	2
10.	2	192.168.12.4/24	6	5	3

3.3. Питання до самоконтролю

1. Що таке транковий порт комутатора, транковий канал?

2. В чому полягає відмінність мережевого кадру Ethernet відповідно до стандарту IEEE 802.1Q?

3. Який недолік стандарту IEEE 802.1Q ви можете сформулювати?

4. Що таке Native VLAN?

5. Яке додаткове мережеве обладнання необхідно для організації обміну даними між користувачами з різних віртуальних мереж?

6. Яка мінімальна кількість портів типу Trunk (марковані), що функціонують згідно стандарту 802.1Q, має бути у наявності загалом на обох комутаторах у мережі, яка була створена в практичній частині?

3.4. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

3.5. Література до Лабораторної роботи 3

Рекомендовані літературні джерела до виконання Лабораторної роботи 3: [1, 2, 7, 8].

ЛАБОРАТОРНА РОБОТА 4. БЕЗПЕКА БЕЗДРОТОВИХ ЛОКАЛЬНИХ МЕРЕЖ WIFI

Мета роботи: набуття навичок безпекового налаштування WiFi-роутерів.

4.1. Теоретичний матеріал до лабораторної роботи

4.1.1. Загальна інформація

Маршрутиза́тор, або ро́утер – електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Для звичайного користувача маршрутизатор – це мережевий пристрій, який підключається між локальною мережею та постачальником послуги доступу до мережі Інтернет (провайдером). Часто маршрутизатор виконує також інші функції: захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до ресурсів Інтернету, роздає IP-адреси, шифрує трафік тощо.

Функції маршрутизатора може виступати як спеціалізований пристрій, так і звичайний комп'ютер.

Бездротова точка доступу – центральний пристрій бездротової мережі, яку використовують для з'єднання між бездротовими клієнтами, а також для з'єднання дротового і бездротового сегментів (виконує функції моста між ними).

Також бездротові точки доступу часто використовуються для створення так званих «гарячих точок» – областей, у межах яких клієнтові надається, як правило, безкоштовний доступ до мережі Інтернет. Зазвичай такі точки містяться в бібліотеках, аеропортах, вуличних кафе великих міст.

Останнім часом бездротові точки доступу набули поширення при створенні домашніх мереж. Для створення такої мережі в межах однієї квартири достатньо однієї точки доступу.

Слід враховувати, що в сенсі розподілу мережевого трафіку маршрутизатор в якості точки доступу функціонує як звичайний концентратор. При декількох підключеннях до однієї точки смуга пропускання ділиться на кількість підключених користувачів. Теоретично, обмежень на кількість підключень немає, але на практиці варто обмежитися, виходячи з мінімально необхідної швидкості передачі даних для кожного користувача.

Зазвичай бездротові маршрутизатори мають вбудований сервер DHCP, який дозволяє автоматично надавати клієнтам локальної мережі налаштування TCP/IP, необхідні для отримання доступу до мережі. До налаштувань серверу DHCP відносяться: діапазон видаваних адрес, резервування IP-адрес, ім'я домену (Domain Name), адреси серверів DNS.

1.2. Безпека бездротових мереж

Бездротовий сегмент мережі завжди має додаткову небезпеку, вимагаючи більшої уваги при установці і налаштування. При налаштування захисту бездротової мережі зазвичай розглядаються декілька методів:

- зміна пароля адміністратора;
- відключення трансляції SSID мережі;
- фільтрація за MAC-адресами;
- шифрування даних;
- зниження потужності передавача тощо.

1.2.1 Зміна пароля адміністратора

Пристрої випускаються із стандартними (однаковими для всіх подібних пристроїв) паролями. У одному з вікон налаштування користувач повинен ввести новий пароль. Якщо налаштування пристрою здійснювалася стороннім майстром, то зміна пароля є одним з перших пунктів в його роботі.

1.2.2 Відключення трансляції SSID мережі

У нормальному режимі точка доступу повідомляє свій мережевий ідентифікатор (SSID), щоб полегшити пошук і підключення до бездротової мережі. Це повідомлення є широкомовним, його можуть отримати не тільки комп’ютери вашої мережі, але і сторонні, які знаходяться в її зоні дії.

У багатьох випадках немає ніякої необхідності демонструвати свою бездротову мережу всім бажаючим, тому цей режим можна відключити. Всі пристрої мають встановлений за умовчанням SSID мережі. Якщо змінити SSID і одночасно з цим відключити його трансляцію, то підключитися до мережі зможе тільки той, хто заздалегідь знає SSID.

1.2.3 Фільтрація за MAC-адресами

Якщо налаштовується невелика бездротова мережа вдома або в офісі, то, як правило, рідко виникає необхідність підключати додаткові комп'ютери.

В цьому випадку можливо використовувати фільтрацію за MAC-адресами. Цей режим дозволить підключатися до мережі тільки заданим пристроям з їх унікальними MAC-адресами.

Як і паролі, адреси, дозволених для даної мережі MAC-адрес, слід зберігати таємно від сторонніх осіб. Але фільтрація за MAC-адресами не може забезпечити стовідсотковий захист. Вона розглядається як один з заходів по забезпеченню безпечної роботи.

1.2.4 Шифрування даних

Щоб захистити дані під час передачі від одного мережевого пристрою до другого, використовується шифрування даних. При шифруванні даних необхідно на кожному з цих пристроїв налагодити протокол шифрування і ключі.

Основні типи шифрування, що використовуються в бездротових мережах: WEP-шифрування та WPA-шифрування

WEP-шифрування. Перший та найбільш простий спосіб шифрування – використання протоколу WEP (Wired Equivalence Privacy). На практиці цей метод шифрування вже не вважається дуже надійним. Використання недостатньо довгих ключів дозволяє дешифрувати повідомлення.

При використанні WEP-шифрування необхідно, щоб на всіх підключених точках застосовувались ідентичні ключі. Чим довше ключ, тим складніше дешифрувати повідомлення. Сучасне бездротове устаткування використовує 64-бітні, 128-бітні та 256-бітні ключі. У сучасному мережевому устаткуванні

може задаватися до чотирьох ключів WEP. За згодою з клієнтами один з них вибирається в якості активного ключа і використовується для шифрування. Періодично (наприклад, раз на тиждень) можна змінювати активний ключ. Ключі задаються ідентичним способом на всіх пристроях бездротової мережі;

WPA-шифрування. У пристроях стандарту 802.11g підтримується поліпшений алгоритм шифрування WPA (Wi-Fi Protected Access). У цей стандарт об'єднується два методи: TKIP і MIC. Протокол TKIP (Temporal Key Integrity Protocol) – це реалізація динамічних ключів шифрування. Ключі шифрування мають довжину 128 біт і генеруються при посиланні кожних 10 Кбайт даних за складним алгоритмом. При цьому загальна кількість можливих варіантів ключів обчислюється сотнями мільярдів. Така система дає найвищі гарантії надійності шифрування даних. Протокол MIC(Message Integrity Check) – це протокол перевірки цілісності пакетів. При його використанні звіряються відправлені і отриманні дані. Це повинно виключити їх зміни в дорозі. Протокол дозволяє відкидати пакети, які були додані в канал третьою особою. Таким чином, хакер не може вбудувати шкідливі коди до даних під час їх передачі.

Крім згаданих протоколів, багато виробників бездротового устаткування вбудовують в свої рішення підтримку стандарту AES (Advanced Encryption Standard), який приходить на заміну TKIP.

Існує два режими WPA-шифрування:

- WPA-EAP (Extensible Authentication Protocol);
- WPA-PSK (Pre-Shared Key).

Режим WPA-EAP використовується в корпоративних мережах, оскільки вимагає наявність сервера автентифікації (RADIUS-сервера). З цієї причини він не може використовуватися в домашніх умовах.

Для персонального використання призначений режим WPA-PSK. Він передбачає застосування заздалегідь заданих ключів шифрування (пароль доступу), однакових для всіх мережевих пристроїв, а первинна автентифікація користувачів здійснюється з використанням даного ключа.

В якості алгоритмів шифрування при використанні стандарту WPA можна вибрати TKIP або AES. Шифрування WPA-PSK по методу TKIP вважається неприступною стіною для хакерів. Шифрування WPA-PSK по методу AES є ще могутнішим способом захисту, раніше використовуваним в мережах VPN. Ця технологія підтримується не всім сучасним мережевим устаткуванням. Існує також алгоритм WPA2 (наступна версія протоколу WPA). Якщо всі пристрої бездротової мережі підтримують даний режим, то можна їм скористатися. Налаштування в даному випадку здійснюються такі самі, як і у разі WPA-шифрування.

1.2.5 Зниження потужності передавача

Для передачі даних в радіоефір кожен бездротовий пристрій забезпечено приймачем і передавачем радіохвиль. Від його потужності залежить радіус дії бездротової мережі, а від чутливості – якість прийому сигналу. Непоганим варіантом захисту мережі є підбір такої потужності передавача, якої достатньо для покриття тільки ваших пристроїв мережі. Цим ви відсікаєте тих, хто може налаштуватися на вашу мережу (з сусіднього будинку або з машини на стоянці поряд з офісом).

Не потрібно відразу встановлювати дуже низьку потужність, оскільки цим можна «відключити» зв’язок з віддаленими комп’ютерами. Зменшуйте потужність поступово, але не встановлюйте ту, на якій спостерігається порогова робота пристрою (в певних умовах сигнал може ще більше послабитись), це може привести до відключення віддалених комп’ютерів. Визначити зону покриття бездротової мережі в умовах реального приміщення можна за допомогою ноутбука або іншого пристрою зі встановленою програмою (наприклад, Network Stumbler або WirelessMon). Network Stumbler видає інформацію про MAC-адреси виявлених бездротових пристроїв, значення SSID, імена пристроїв, канали, повідомляє про те, чи включено шифрування і т.д. Network Stumbler допоможе визначити, чи вірно налаштована ваша бездротова мережа, а також знайти місця з недостатнім радіопокриттям,

встановити наявність і характеристики інших мереж, які можуть заважати роботі вашої мережі.

1.2.6 Додаткові заходи

Якщо точка доступу або маршрутизатор дозволяє настроювати даний пристрій по дротовому підключенню при відключеному режимі бездротового налаштування, то доцільно застосувати цей метод. В такому випадку хакер не зможе підключитися до точки доступу, навіть знаючи пароль адміністратора. При підключенні по бездротовій мережі до Інтернету за допомогою маршрутизатора можна використовувати його вбудовані засоби захисту. Зазвичай маршрутизатори мають вбудований міжмережевий екран (файрвол). Налаштування його параметрів не дуже складне, і не слід їм нехтувати, оскільки в цьому випадку від погроз проникнення хакерів з Інтернету може бути захищена цілком вся мережа.

1.2.7 Організаційні заходи

Для підвищення рівня захищеності Wi-Fi-зв'язку (особливо в корпоративних мережах) необхідно дотримуватися наступних вимог:

- обмежувати доступ до мережі на фізичному рівні;
- оптимально налаштувати параметрів конфігурації механізмів автентифікації та шифрування для забезпечення ефективності роботи, надійності та безпеки мережі;
- використовувати програмні засоби захисту пристроїв користувача та контролю усієї мережі;
- здійснювати постійний моніторинг мережі для запобігання створенню в корпоративній мережі несанкціонованих точок доступу чи підключення;
- використовувати VPN для усіх пристрої в корпоративних клієнтів, що забезпечить захист при використанні різних точок доступу, що не належать корпоративної інфраструктурі, а також широкі можливості з вибору алгоритмів автентифікації, шифрування та перевірки цілісності потоку даних;
- формувати політики безпеки та складати відповідну документацію;

- проводити інструктажі та семінари для ознайомлення корпоративних робітників з основами правилами безпеки під час роботи з офісною технікою та засобами зв'язку, зокрема, з мережею Інтернет;
- використовувати міжмережеві екрани.

4.2. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи, виконати завдання та вирішити задачі.

4.2.1. Опис завдання

Уявно (тобто без використання реального обладнання чи програмного емулятора) виконати налаштування умовного WiFi-роутера виробництва фірми TP-Link згідно наступної інструкції.

4.2.1.1. Використовуючи стаціонарний комп’ютер або ноутбук з Ethernet-роз'ємом типу RJ-45, під'єднатися кабелем (патч-кордом) до WiFi-роутера.

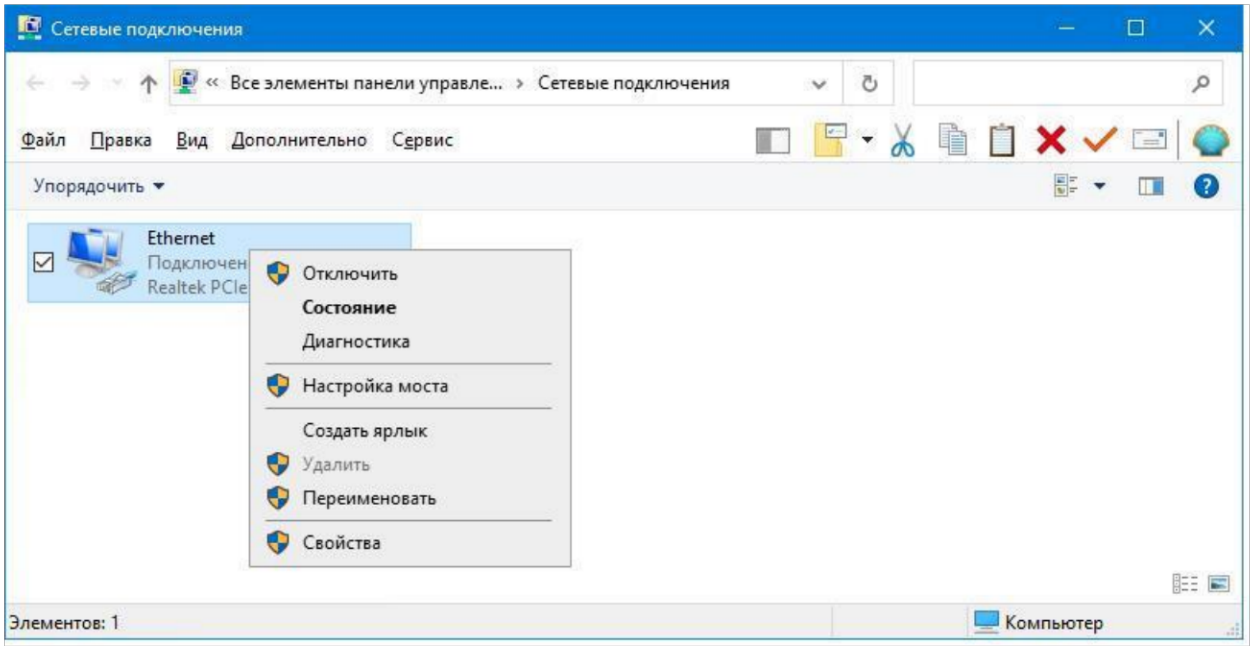
4.2.1.2. Налаштувати мережевий Ethernet-адаптер на роботу в мережі 192.168.0.X з маскою 255.255.255.0 наступним чином:

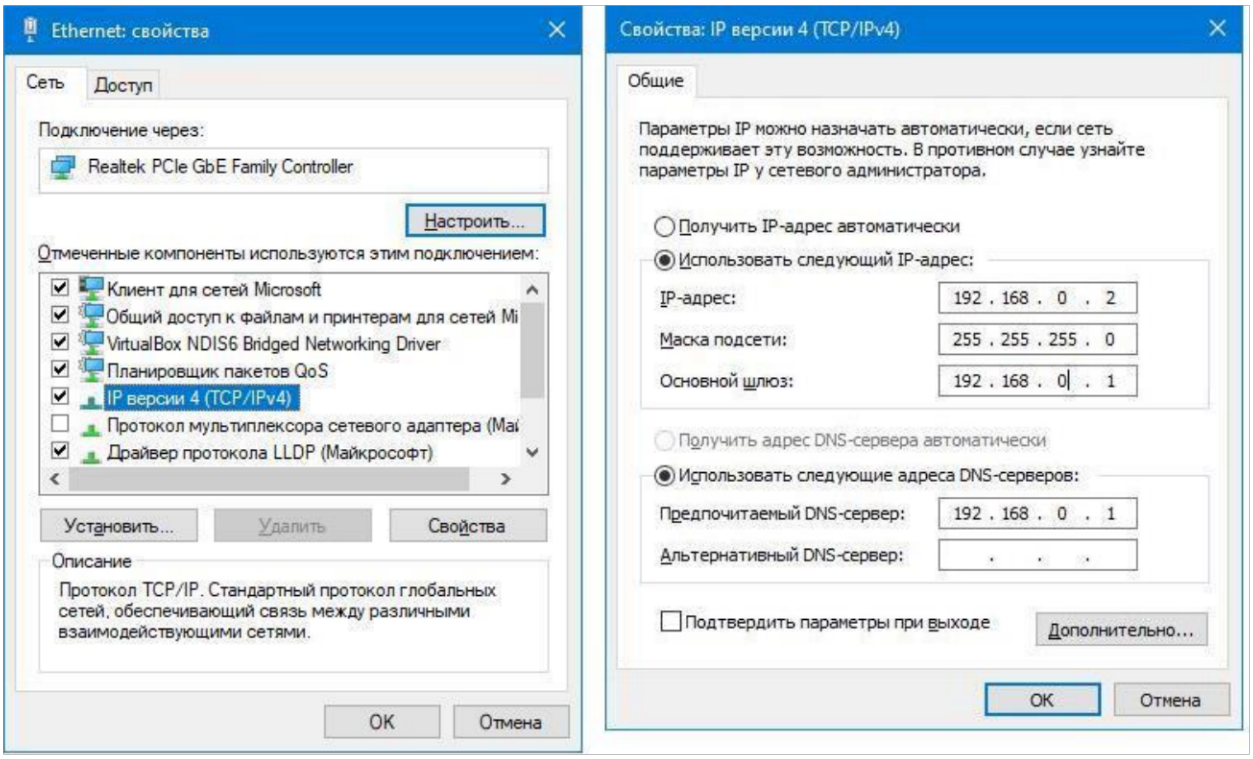
Пуск / Параметри / Мережа та Інтернет / Ethernet / Налаштування параметрів адаптера / Клік правою кнопкою миши на позначці мережевого адаптера / Властивості / IP версії 4 (TCP/IPv4) / Властивості / Використовувати наступну IP-адресу:

- IP-адреса: 192.168.0.2
- Маска підмережі: 255.255.255.0
- Основний шлюз: 192.168.0.1

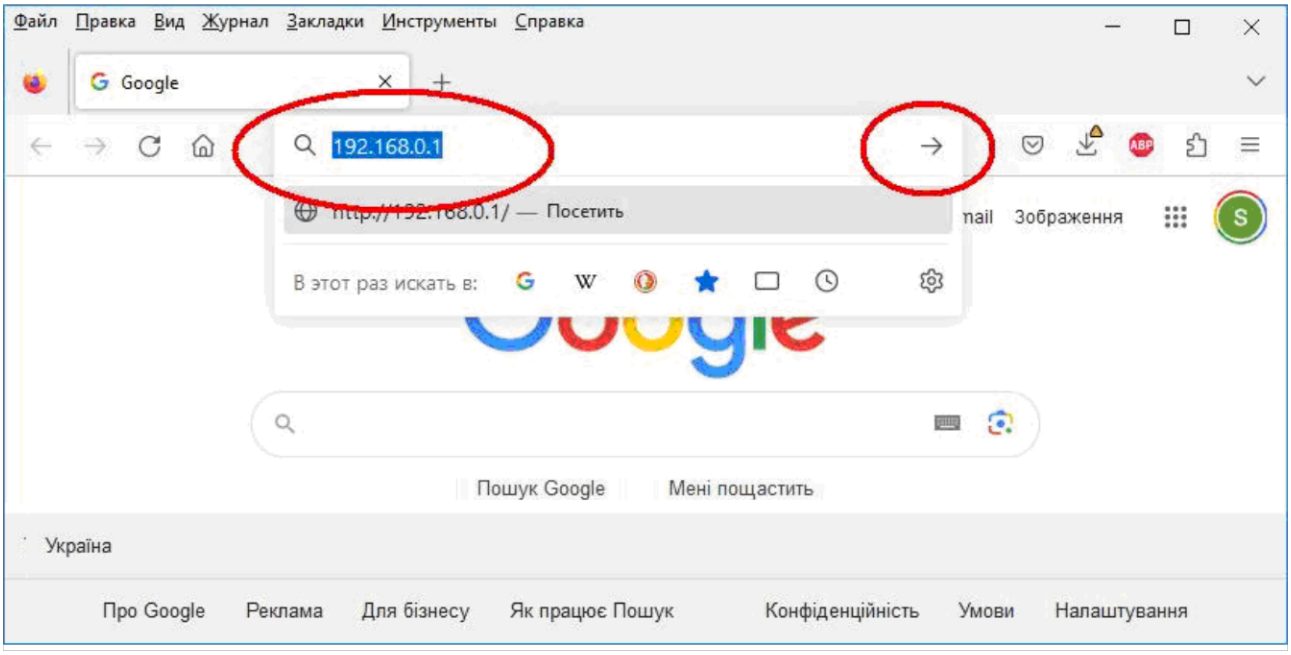
/ Використовувати наступі адреси DNS-серверів:

- Бажаний DNS-сервер: 192.168.0.1

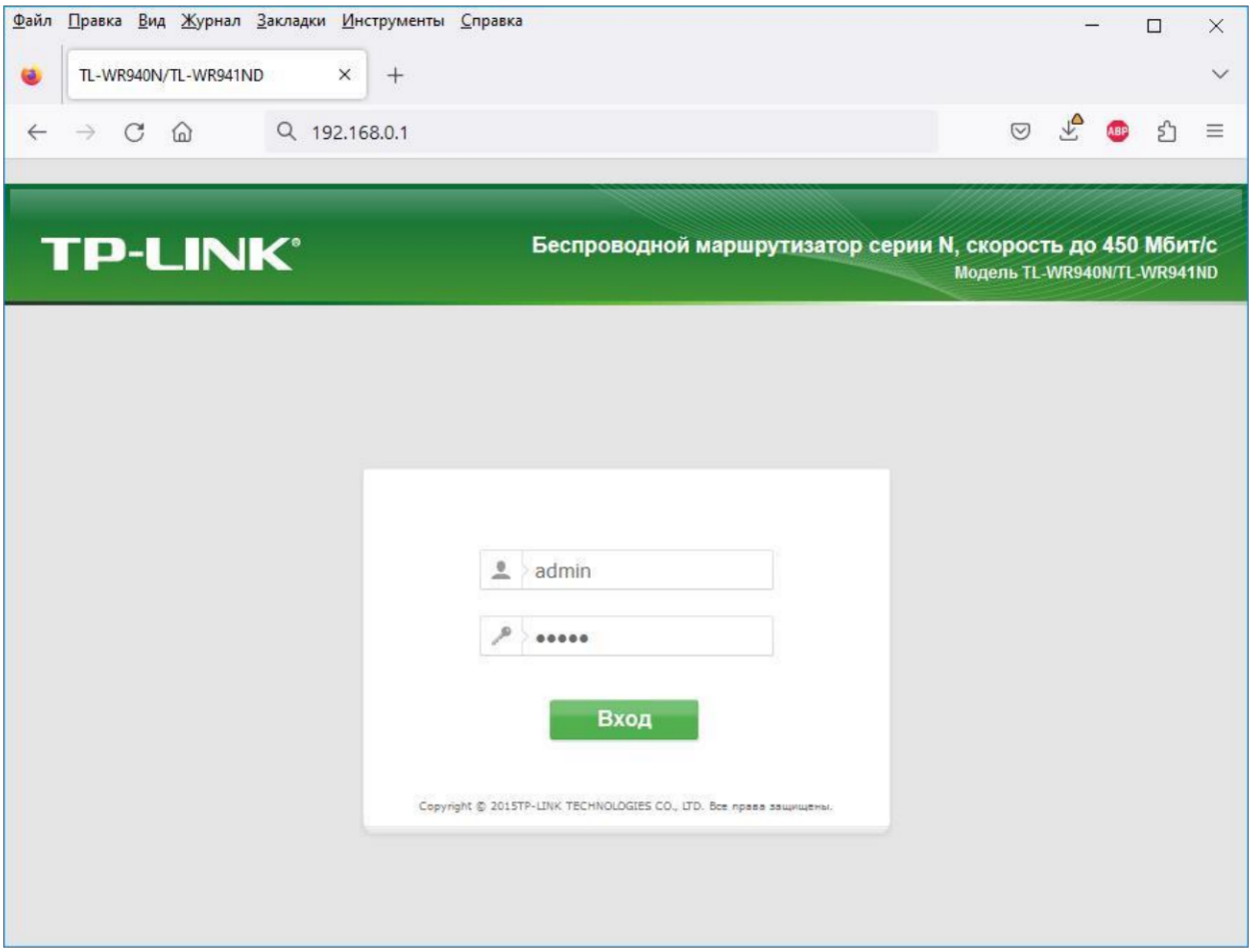




4.2.1.3. Запустити на комп’ютері будь-який веб-браузер. В полі адреси браузера ввести IP-адресу WiFi-роутера виробництва фірми TP-Link (за замовченням – 192.168.0.1), натиснути на піктограму "стрілка":

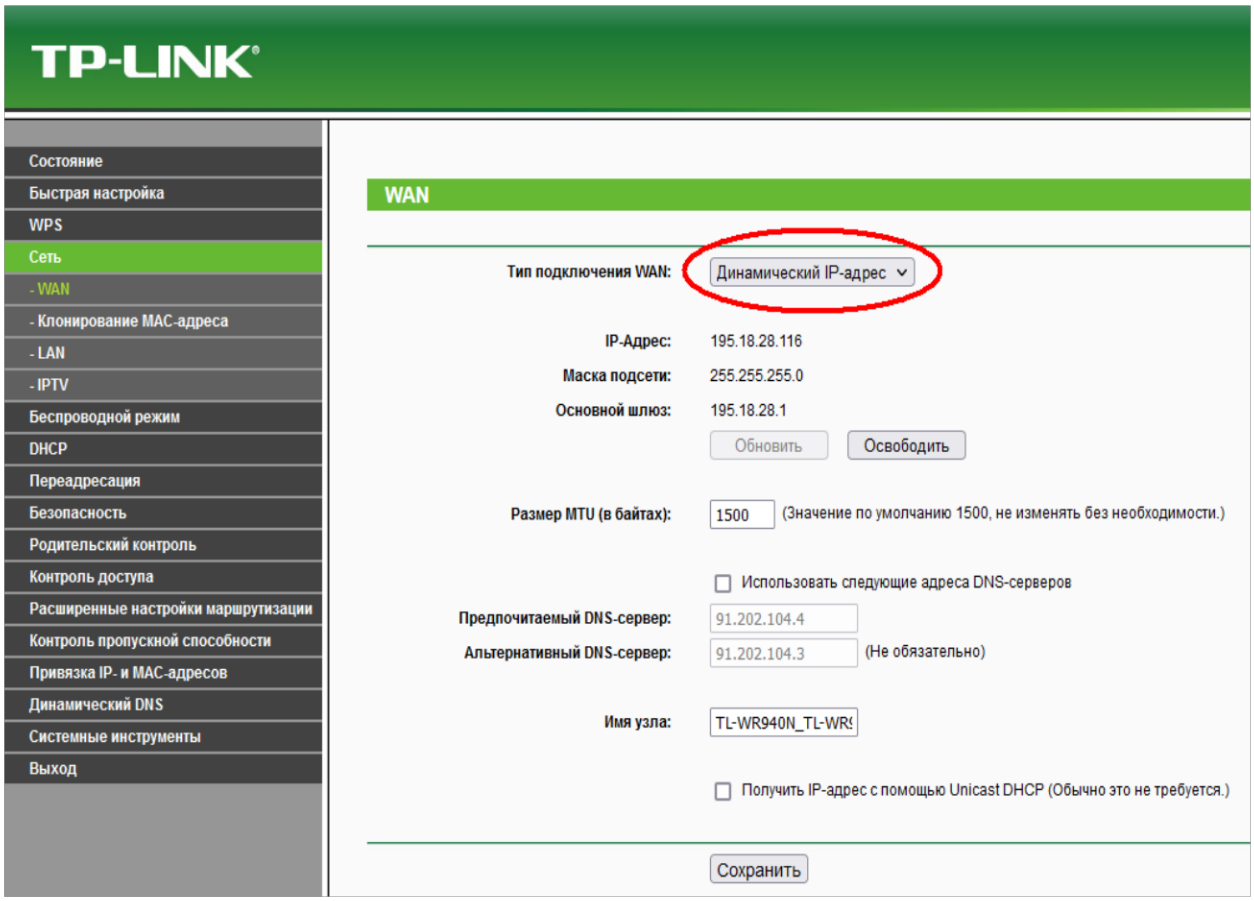


4.2.1.4. У вікні, що відкрилося, ввести логін та пароль входу до інтерфейсу налаштування роутера за замовченням – логін "admin"; пароль "admin":

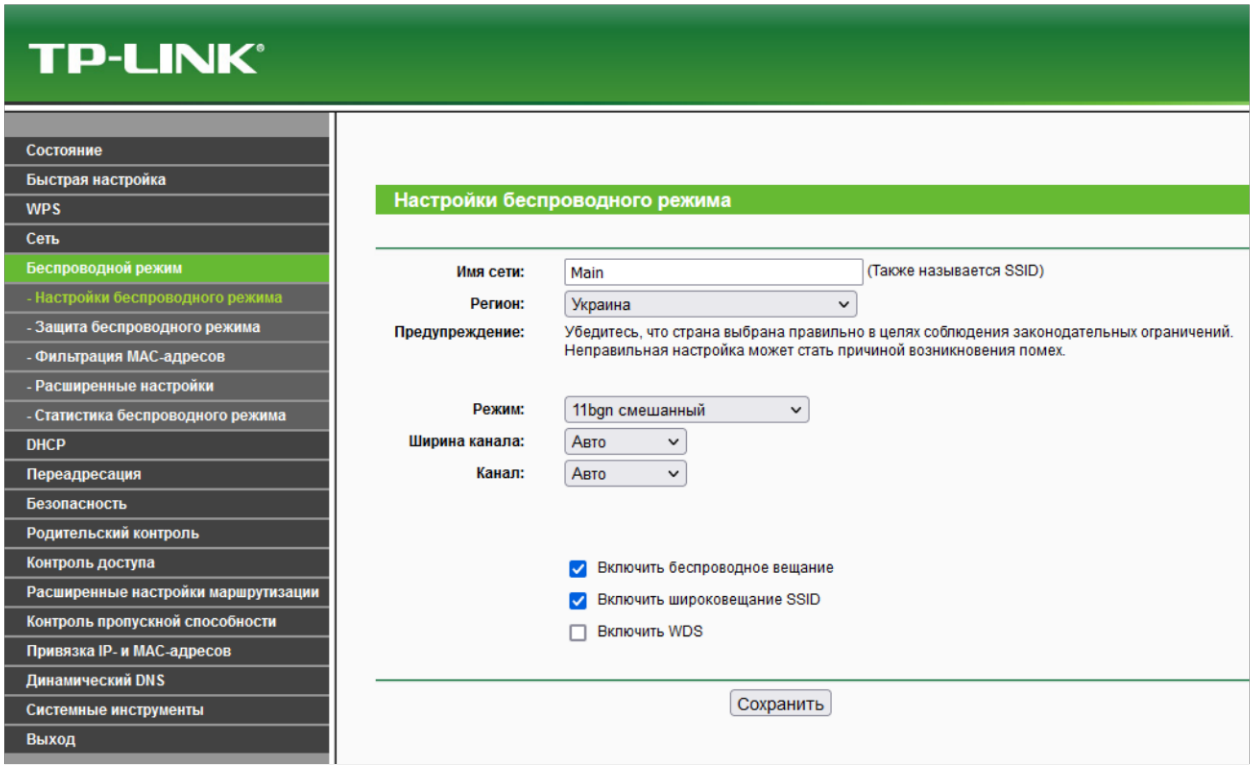


4.2.1.5. Після автентифікації та доступу до налаштувань роутера ознайомитись з пунктами меню панелі адміністрування. (Якщо під'єднатися до налаштувань роутера не вдалося, здійснити примусове скидання роутера до заводських налаштувань).

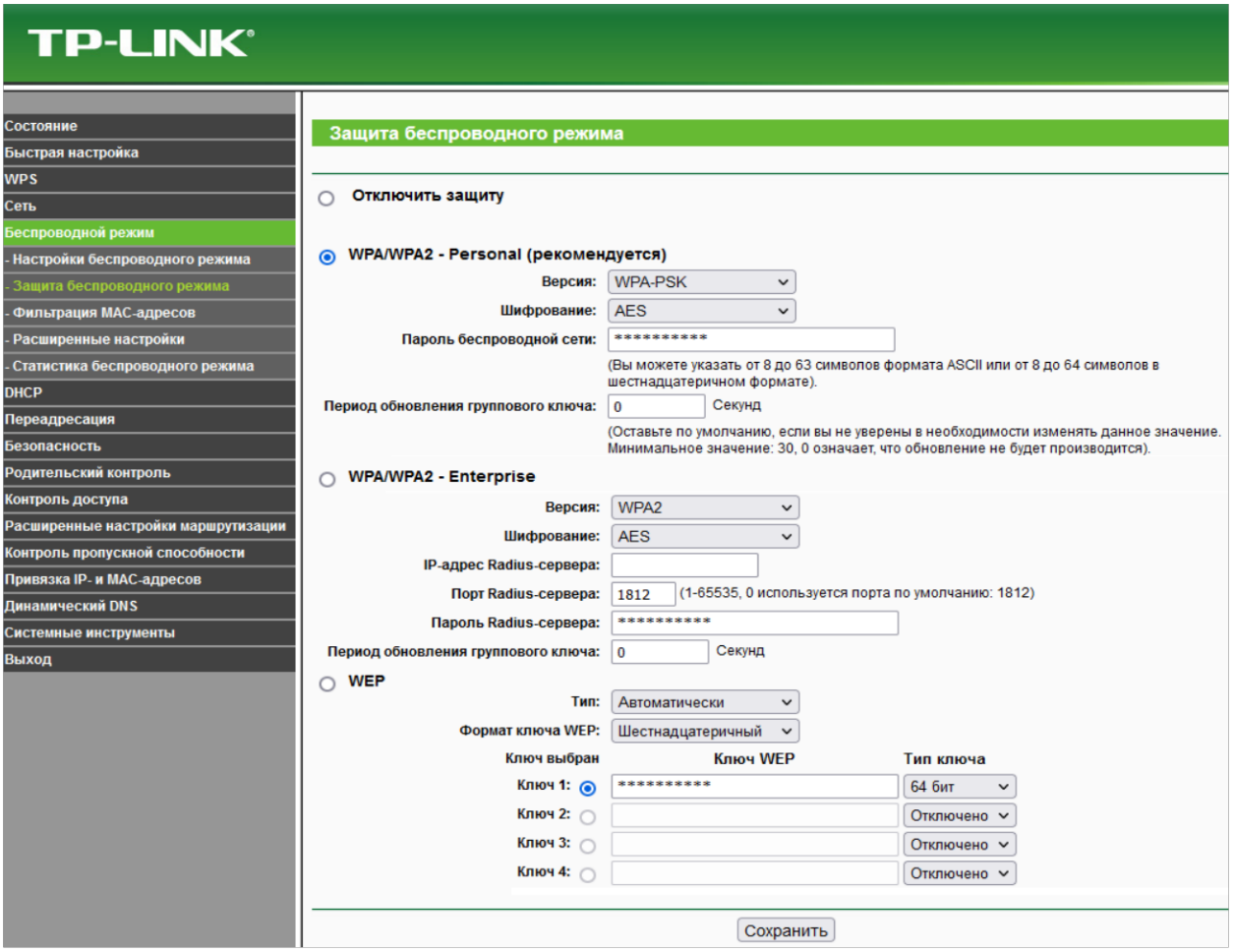
4.2.1.6. Перевірити налаштування з’єднання з провайдером (пункт меню Сеть / WAN):



4.2.1.7. Налаштувати параметри WiFi-мережі – назву бездротової мережі (SSID), регіон, режим (Беспроводный режим / Настройки беспроводного режима):

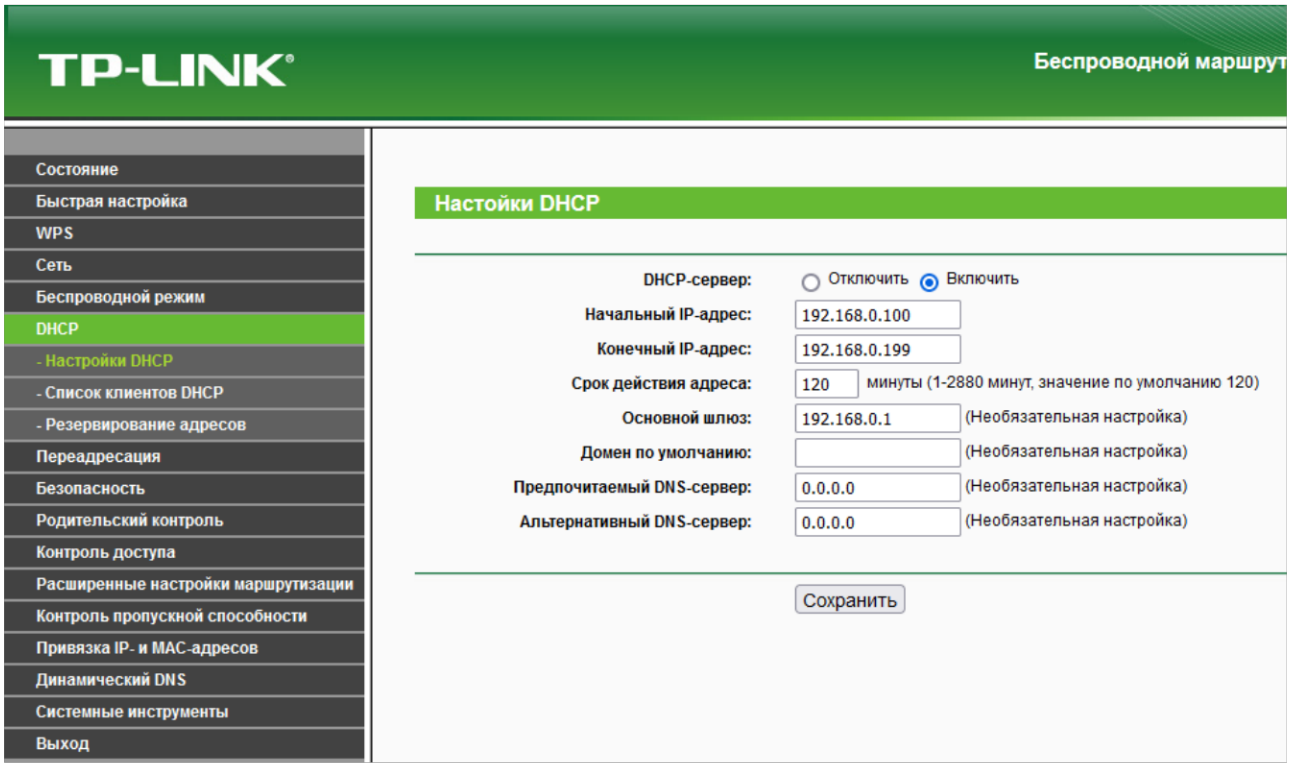


4.2.1.8. Налаштувати тип та параметри захисту бездротової мережі (Беспроводный режим / Защита беспроводного режима):

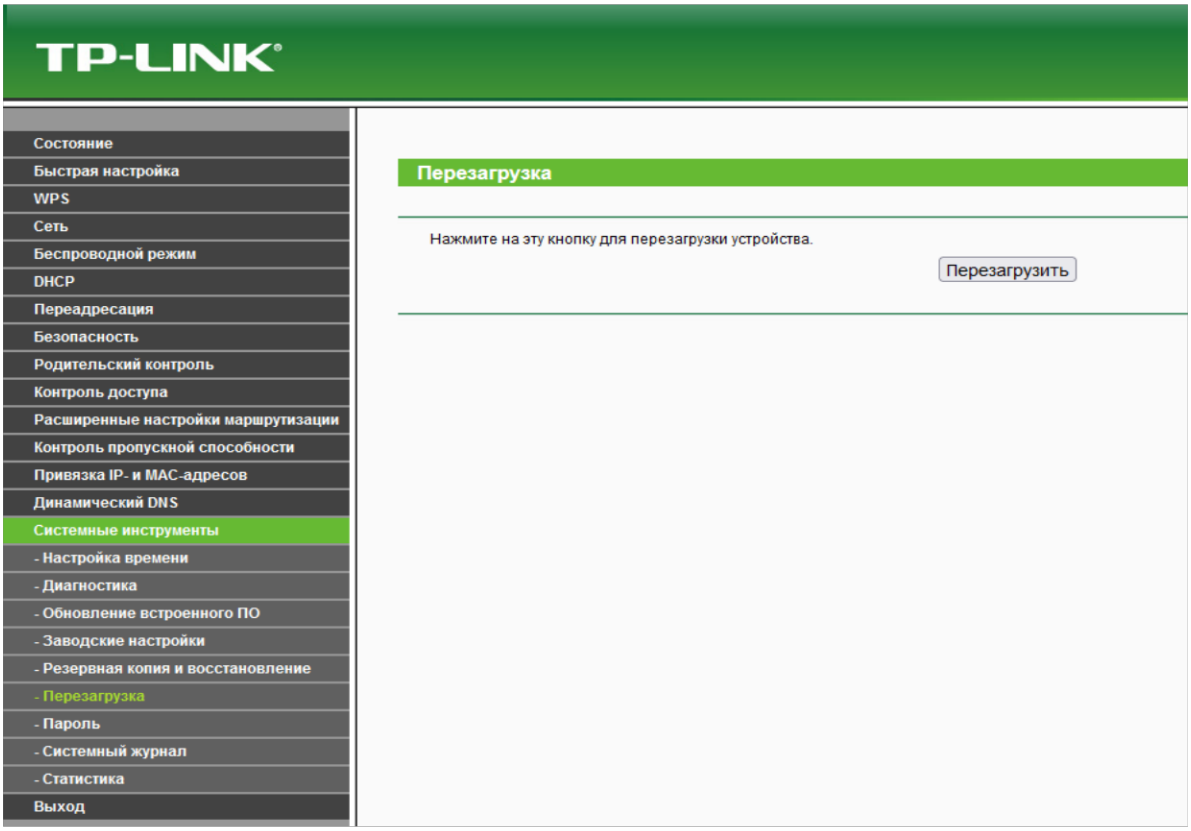


4.2.1.9. Налаштувати параметри роботи вбудованого DHCP-сервера.

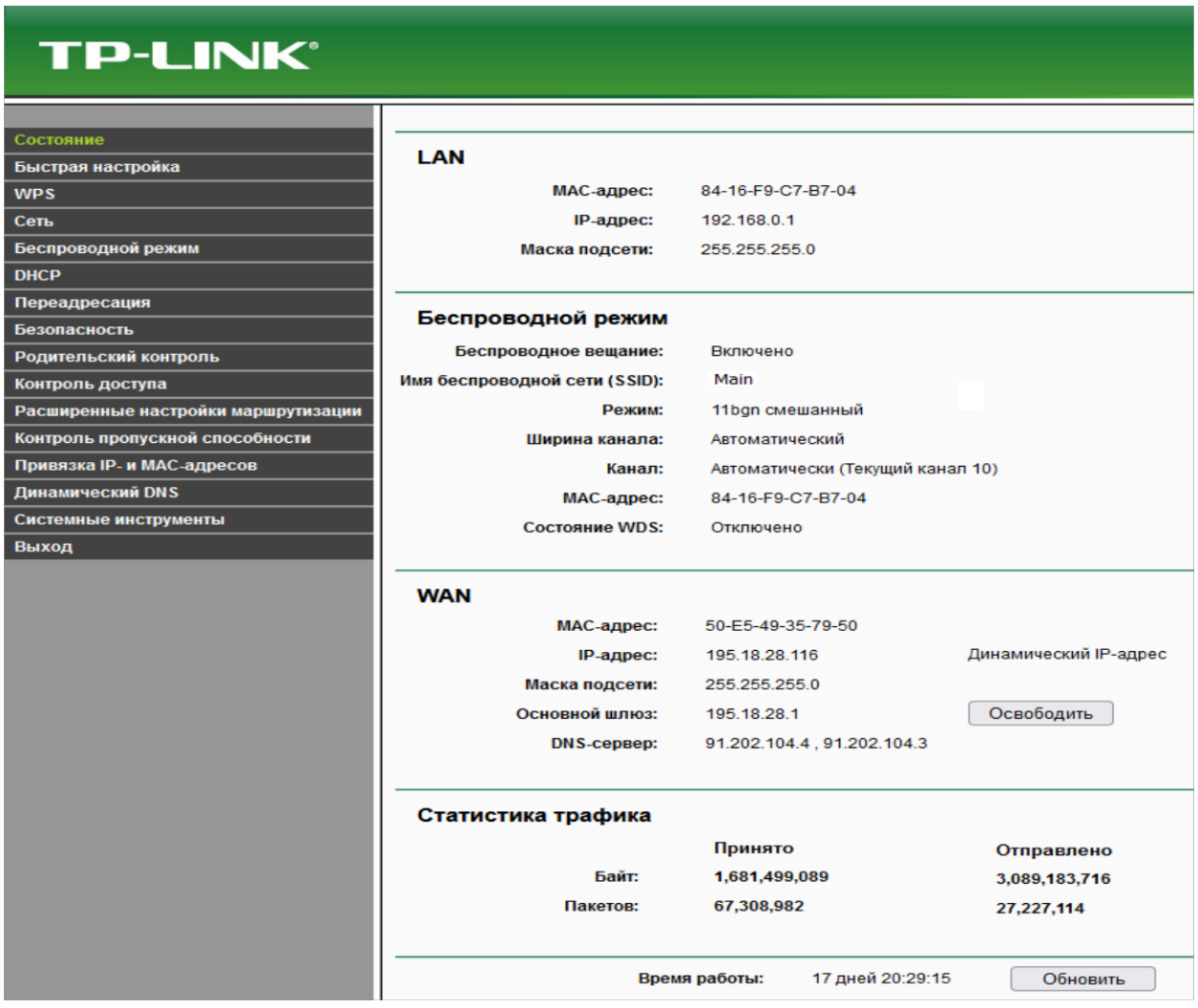
Таке налаштування зводиться до встановлення діапазону IP-адрес, в межах якого сервер буде обирати випадковим чином IP-адресу та автоматично призначати її кожному клієнтському комп'ютеру, який буде під'єднатися до WiFi-мережі. Діапазон встановлюється шляхом надання значень полям "Початкова IP-адреса" та "Кінцева IP-адреса" на сторінці "Налаштування DHCP" роутера. Наприклад, простір IP-адрес в локальній мережі заданий виразом "192.168.0.0/24". Це означає, що перші 24 біти маски підмережі задають адресу мережі (192.168.0.X), а останні 8 бітів - множину адрес всередині підмережі (загалом 2^8 = 256 адрес), тобто простір починається з адреси 0 і закінчується адресою 255. Якщо потрібно задати діапазон адрес для сервера DHCP, що починається зі 101-ї адреси від початку простору IP-адрес і містить 100 адрес, початкова IP-адреса матиме значення 100, а кінцева - 199:



4.2.1.10. Перезавантажити роутер TL-Link для застосування збережених налаштувань (Системные инструменты / перезагрузка):



4.2.1.11. Переконатися в коректності налаштувань (Состояние):



4.2.2. Задача 1

Розглянути метод захисту бездротової мережі згідно свого варіанту (табл. 4.1). Відповісти на питання: в чому полягає сутність даного методу, за рахунок чого підвищується захищеність бездротових мереж даним методом, чи можна сформулювати якісь недоліки методу, в яких випадках рекомендується використовувати даний метод захисту.

Таблиця 4.1 – Варіанти завдань до Задачі 1 Лабораторної роботи 4

№ з/п	Номер підпункту в опису Лаб. роб.	Метод захисту бездротової мережі
1.	4.1.2.5	Зниження потужності передавача
2.	4.1.2.6	Додаткові заходи
3.	4.1.2.7	Організаційні заходи
4.	4.1.2.1	Зміна пароля адміністратора
5.	4.1.2.2	Відключення трансляції SSID мережі
6.	4.1.2.3	Фільтрація за MAC-адресами
7.	4.1.2.4	WEP-шифрування даних
8.	4.1.2.4	WPA-шифрування даних
9.	4.1.2.4	WPA-шифрування в режимах WPA-EAP та WPA-PSK
10.	4.1.2.5	Зниження потужності передавача

4.2.3. Задача 2

Розрахувати налаштування вбудованого DHCP-серверу роутера TP-Link згідно свого варіанту (табл. 4.2), а саме - знайти значення полів "Початкова IP-адреса" та "Кінцева IP-адреса".

4.3. Питання до самоконтролю

1. Чим на ваш погляд відрізняються поняття "роутер" (тобто бездротовий маршрутизатор) і "точка доступу"?

2. Скільки вбудованих мережевих адаптерів (інтерфейсів) повинен містити Wi-Fi-роутер?

3. Які переваги надає використання протоколу DHCP в бездротових WiFi-мережах?

Таблиця 4.2 – Варіанти завдань до Задачі 2 Лабораторної роботи 4

№ з/п	Простір IP-адрес в локальній мережі	Начальна IP-адреса	Кількість IP-адрес
1.	172.16.6.0/24	середина простору IP-адрес	100
2.	192.168.3.28/24	51-а адреса від початку простору IP-адрес	50
3.	172.16.56.0/24	150-та адреса від кінця простору IP-адрес	100
4.	192.168.10.0/24	середина простору IP-адрес	50
5.	172.16.12.4/24	151-а адреса від початку простору IP-адрес	100
6.	192.168.12.0/24	50-та адреса від кінця простору IP-адрес	30
7.	172.16.10.0/24	середина простору IP-адрес	150
8.	192.168.1.23/24	201-а адреса від початку простору IP-адрес	20
9.	172.16.3.0/24	200-та адреса від кінця простору IP-адрес	150
10.	192.168.12.0/24	середина простору IP-адрес	120

4. Які протоколи шифрування даних застосовуються в бездротових мережах?

5. Чи варто використовувати вбудований міжмережевий екран (файрвол) WiFi-адаптера і наскільки це складна процедура?

6. Чи потрібно обмежувати фізичний доступ зловмисників до бездротового обладнання?

7. Наведіть приклади програм, за допомогою яких можна досліджувати зону покриття бездротової мережі в умовах реального приміщення.

8. Яким чином зниження потужності передавача знижує ризики інформаційної безпеки?

4.4. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

4.5. Література до Лабораторної роботи 4

Рекомендовані літературні джерела до виконання Лабораторної роботи 4: [1, 2, 9, 10].

ЛАБОРАТОРНА РОБОТА 5. БЕЗПЕКА ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Мета роботи: набуття навичок захисту інформації в дротових лініях телефонного зв'язку.

5.1. Теоретичний матеріал до лабораторної роботи

5.1.1. Пристрої перехоплення телефонних повідомлень

5.1.1.1. Основні методи прослуховування телефонних ліній

Цінність інформації, що передається по телефонних лініях в організаціях і приватними особами обумовлює необхідність вивчання методів, за допомогою яких зловмисником можуть бути здійснені операції по перехопленню та, відповідно, порушенню конфіденційності переговорів саме по телефонних каналах.

На рис. 5.1 наведено узагальнену структурно-топологічну схему абонентської телефонної лінії. Тут цифрами позначено як місця можливого витоку інформації, так і місця можливого використання засобів несанкціонованого перехоплення, що вони перелічені нижче:

1 – радіозакладка паралельного підключення;

2 – комбінована телефонно-акустична радіозакладка;

3 – радіозакладка послідовного підключення;

4 – закладка типу "довге вухо";

5 – низькоомний адаптер;

6 – високоомний адаптер;

7 – безконтактний адаптер;

8 – наводки телефонного сигналу на інші кола;

9 – акустоелектричне перетворення;

10 – високочастотне (ВЧ) випромінювання схем телефонного сигналу;

11 – ВЧ-нав'язування;

12 – паразитні випромінювання підсилювача;

13 – зняття інформації на автоматичній телефонній станції (АТС);

14 – радіовипромінювання телефонного подовжувача;

15 – перехват інформації з лінії зв’язку;

16 – складна високочутлива апаратура;

17 – виток інформації на лініях відводу від АТС.

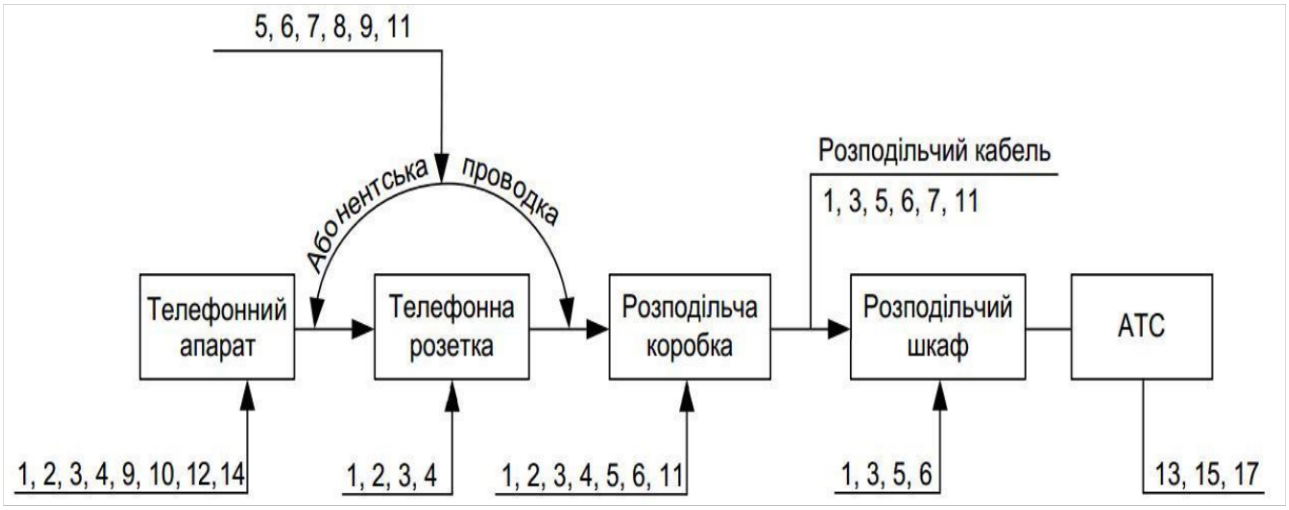


Рисунок 5.1 – Структурно-топологічна схема абонентської телефонної лінії

Можна умовно виділити шість основних зон прослуховування:

- телефонний апарат;
- лінія від телефонного апарата до розподільної коробки;
- кабельна зона;
- зона АТС;
- зона багатоканального кабелю;
- зона радіоканалу.

Найбільш імовірна організація прослуховування перших трьох зон, тому що саме в цих зонах найлегше підключитися до телефонного лінії. Фахівці, що займаються захистом інформації, стверджують, що найчастіше використовується прослуховування за допомогою паралельного апарата. У більшості випадків для цього навіть не потрібно прокладати додаткові проводи – телефонна мережа настільки заплутана, що завжди є невикористані лінії. Крім того, нескладно підключиться до розподільної коробки.

Підключення в третій зоні менш поширено, тому що необхідно проникати в систему телефонних комунікацій, що складається з труб із прокладеними всередині них кабелями, а також розібратися в цій системі й визначити потрібну пару серед сотень інших. Однак не слід вважати, що це нездійсненна задача, оскільки існує вже необхідна для цього апаратура. За допомогою спеціального індуктивного датчика, що охоплює кабель, знімається передана по ньому інформація. Для установки датчика на кабель використовуються колодязі, через які проходить кабель. Датчик у колодязі фіксується на кабелі і для ускладнення виявлення проштовхується в трубу.

Для різних типів підземних кабелів розроблені різні датчики: для симетричних високочастотних – індуктивні для відводу енергії з коаксіальних кабелів, для кабелів з надлишковим тиском – пристрої, що виключають його зниження. Деякі прилади забезпечуються радіопередавачем для передачі записаних повідомлень чи перехоплення їх у реальному масштабі часу.

5.1.1.2. Способи підключення до телефонної лінії

У технічному плані найпростішим способом є контактне підключення. Однак підключення такого типу легко виявляється за допомогою найпростіших засобів контролю напруги телефонної мережі. Зменшити ефект спадання напруги можна шляхом підключенням слухавки через резистор опором 0,6-1 кОм. Підключення здійснюється за допомогою дуже тонких голок і тонких, покритих лаком, проводів, що прокладаються в якій-небудь існуючій чи виготовленій щілині. Щілина може бути зашпакльована і пофарбована так, що візуально визначити підключення дуже важко.

Більш кращим варіантом є підключення за допомогою узгоджувального пристрою (рис. 5.2). Тут Тр – це узгоджувальний трансформатор. Такий спосіб істотно менше знижує напругу в телефонній мережі й ускладнює виявлення факту прослуховування.

Також існує відомий спосіб підключення до ліній зв'язку апаратури з компенсацією спадання напруги (рис. 5.3).

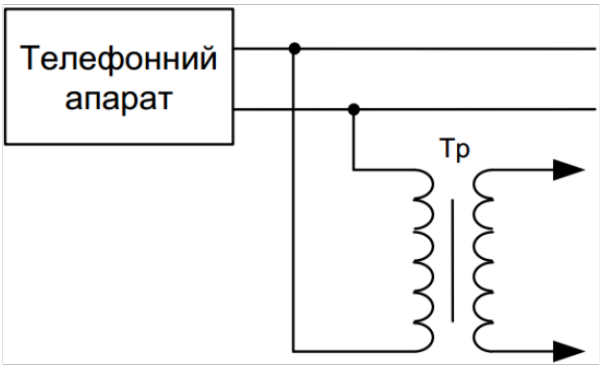


Рисунок 5.2 – Підключення за допомогою узгоджувального пристрою

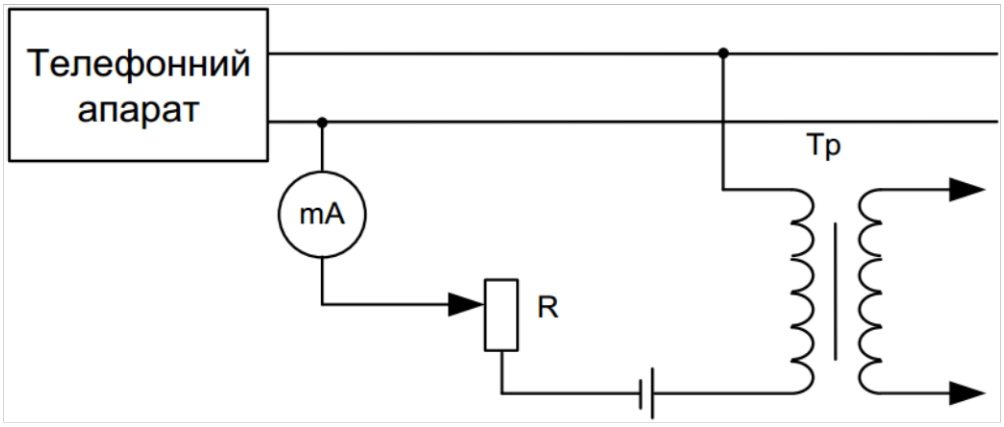


Рисунок 5.3 – Підключення з компенсацією напруги

Істотними недоліками контактного способу підключення є порушення цілісності проводів і вплив підключеного пристрою на характеристики ліній зв'язку. З метою усунення цього недоліку застосовується індуктивний датчик, виконаний у вигляді трансформатора. Існують також датчики, принцип роботи яких заснований на ефекті Холла.

5.1.1.3 Телефонні радіоретранслятори

Телефонні радіоретранслятори (рис. 5.4) являють собою радіоподовжувачі для передачі телефонних розмов по радіоканалах. Більшість телефонних закладок автоматично включаються при піднятті слухавки і передають інформацію до пункту перехоплення і запису. Джерелом живлення для радіопередавача зазвичай є напруга телефонної мережі. Недоліком подібних пристроїв є те, що вони можуть бути виявлені за радіовипромінюванням.

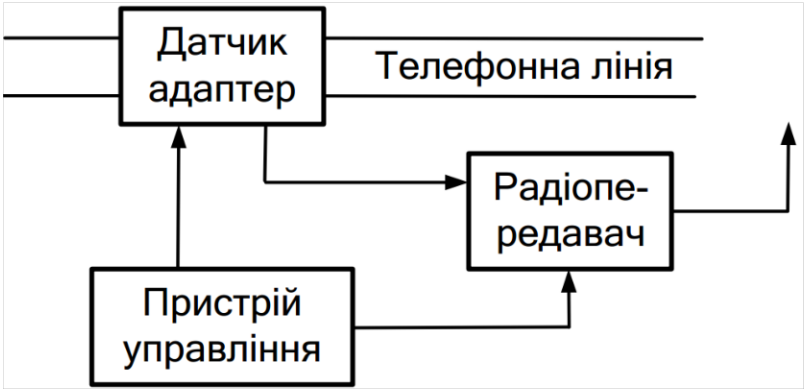


Рисунок 5.4 – Структурна схема радіоретранслятора

Щоб зменшити можливість виявлення радіовипромінювання зменшують потужність випромінювання передавача, установленого на телефонній лінії. А в безпечному місці встановлюють більш потужний ретранслятор, що перевипромінює сигнал на іншій частоті та у зашифрованому вигляді. З метою маскування телефонні радіоретранслятори випускаються у вигляді конденсаторів, фільтрів, реле та інших стандартних елементів, що входять до складу телефонної апаратури. Існують навіть ретранслятори, виконані у вигляді мікрофона слухавки. Подібні вироби дуже легко і швидко можна встановити в телефонний апарат суб’єкта прослуховування.

5.1.1.4. Використання телефонної лінії для прослуховування приміщень

Телефонна лінія використовується не тільки для передачі телефонних повідомлень, але і для прослуховування приміщення (рис. 5.5). Щоб увімкнути такий пристрій, потрібно набрати номер абонента. Перший гудок "ковтається" пристроєм, тобто телефон не дзвонить. Після цього необхідно покласти трубку і через визначений час (30-60 сек.) подзвонити знову. Тільки після цього система включається в режим прослуховування.

Для розуміння фізики процесів, які виникають при цьому, розглянемо види акустичних перетворень, що дозволяють перехоплювати інформацію. Як відомо, під час розмови утворюються звукова хвиля, яка може викликати механічні коливання елементів електричної апаратури, що в свою чергу

приводить до появи електромагнітного випромінювання. Види акустоелектричних перетворювань наведені на рис. 5.6.

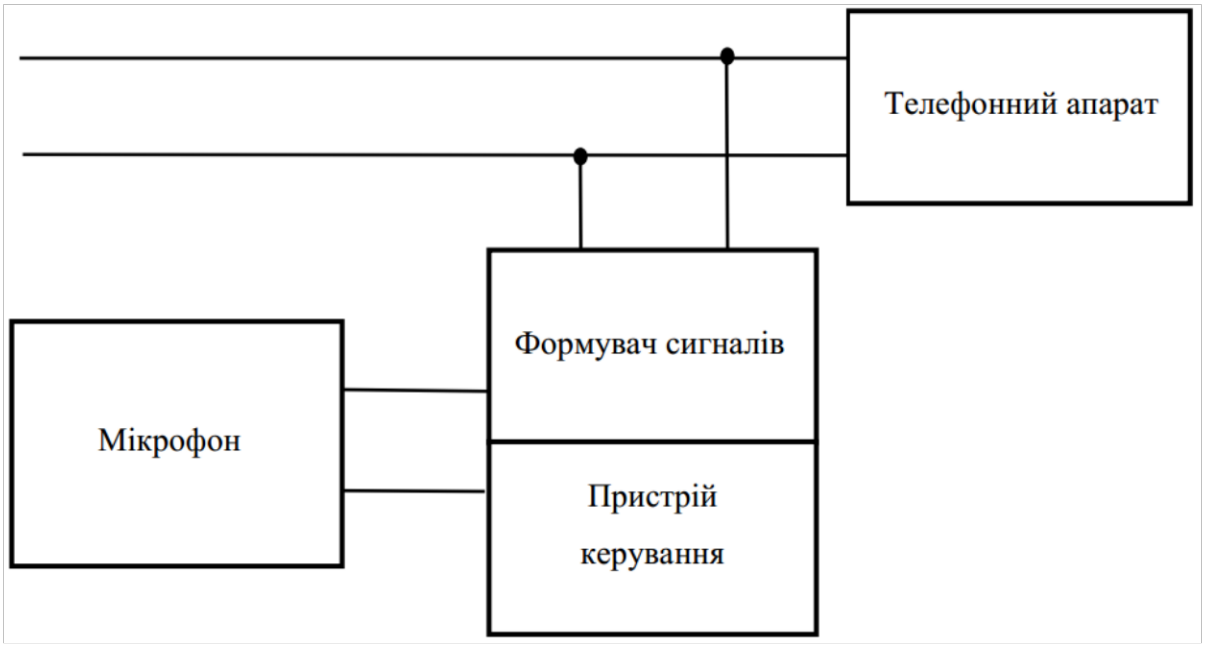


Рисунок 5.5 – Використання телефонної лінії для прослуховування приміщень

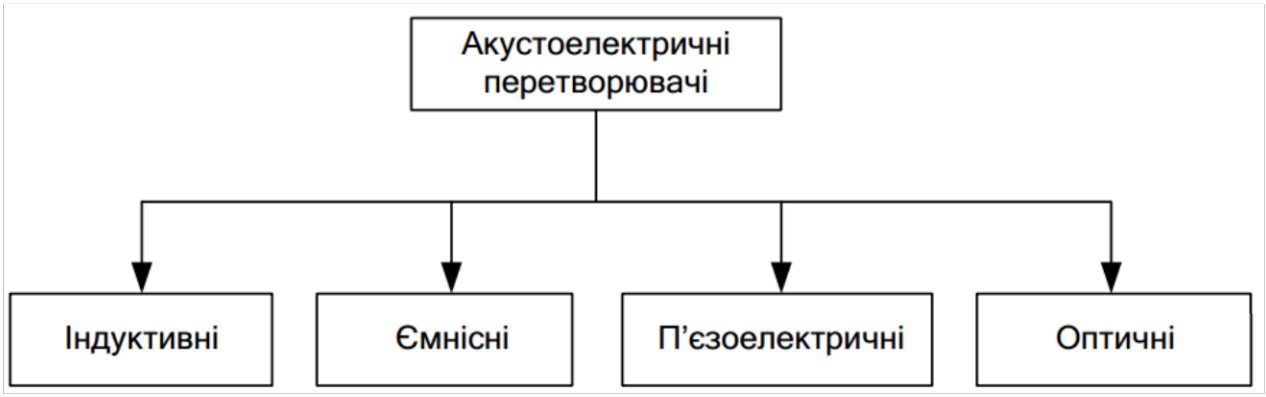


Рисунок 5.6 – Види акустоелектричних перетворень

5.1.2. Пристрої захисту інформації в телекомунікаційних системах

5.1.2.1 Принципи захисту інформації в приміщеннях та мережах телефонного зв'язку

Апаратуру захисту телефонних мереж можна умовно розділити на дві підгрупи: апаратуру контролю та апаратуру захисту ліній зв'язку.

До апаратури контролю ліній зв'язку відносяться:

– аналізатори та індикаторні пристрої;

– кабельні локатори (рефлектометри та прилади, які використовують принципи

– нелінійної локації);

– детектори поля, частотоміри, спеціальні радіоприймальні пристрої та універсальні комплекси контролю.

До апаратури захисту ліній зв‘язку відносяться:

– багатофункціональні пристрої захисту телефонних ліній;

– пристрої знищення закладок;

– апаратура криптозахисту;

– пристрої захисту від піратських підключень;

– апаратура лінійного та просторового шумоутворення;

– апаратура захисту від ВЧ - нав‘язування.

5.1.2.2. Пристрої захисту телефонних апаратів.

При організації захисту телефонних ліній необхідно враховувати наступні фактори:

– телефонні апарати можуть використовуватись для підслуховування переговорів, що ведуться в приміщенні, де вони встановлені;

– прослуховування телефонних розмов можливе через безпосереднє підключення до телефонного апарату, шляхом прийому та обробки випромінювання електромагнітних хвиль телефонним апаратом у простір, в телефонну або енергетичну лінію;

– використання мікрофонного ефекту та ефекту високочастотного нав’язування для зняття інформаційного сигналу з телефонного апарату при покладеній трубці.

Крім цього, телефонні лінії, що проходять в приміщенні можуть використовуватись в якості:

– лінії для передачі отриманої інформації;

– джерела живлення для пристроїв зняття інформації;

– дистанційного керування пристроями зняття інформації.

Як наслідок методи та пристрої захисту телефонних апаратів телефонних ліній повинні бути направлені на виключення:

- використання телефонних апаратів та ліній для прослуховування переговорів, що ведуться у приміщенні;
- безпосереднього прослуховування телефонних апаратів;
- несанкціонованого використання телефонної лінії.

Загалом, всі методи захисту телефонного зв'язку поділяються на:

- організаційно-технічні;
- технічні;
- контролю стану.

Технічні методи захисту поділяються на:

- криптографічні;
- інженерно-технічні.

А інженерно-технічні методи в свою чергу поділяються на:

- активні;
- пасивні;
- комбіновані.

До ***пасивних методів*** захисту телефонних ліній зв’язку відносяться:

- амплітудне обмеження небезпечних сигналів;
- фільтрація небезпечних сигналів;
- відключення джерел небезпечних сигналів.

Амплітудне обмеження основане на використанні схем амплітудних обмежувачів на діодах. Завдяки вольт-амперній характеристиці діодів слабкі небезпечні сигнали обмежуються і сильно ослабляються.

Як будь-який електронний пристрій, телефонний і факсимільний апарати, концентратор і з'єднуючі його лінії створюють у відкритому просторі досить високі рівні випромінювання в діапазоні частот аж до 150 МГц. Завдяки малим розмірам джерела випромінювання і, отже, незначній довжині його внутрішніх монтажних проводів, рівень випромінювання самого апарата швидко зменшується відповідно до віддалення від нього. Крім того, несиметричний

внутрішній опір телефонного апарата як джерела випромінювання щодо землі завжди значно більше аналогічного опору телефонної лінії.

Унаслідок цієї напруги випромінювання в провідних лініях, обмірювані між ними і землею, звичайно бувають менше, ніж аналогічні напруги, вимірювані між лінійними проводами і корпусом телефонного апарата. Для того щоб цілком придушити усі види випромінювань, створювані телефонними апаратами, необхідно відфільтрувати випромінювання в лінійних проводах, що відходять від апаратів, і проводах мікротелефону, а також забезпечити достатній захист внутрішньої схеми телефонного апарата. Це можливо тільки при значній схемній переробці телефонних апаратів і зміні їхніх електричних параметрів. Зі сказаного випливає, що для того, щоб захистити телефонний апарат, необхідно захистити ланцюг мікрофона, ланцюг дзвоника, двох провідну лінію телефонного зв'язку

Активні методи захисту телефонних ліній зв’язку від витоку інформації включають в себе:

- використання завад у смузі частот голосового каналу (100 Гц... 10 кГц) − метод синфазної низькочастотної маскуючої перешкоди, яка нейтралізується на боці абонента, але заважає прослуховуванню при підключенні до одного дроту телефонної лінії;
- використання пригнічуючих завад поза смугою частот голосового каналу − маскування розмови сигналом на ультразвукових частотах;
- використання низькочастотної шумової завади маскування при покладеній слухавці;
- підвищення напруги телефонної лінії (випалювання зловмисного обладнання);
- подача на лінію напруги зворотної полярності;
- використання комплексних систем захисту.

Комбіновані методи захисту поєднують в себе можливості як пасивних, так і активних методів захисту.

5.1.2.3. Аналізатори телефонних ліній

Принцип дії аналізаторів мереж телефонного зв'язку базується на виявленні підключень до енергонесучих ліній.

Прилади однієї з груп аналізаторів телефонних ліній можуть бути орієнтовані на установку і безупинну роботу безпосередньо в тих енергонесучих лініях (телефонна, енергопостачання, радіотрансляція), у яких необхідно своєчасне виявлення факту підключення пристроїв несанкціонованого з'йому інформації (ПНЗІ). У цьому випадку в сучасних розробках усі методики перевірки ліній реалізуються автоматично за програмою, що керує роботою мікропроцесора аналізатора. У випадку появи ознак розпізнавання несанкціонованого підключення, прилад формує спеціальний сигнал і при необхідності включає захист. За запитом зовнішньої ЕОМ такі прилади можуть видавати протокол, що містить результати спостереження за станом лінії. Деякі моделі оснащуються пристроями безупинного запису переговорів, що ведуться в контрольованій телефонній лінії.

Інший напрямок цієї ж (першої) групи приладів — для проведення спеціальних перевірок при періодичних вимірах. У таких випадках імовірність правильного виявлення стає залежною як від метрологічних характеристик приладу, так і від мистецтва оператора. Періодичній перевірці можуть піддаватися відсіки, шахти, люки чи траси, розподільні щити, де встановлення постійних приладів контролю з різних причин неможливе.

Для того, щоб полегшити виявлення грубих підключень навіть некваліфікованим користувачем, у першій групі приладів розроблені пристрої, які відображають відхилення напруги від установлених значень. Найбільш прості з них не мають індикації значень напруги чи струму і дозволяють тільки контролювати відхилення напруги від заданого, подаючи сигнал при несанкціонованому підключенні. Значення заданої напруги встановлюється вручну, за допомогою елементів налаштування. Звільняючи користувача від процедури ведення журналу вимірів, такі прилади на практиці можуть знайти

тільки "грубі" вторгнення, подібні до зняття трубки на паралельному телефоні, і не вирішують ані задачі виявлення сучасних ПНЗІ, ані задачі їхнього придушення.

Структурні схеми подібних пристроїв наведені на рис. 5.7.

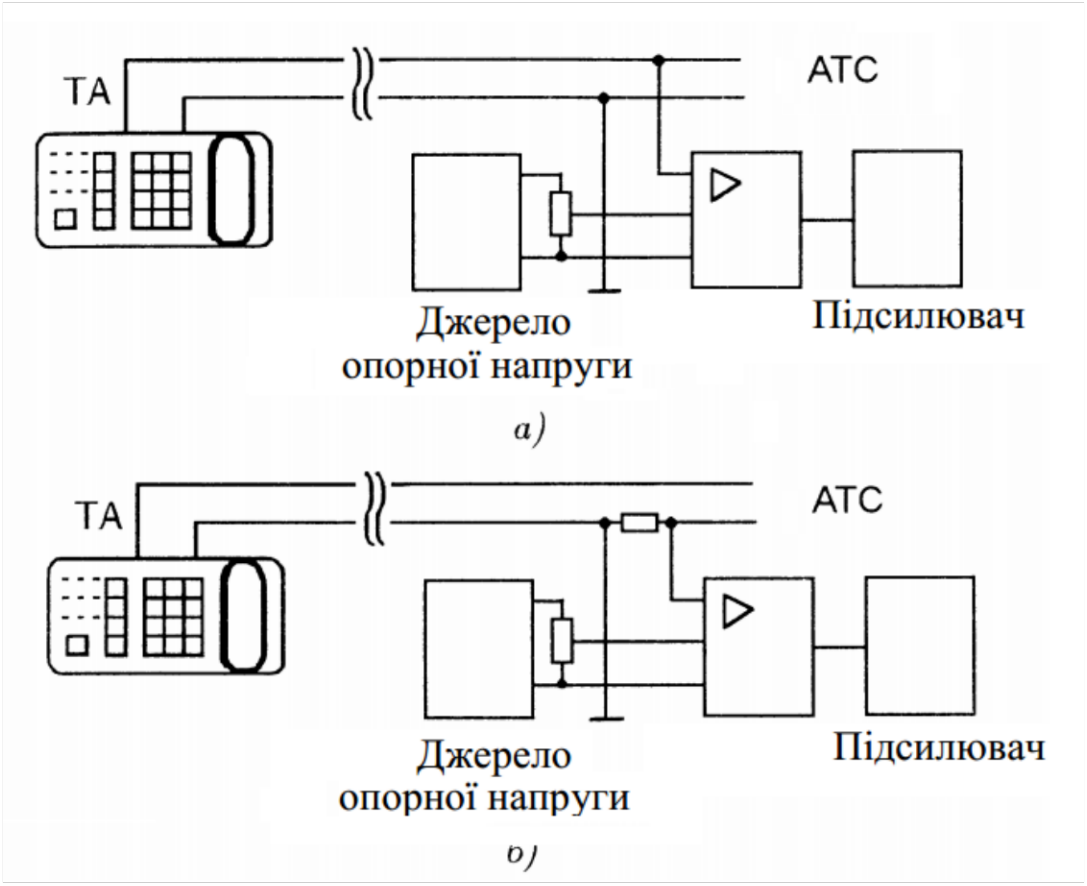


Рисунок 5.7 – Пристрій контролю телефонної лінії: а – напруги; б – струму

Пристрій, вказаний на рис. 5.7, а, дозволяє уловити момент зменшення напруги в лінії. Він може бути налаштований як на напругу у лінії за умови, що слухавка покладена, так і на напругу в лінії при знятій слухавці. Пристрій, показаний на рис. 5.7, б, має у своєму складі шунт і дозволяє уловити момент, коли струм, що протікає через телефонний апарат (ТА) при розмові, стає менше норми.

В табл. 5.1 наведені приклади падіння напруги на лінії при підключенні деяких типів телефонних радіозакладок.

Таблиця 5.1 – Падіння напруги на лінії при підключенні радіозакладок

Тип радіозакладки	Напруга в лінії					
	Трубка покладена			Трубка знята		
	U, В	DU, В	DU,%	U, В	DU, В	DU %
Закладки немає	63.7	**0**	0.00	10.4	**0**	0.00
З послідовним включенням, параметрична стабілізація частоти (f = 140 Мгц)	63.2	**- 0.5**	- 0.78	9.9	**- 0.5**	- 4.81
З послідовним включенням, кварцева стабілізація частоти (f = 140 Мгц)	61.8	**- 1.9**	- 2.98	10	**- 0.4**	- 3.85
З послідовним включенням, кварцева стабілізація частоти (f = 472 Мгц)	62.5	**- 1.2**	- 1.88	9.7	**- 0.7**	- 6.73
З паралельним включенням, кварцева стабілізація частоти (f = 640 Мгц)	61.7	**- 2**	- 3.14	9.3	**- 1.1**	- 10.58
Комбінована з паралельним включенням, параметрична стабілізація частоти (f = 140 Мгц)	61.9	**- 1.8**	- 2.83	10.3	**- 0.1**	- 0.96
Комбінована з паралельним включенням, кварцева стабілізація частоти (f = 420 Мгц)	62.1	**- 1.6**	- 2.51	9.4	**- 1**	- 9.62
"Телефонне вухо"	60	**- 3.7**	- 5.81	-	**-**	-

Асортимент і конструктивне виконання приладів для контролю і проведення вимірів параметрів лінії при пошуку пристроїв несанкціонованого доступу досить різноманітні. Усі пристрої критичні до заміни типу ТА.

Інший клас приладів призначений для вимірів і реєстрації показань у журналі.

Наявні моделі приладів найчастіше дозволяють вимірювати тільки напругу в телефонній лінії при покладеній і знятій слухавці. Практично такі прилади дозволяють вирішувати задачу виявлення лише частково, а обов'язковою умовою вірогідності результатів, одержуваних з їхньою допомогою, є використання при вимірах того самого ТА. Недотримання цієї вимоги приведе до додаткових погрішностей, обумовлених значним розкидом параметрів різних ТА.

Виявлення ланцюгів живлення пристроїв несанкціонованого підключення до телефонних ліній і мереж електропостачання, включених послідовно з опором не менш 5 Ом, пристроїв, включених паралельно з опором не більш 1,5

МОм, може проводитися на екрані пристрою за зображенням сигналу, що зондує лінію.

Завдяки наочності зображення оператор легко може виявляти пристрої, що володіють підвищеною вхідною ємністю чи мають нелінійні елементи в ланцюгах живлення – діоди, тиристорні чи транзисторні ключі.

5.2. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи, розв'язати задачі.

5.2.1. Задача 1

Відповідно до узагальненої структурно-топологічної схеми абонентської телефонної лінії (рис. 5.1) та нумерованого переліку місць можливого витоку та перехоплення інформації (пп. 5.1.1.1. теоретичних відомостей) згідно свого варіанту (табл. 5.2) знайдіть ті ділянки абонентської телефонної лінії, на яких можливі витоки інформації такого типу, як вказано для вашого варіанту (табл. 5.2).

Тобто надайте перелік всіх ділянок телефонної лінії (як вони названі на рис. 5.1), на яких можливі витоки інформації даного типу.

Таблиця 5.2 – Варіанти завдань до Задачі 1 Лабораторної роботи 5

№ з/п	Різновиди витоку інформації
1.	Радіовипромінювання телефонного подовжувача
2.	Паразитні випромінювання підсилювача
3.	Високочастотне (ВЧ) випромінювання схем телефонного сигналу
4.	Акустоелектричне перетворення
5.	Виток інформації на лініях відводу від АТС
6.	Радіовипромінювання телефонного подовжувача
7.	Паразитні випромінювання підсилювача
8.	Високочастотне (ВЧ) випромінювання схем телефонного сигналу
9.	Акустоелектричне перетворення
10.	Наводки телефонного сигналу на інші кола

5.2.2. Задача 2

Відповідно до узагальненої структурно-топологічної схеми абонентської телефонної лінії (рис. 5.1) та нумерованого переліку місць можливого витоку та перехоплення інформації (пп. 5.1.1.1. теоретичних відомостей) знайдіть ті ділянки абонентської телефонної лінії, на яких зловмисники можуть використовувати засоби несанкціонованого перехоплення, що вказані для вашого варіанту (табл. 5.3).

Тобто надайте перелік всіх ділянок телефонної лінії (як вони названі на рис. 5.1), на яких можуть бути використані дані засоби перехоплення.

Таблиця 5.3 – Варіанти завдань до Задачі 2 Лабораторної роботи 5

№ з/п	Засоби несанкціонованого перехоплення
1.	Радіозакладки паралельного та послідовного підключення
2.	Будь-які радіо закладки
3.	Комбінована телефонно-акустична радіозакладка
4.	Закладка типу "довге вухо"
5.	Метод ВЧ-нав’язування
6.	Будь-який адаптер
7.	Низькоомний або високоомний адаптер
8.	Безконтактний адаптер
9.	Перехват інформації з лінії зв’язку
10.	Зняття інформації на автоматичній телефонній станції (АТС)

5.3. Питання до самоконтролю

1. Які методи прослуховування телефонних ліній ви можете назвати?
2. На які групи поділяються інженерно-технічні методи захисту телефонного зв'язку?
3. До якої групи інженерно-технічних методів захисту телефонних ліній зв’язку відноситься метод випалювання зловмисного обладнання?
4. До якої групи інженерно-технічних методів захисту телефонних ліній зв’язку відноситься фільтрація небезпечних сигналів?
5. Що таке аналізатор телефонних ліній?

5.4. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

5.5. Література до Лабораторної роботи 5

Рекомендовані літературні джерела до виконання Лабораторної роботи 5: [1, 2, 11].

ЛАБОРАТОРНА РОБОТА 6. БЕЗПЕКА МОБІЛЬНОГО ЗВ'ЯЗКУ

Мета роботи: набуття навичок захисту інформації та безпечного використання засобів мобільного зв'язку та мобільних пристроїв.

6.1. Теоретичний матеріал до лабораторної роботи

6.1.1. Загальні міркування

Умови 21 століття вимагають активного використання мобільних інформаційних технологій та пристроїв (гаджетів). Щоденним супутником сучасної людини є мобільний телефон (смартфон). Але з поширенням використання мобільних пристроїв зростає і небезпека витоку та втрати даних. Тому кожному користувачеві варто дбати про належний рівень безпеки (кібербезпеки) мобільних цифрових пристроїв.

Перш за все, всім користувачам, які користуються мобільними телефонами, а особливо смартфонами, важливо розуміти, що пристрій, який вони носять у себе у кишені, є повнофункціональним комп'ютером з функцією постійного доступу до мережі Інтернет, мікрофоном, камерою, GPS-навігатором. Тому для смартфонів характерні ті ж самі загрози, що існують для персональних комп'ютерів – "троянські" та шпигунські програми, інше шкідливе програмне забезпечення, крадіжка конфіденційної інформації. Існують для мобільних пристроїв також і специфічні додаткові загрози – шпигунство за користувачами смартфонів, крадіжка грошей з мобільних рахунків тощо.

6.1.2. Шкідливе програмне забезпечення для мобільних пристроїв

Першим шкідливим засобом проти мобільних телефонів були шкідливі SMS-повідомлення. На телефонний номер користувача приходило певне SMS-повідомлення, відкриття якого призводило до збою роботи телефону. Атака могла призвести до зависання телефону, була спроможна «обнулити» телефонну книгу, здійснити певний дзвінок, тобто телефон виконував якусь непотрібну користувачу функцію. Згодом з'явились повноцінні віруси та

хробаки. Перші віруси були виявлені ще на комунікаторах під управлінням мобільних операційних систем Palm OS, Windows CE, Windows Mobile. Далі їм на заміну прийшов Symbian, для якого також було створено досить багато шкідливих програм, мережевих хробаків, що мали можливість розповсюджуватись від одного пристрою до іншого використовуючи Bluetooth з'єднання і виконувати шкідливі дії.

На той час розповсюдження хробаків було в основному побудовано на методах соціальної інженерії. Приклад – смартфон на базі Symbian, заражений хробаком, що розповсюджується через Bluetooth. Радіус дії Bluetooth передачі 10-15 метрів, при цьому автоматичної передачі не відбувається. Заражений смартфон сканував оточення знаходив інші телефони із увімкненим Bluetooth і намагався їм розіслати копії себе. Звичайний користувач перебував у метро чи кафе і бачив на телефоні пропозицію прийняти певний файл. Ця ситуація була не висвітлена у ЗМІ і звичайної цікавості вистачало щоби прийняти файл, тим більше він міг цікаво називатись. Людина приймала файл, відкривала його і якщо приймаючий прилад був на базі Symbian, хробак активізувався, заражав пристрій і потім заражав інших, виконуючи нову розсилку.

Перші модифікації хробака просто розмножувались і наносили певну шкоду, блокуючи деякі додатки у смартфоні. Більш пізніші модифікації вже намагались заробляти кошти зловмисникам – шкідлива програма вже мала нову функцію – відправку SMS-повідомлень на платні номери. Для цього зловмисники реєстрували короткі платні номери, за відправлення на які SMS-повідомлень з користувача знімалися певні кошти. І троянська програма з зараженого пристрою відправляла sms-повідомлення, а зловмисники таким чином отримували зиск.

Згодом мобільні пристрої почали отримувати більше можливостей з'єднання з мережею Інтернет. Спочатку це були технології WAP та GPRS, потім з'явились мережі 3G, далі – Wi-Fi з'єднання. На сьогодні існує багато місць, де можна отримати доступ до глобальної мережі через Wi-Fi, така можливість присутня майже всюди: вдома, в офісах, в метро, в кафе, і т.п.

Маючи доступ до Інтернет хробаки отримали можливість, перш за все, більш швидко розповсюджуватись через електронну пошту, веб-сайти і наносити більш суттєву шкоду, адже вони вже могли не тільки відправляти платні SMS-повідомлення, але й красти дані кредитних карток, про акаунти в соціальних мережах, електронній пошті тощо. Віруси для мобільних пристроїв отримали всі ті властивості, що притаманні класичним шкідливим програмам для персональних комп'ютерів.

Подібно до персональних комп'ютерів існує багато троянських програм, що заражаючи телефон, перетворюючі його на бота, формуючи бот-мережу. Існують бот-нети на основі мобільних пристроїв. Таким чином DDoS-атаки на сайти можуть проводитись не тільки з заражених комп'ютерів, але й з заражених смартфонів, які по суті також є комп'ютерами, але які ми постійно носимо з собою.

Класичні віруси для мобільних пристроїв майже не розробляються. Переважно для мобільних пристроїв розробляють троянські програми, рекламні модулі та бекдор-програми, які дозволяють обійти автентифікацію.

Варто розуміти, що шкідливі програмні засоби створюються для всіх операційних систем, на які можна встановити додаткове програмне забезпечення. Якщо в телефон можна встановити додаткові програми, то туди може потрапити також шкідлива програма. Якщо вона не потрапить туди самостійно, автоматично, то програма може зробити це за допомогою користувача методами соціальної інженерії. Наприклад, власнику смартфони пропонують встановити цікаву гру, яка також виконує шкідливі функції. Або вона навіть не буде маскуватись під гру, а одразу почне надсилати SMS-повідомлення на короткі номери. Тільки пристрої з повною забороною на встановлення додаткового ПЗ є захищеними. Існують віруси навіть для операційної системи iOS (мобільна операційна система від Apple).

Ще один аспект загроз для користувачів мобільних телефонів полягає у моделі роботи з платними послугами, що можуть бути не зовсім зрозумілі користувачу. Тобто користувача можуть ввести в оману попросивши набрати

певний номер, надіслати SMS-повідомлення. У всіх цих випадках з мобільного рахунку знімаються певні кошти. Також дуже популярною є послуга SMS-підписок, коли користувачу пропонують підписатись на певний сервіс за допомогою SMS-повідомлень. Це може бути все що завгодно: підписка на онлайн гру, певний сайт, якийсь сервіс, що вимагає регулярну оплату. У подальшому користувач може забути про це. З мобільного рахунку періодично буде зніматись певна сума, власник якого навіть не буде цього помічати.

6.1.3. Шпигунські засоби

Існує багато легальних програмних додатків, які по суті є шпигунськими засобами. Такі програми мають офіційного власника, фірменний сайт, забезпечення технічною підтримкою. Встановлюючи такий додаток на свій мобільний пристрій користувач дозволяє повноцінно стежити за ним, а саме – перехоплювати інформацію про дзвінки, вміст SMS-листування, показувати інформацію про відвідувані сайти, знімати за допомогою камери телефону оточуючу ситуацію, визначати місце розташування, сканувати Bluetooth чи Wi-Fi оточення, включати мікрофон і записувати аудіодані з його оточення.

Але встановлення подібного додатку на телефон користувача дозволяє шпигувати не тільки за діями в самому телефоні, але й відслідковувати фізичні переміщення користувача, адже мобільний телефон практично завжди знаходиться поруч з його власником.

6.2. Кібербезпека смартфонів та мобільних пристроїв

6.2.1. Рівні безпеки смартфонів

Можна розрізнити два основні рівні захисту смартфона:

- фізичний захист;
- захист інформації.

6.2.1.1. Фізичний захист

Сюди входять базові правила поводження з мобільним телефоном. Наприклад, не варто залишати його без нагляду, вводити код доступу на очах у

інших людей чи носити смартфон в задній кишені. Адже хтось може "зламати" ваш пристрій та використати його у власних інтересах, наприклад спустошити рахунки, підв'язані до смартфона, отримати бажані дані чи видалити потрібну вам інформацію. В найгіршому випадку, телефон буде викрадено.

6.2.1.2. Захист інформації

Захист інформації – це захист операційної системи, програм та інших застосунків. Існує багато способів захистити смартфон від таких ризиків. Насамперед це – вчасне оновлення операційної системи, використання багатофакторної автентифікації та складних паролів.

6.2.2. Основні правила мобільної кібербезпеки

6.2.2.1. Вчасне оновлення операційної системи мобільного пристрою

Компанії-виробники смартфонів постійно оновлюють їх системне програмне забезпечення. Такі оновлення найчастіше виправляють усі виявлені вразливості операційних систем, запобігають витоку даних користувача, блокують несанкціоновані доступи тощо. 90% оновлень усіх операційних систем включають поліпшення заходів безпеки. Деякі компанії приділяють окрему увагу питанню захисту смартфонів. Наприклад, Samsung випустила сервіс Knox, який виводить безпеку смартфона Samsung на принципово новий рівень захисту даних. Це мобільна платформа безпеки, розроблена для компаній з розвиненою системою корпоративної мобільності. Knox пропонує:

- віддалене налаштування великої кількості пристроїв Samsung та їхню адаптацію до конкретних потреб;
- одночасне додавання тисяч пристроїв в EMM без необхідності вручну реєструвати кожен пристрій;
- просте керування безліччю пристроїв за допомогою хмарного рішення EMM;
- застосування комплексних функцій захисту та керування для корпоративних пристроїв;

– керування версіями ОС на мобільних пристроях Samsung для максимальної економічної ефективності.

6.2.2.2. Використання складних паролів та менеджерів паролів

Перш за все, не варто застосовувати однакові паролі для різних сервісів. Це те ж саме, що мати один ключ для автомобіля, будинку і сейфа. Якщо пароль розгадають або підберуть, то постраждають усі сервіси, де використовувалася ця комбінація символів. Рекомендується обирати справді важкі паролі, які складаються з комбінації різних символів та чисел. Адже, дізнатися дівоче прізвище мами чи ім'я домашнього улюбленця можна дуже швидко. Більше того, для таких дій використовується аналіз вашого профілю в соціальних мережах (соціальна інженерія). Тому намагайтеся не використовувати стандартні типи питань, пропоновані сервісом, а будьте оригінальними. Обирайте паролі з 8 символів, до того ж це повинні бути і букви (великі і маленькі), і спеціальні знаки, і числа. Крім того, рекомендуємо користуватися менеджером паролів. Це спеціальні сервіси і додатки, які зберігають логіни і паролі в зашифрованому вигляді. Адже, запам'ятати всі складні паролі практично неможливо. Доступ до таких менеджерів паролів найчастіше має максимальний рівень захисту з використанням і паролів, і кодів SMS, і відбитків пальців, повністю відповідаючи правилам багатофакторної автентифікації.

6.2.2.3. Використання багатофакторної автентифікації

Використовуйте двофакторну (або багатофакторну) аутентифікацію всюди, де це можливо. Під двофакторною автентифікацією мається на увазі захист за допомогою 2-х паролів з різними каналами доступу. Наприклад, отримання захисного коду в SMS на смартфон після введення логіна і пароля. В цьому випадку, навіть якщо хтось дізнається ваш логін і пароль, то все одно не отримає доступу до смартфона і не зможе отримати код SMS, отже і не увійде до профілю. Іноді замість SMS-повідомлень для доступу використовуються програми-месенджери (Viber, Telegram та ін.). До того ж, фахівці з кібербезпеки

радять захистити особистий мобільний номер, зробивши його прив'язку до своїх даних у оператора мобільного зв'язку.

6.2.2.4. Використання біометричного захисту

Рекомендується користуватися додатковим захистом – з використанням відбитку пальців або сканування особистості (faceID для IOS). Щоб заблокувати доступ до телефону, не обов'язково використовувати паролі і пін-коди, вони не завжди можуть надати належний захист даних. Набагато безпечніше застосовувати біометричну ідентифікацію. Це досить надійний і комфортний інструмент. Крім того, сьогодні майже усі смартфони надають таку можливість.

6.2.2.5. Встановлення додатків лише з офіційних джерел

Не рекомендується завантажувати та встановлювати програми для смартфонів з невідомих джерел. Часто самі операційні системи, встановлені в смартфонах, не дозволяють (або попереджають про небезпеку) інсталювати таке програмне забезпечення. ОС обмежує користувача тільки своїми додатками з офіційного магазину – App Store, Google Play, Galaxy Store, AppGallery та ін. Безпечним також є скачування додатків з офіційних сайтів виробника. Часто, встановлюючи додатки з інших джерел (наприклад, піратські версії платних програм), ви встановлюєте і віруси чи інші шкідливі дані. Особливо проблемним це явище є для смартфонів на Android OS. Проте, навіть завантажуючи застосунок з офіційного магазину, слід перевірити усі доступні дані, такі як інформація про розробників, доступи, які додаток вимагає при встановленні, відгуки користувачів.

6.2.2.6. Користування лише відомими, безпечними Wi-Fi мережами

Відкриті, загальнодоступні мережі Wi-Fi небезпечні для використання, адже через них можна отримати доступ до смартфона чи інших гаджетів. Часто зловмисники створюють точки доступу з назвами, ідентичними до тих, які пропонують заклади. Таким чином шахраї можуть отримати доступ до електронної пошти, акаунтів у соціальних мережах, персональних даних та

навіть банківських карток. Також, при підключенні до таких мереж, вас можуть попросити перейти за посиланням чи натиснути якусь кнопку, це може бути ознакою шахрайства. Рекомендуємо користуватись мобільними даними в загальнодоступних місцях або, принаймні, користуватися VPN.

6.2.2.7. Встановлення додаткового захисту

В якості додаткового захисту варто використовувати антивірусне програмне забезпечення. Зазвичай воно вже встановлене у смартфоні. Проте не варто встановлювати одразу кілька таких застосунків, адже вони почнуть конфліктувати між собою, що призведе до проблем у роботі пристрою. Також рекомендується вмикати усі доступні "захисти", які пропонує операційна система та застосунки смартфона, наприклад, в розділі "Конфіденційність". Варто зберігати дані у безпечній хмарі, ізольованій від решти системи; вона забезпечує додатковий захист даних навіть у разі злому чи втрати смартфона.

6.2.2.8. Постійне увімкнення геолокації

Не варто відключати геолокацію, хоча часто користувачі бажають приховати місце свого розташування. Адже з допомогою додаткових сервісів можна локалізувати викрадений або загублений телефон. Наприклад, Google розробила для таких випадків сервіс Find My Phone для Android. Він не тільки дозволяє активувати дзвінок (навіть якщо до цього гаджет був поставлений на беззвучний режим), але й заблокувати пристрій і видалити всі особисті дані на ньому. Іншими словами, власник телефону зможе самостійно контролювати його навіть на відстані. Єдине що для цього потрібно – підключення до Інтернету.

6.3. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи та виконати наступне завдання.

6.3.1. Завдання

1. Користуючись пошуковою системою, знайдіть інформацію про антивірусне програмне забезпечення, яке може бути встановлено на ваш мобільний телефон. Наведіть у звіті назву, короткий опис, можливості та особливості даного програмного продукту.

2. Користуючись пошуковою системою, знайдіть та наведіть у звіті відомості про резонансні випадки втрати інформації через мобільний телефон (не менш за 2 випадки).

3. Користуючись пошуковою системою, знайдіть інформацію про кілька відомих вірусів для мобільних телефонів. Наведіть у звіті їх назви, особливості, опишіть шкоду, яку вони можуть завдати мобільному пристрою.

6.4. Питання до самоконтролю

1. Назвіть причини втрати інформації на мобільних телефонах.

2. Що називається мобільним вірусом?

3. З якою метою створюється шкідливе програмне забезпечення для мобільних пристроїв?

4. Який антивірус може бути встановлений на ваш мобільний телефон? Які його основні властивості?

5. Які вам відомі вірусні програми, що спрямовані на ураження мобільного телефону?

6. Якими правилам з пункту 6.2.2 ви користуєтесь постійно? Користь від яких, якщо є такі, вважаєте недостатньою порівняно з загрозами від їх здійснення? Чому?

6.5. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

6.6. Література до Лабораторної роботи 6

Рекомендовані літературні джерела до виконання Лабораторної роботи 6: [1, 2, 12-14].

ЛАБОРАТОРНА РОБОТА 7. БЕЗПЕКА ВОЛОКОННО-ОПТИЧНИХ ЛІНІЙ ЗВ'ЯЗКУ

Мета роботи: набуття навичок захисту інформації у волоконно-оптичних лініях зв'язку.

7.1. Теоретичний матеріал до лабораторної роботи

7.1.1. Історична довідка

Застосування світла в якості носія інформації використовувалося ще в стародавні часи. В загальному випадку передача інформації за допомогою світла потребує наявності наступних компонентів: джерело інформації, оптичний передавач, середовище розповсюдження сигналу і приймач інформації.

Розробка оптичного волокна почалася у 1951 році. Перші дослідження на предмет створення ліній зв'язку на основі оптичних діелектричних волокон були розпочаті вченими Косинським, Кузмічевим, Власовим та іншими. Але в той час майже ніхто не вбачав практичну користь цих досліджень.

Експерименти зі світлопоглинання скла розпочалися у 1958 році. Варгін і Вайнберг довели, що на цю величину впливають домішки кольорових металів, внесеними шихтою і вогнетривами. Було визначено, що світлопоглинання ідеально чистого скла дуже мале. Тому у 1963 році були створені перші світловоди, що мали довжину всього у кілька метрів. На той час постала проблема великих втрат в оптоволокні. У 1970 на кілометровій ділянці енергія зменшується в 100 разів, що складає 20 дБ на 1 км втрат. На практиці це підтвердив інженер відомої американської фірми «Corning Glass» Капроні і його співробітники, які прослідкували втрати на реальних світловодах. З цього часу почався стрімкий розвиток у галузі волоконної оптики. Тому часто саме 1970 рік вважається початком епохи волоконно-оптичного зв'язку, одного з найвидатніших технічних досягнень XX століття.

7.1.2. Основні принципи волоконно-оптичної передачі інформації

Якісний опис процесу поширення хвиль в оптичному волокні (ОВ) надає променева теорія, яка дозволяє також отримати деякі важливі кількісні оцінки. Більш повний і чіткий опис хвиль в ОВ забезпечує теорія електромагнітного поля.

Суть явища заломлення світла полягає у наступному (рис. 7.1). Коли промінь світла входить під кутом падіння α в оптично більш щільне середовище (наприклад, скло або воду) з оптично менш густого середовища (наприклад, повітря), то його напрямок поширення щодо нормалі до поверхні падіння змінюється, тобто він переломлюється під кутом заломлення β.

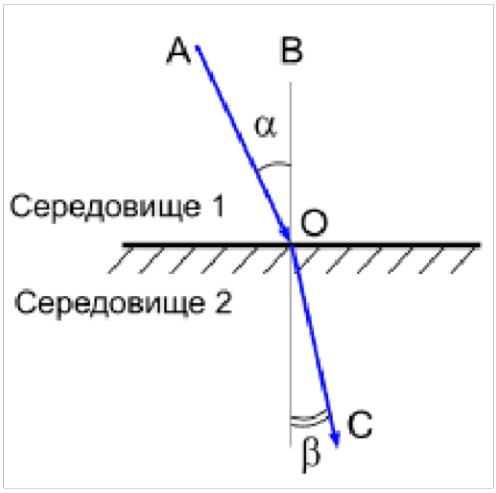


Рисунок 7.1 – Заломлення світла

Для ізотропних середовищ, тобто матеріалів або речовин, які мають однакові властивості в усіх напрямках, справедливий закон заломлення Снелліуса: відношення синуса кута падіння α до синусу кута заломлення β є величиною постійною і також ідентично відношенню швидкостей світла c_1 в першому середовищі і c_2 в другому середовищі:

$$\frac{\sin\alpha}{\sin\beta} = \frac{c_1}{c_2},$$

де α – кут падіння; β – кут заломлення; c_1 – швидкість світла в середовищі 1; c_2 – швидкість світла в середовищі 2.

З двох прозорих середовищ оптично більш щільним називається те, в якому швидкість світла менше. При переході з вакууму (повітря), в якому світло поширюється зі швидкістю $c0$, в середу зі швидкістю розповсюдження світла c має силу співвідношення:

$$\frac{\sin\alpha}{\sin\beta} = \frac{c_0}{c} = n$$

Відношення швидкості світла $c0$ вакуумі до швидкості світла с в середовищі називається показником заломлення n відповідного середовища. Показник заломлення вакууму (повітря) n_0 дорівнює 1.

Для двох різних середовищ з показниками заломлення $n1$ і $n2$ і швидкостями розповсюдження світла в них c_1 і c_2 мають силу наступні вирази:

$$c_1 = \frac{c_0}{n_1} \quad \text{та} \quad c_2 = \frac{c_0}{n_2}$$

Звідси виводиться інша форма закону заломлення Снелліуса:

$$\frac{\sin\alpha}{\sin\beta} = \frac{n_1}{n_2}$$

Відношення синуса кута падіння до синуса кута заломлення дорівнює зворотному відношенню відповідних показників заломлення.

Приклад. При показнику заломлення n_1 = 1,5, що зазвичай приймається для скла в волоконному світловоді, швидкість світла в світловоді дорівнює:

$$c_1 = \frac{300000\ \text{км/с}}{1{,}5} = 20000\ \text{км/с} = 200\ \text{м/мкс},$$

або затримці світла на 5 мкс на кожен кілометр світловода, або 5 нс на кожен метр світловода.

Показник заломлення *n* середовища залежить від довжини хвилі світла. Для довжин хвиль в інфрачервоному діапазоні, які важливі для оптичного зв'язку з використанням кварцового скла, він постійно зменшується в бік збільшення довжини хвилі.

На рис. 7.2 зображено явище повного внутрішнього відбиття в ОВ.

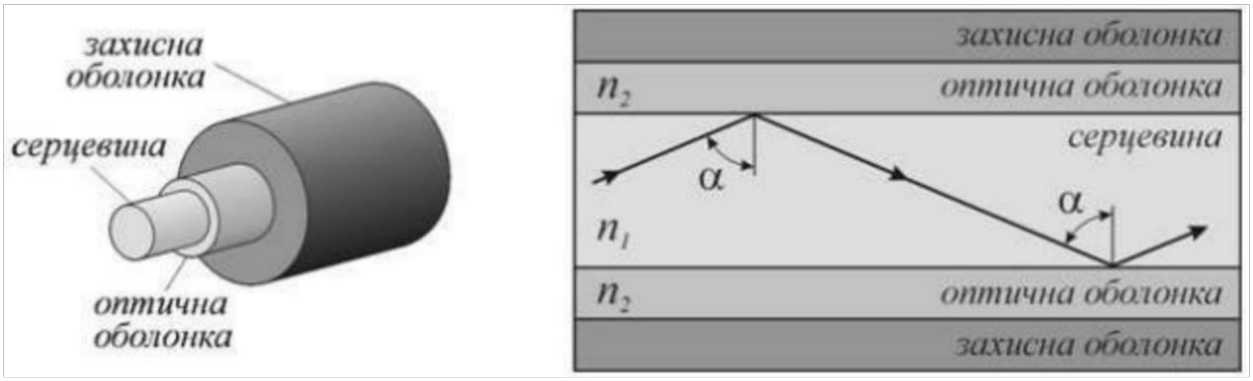


Рисунок 7.2 – Явище повного внутрішнього відбиття в оптоволокні

Оскільки $n1 > n_2$, то видно, що $\beta > \alpha$. Отже, збільшуючи кут падіння α оптичного променя, можна досягнути такого стану коли заломлений промінь почне ковзати на границі "серцевина-оболонка" без переходу в оптичну оболонку. Кут падіння, при якому спостерігається такий ефект, називається граничним кутом повного внутрішнього відбиття $\alpha_{гр}$ і визначається з наступного виразу:

$$\sin \alpha_{гр} = \frac{n_2}{n_1}$$

Для всіх кутів α, які більші за граничний $\alpha_{гр}$, буде мати місце тільки відбиття світла, а заломлена хвиля буде відсутня. Це явище називається повним

внутрішнім відбиттям (ПВВ) і саме воно лежить в основі передачі випромінювання по оптичному волокну.

При цьому залежно від виду оптичного волокна явище ПВВ може виглядати по-різному. Це пов'язано з тим, що коли випромінювання лазера надходить в серцевину волокна, то сигнал передається по ньому у вигляді окремих мод (можна сказати променів світла). Причому входять «промені» під різними кутами, тому час поширення енергії окремо взятих мод різниться. Це проілюстровано на рис. 7.3.

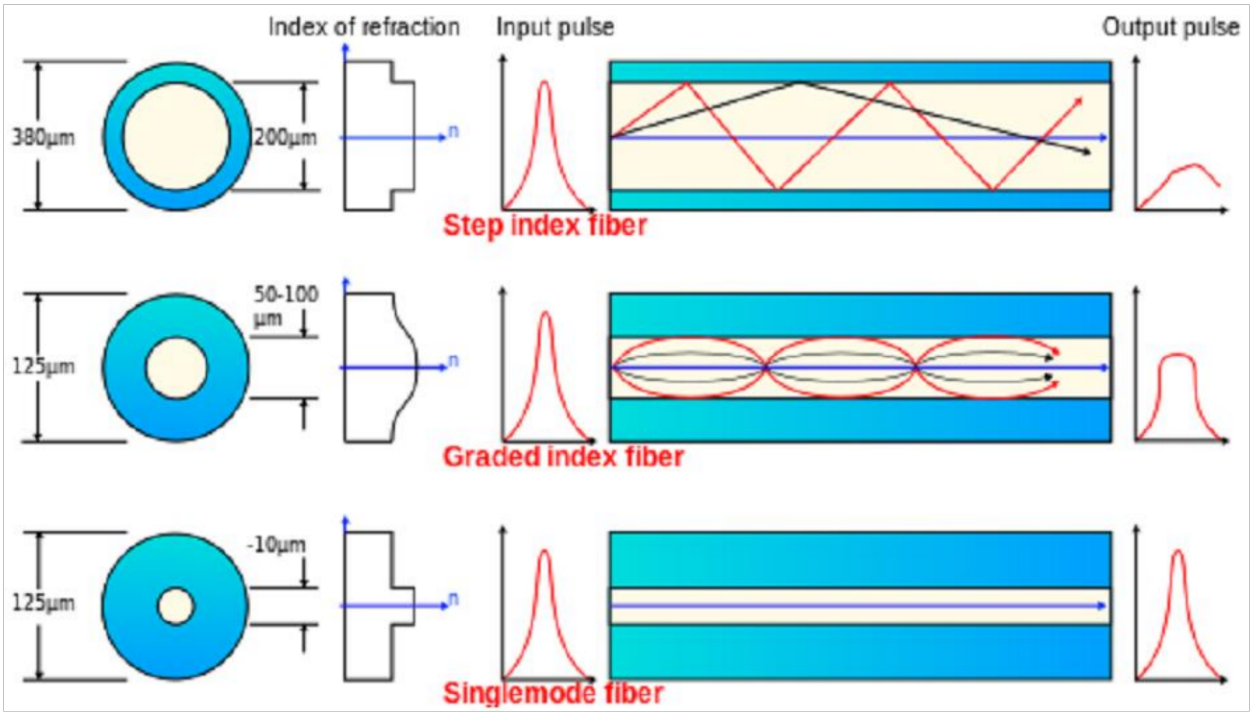


Рисунок 7.3 – Профілі заломлення світла в залежності від типу ОВ

Тут зображено 3 профілі заломлення: ступінчастий і градієнтний для багатомодового волокна і ступінчастий для одномодового.

Видно, що в багатомодових волокнах моди світла поширюються за різними шляхами, але, через постійний коефіцієнт заломлення серцевини вони мають однакову швидкість. Тобто ті моди, які змушені йти по ламаної лінії приходять пізніше, ніж моди, що йдуть по прямій. Тому вихідний сигнал розтягується в часі.

Інша справа з градієнтним профілем, ті моди які раніше йшли по центру – сповільнюються, а моди, які йшли по ламаному шляху, навпаки, прискорюються. Це сталося тому, що коефіцієнт заломлення сердечника тепер непостійний. Він збільшується параболічно від країв до центру.

Це дозволяє збільшити швидкість передачі і отримати сигнал на прийомі з кращими розпізнавальними якостями.

Завдяки такому різноманіттю можна скласти таблицю, що пояснює області застосування оптоволокна (табл. 7.1).

Таблиця 7.1 – Область застосування ОВ

Багатомодове волокно	Одномодове волокно	
ММF 50 (62.5) / 125 Градієнтне	SF 9/125 Ступінчасте	SF 9/125 Зі зміщеною дисперсією (з ненульовою зміщеною дисперсією)
ЛВС (GigaEther, FDDI, ATM)	Протяжні ЛВС, магістралі SDH	Надпротяжні магістралі SDH

На даний час магістральні кабелі майже всі йдуть з ненульовою зміщеною дисперсією, що дозволяє використовувати на цих кабелях спектральне ущільнення каналів (WDM) без потреби заміни кабелю. А при побудові пасивних оптичних мереж часто використовують багатомодове волокно.

7.1.3. Переваги та недоліки використання оптичного волокну у системах передачі

У порівнянні з дротовими системами волоконно-оптичні лінії зв’язку мають ряд істотних переваг:

- висока завадостійкість;
- слабка залежність якості передачі від довжини лінії зв'язку;
- висока стабільність параметрів каналів зв'язку;

– ефективність використання високої пропускної здатності оптоволоконної лінії зв'язку при побудові багатоканальних систем;

– висока уніфікація і надійність апаратури цифрової обробки сигналів.

Крім перерахованих переваг волоконно-оптичних ліній зв’язку мають підвищену захищеністю від несанкціонованого доступу за рахунок:

– високої захищеності від зовнішніх електромагнітних полів: лінії оптичної зв'язку не сприйнятливі до будь-яких електромагнітних зовнішніх впливів;

– в волоконно-оптичній лінії зв’язку відсутні проблеми перехресних перешкод від поруч розташованих ОВ і виключається перехід конфіденційної інформації з одного ОВ в інше;

– висока прихованість переданої інформації, що обумовлено дуже малою інтенсивністю випромінювання, що розсіюється;

– захищеність переданої інформації за рахунок можливості прокладки волоконно-оптичного кабелю в зонах важкодоступних для зловмисників.

В якості недоліків волоконно-оптичних ліній зв’язку можна відмітити наступне:

– мала механічна міцність;

– чутливість до згинання;

– чутливість до іонізуючих випромінювань;

– наявність витікаючих мод.

У зв'язку з усе більш зростаючими обсягами інформації, що передається, ВОЛЗ будуються як багатоканальні цифрові системи, здатні по одному оптоволокну за допомогою ущільнення каналу зв'язку передавати, в тому числі в дуплексному режимі, цифрові потоки від багатьох джерел сигналу.

7.1.4. Вразливості волоконно-оптичної лінії зв’язку

Під волоконно-оптичною лінією зв’язку (ВОЛЗ) надалі будемо розуміти волоконно-оптичну систему, що складається із пасивних та активних елементів, яка призначена для передачі інформації у оптичному (як правило – в ближньому інфрачервоному) діапазоні.

До активних компонентів відносяться: мультиплексори, демультиплексори, лазерні випромінювачі, фотоприймачі, регенератори, підсилювачі тощо. В якості пасивних елементів можуть бути: оптичний кабель, оптична муфта, оптичний крос, оптичні конектори.

До складу ВОЛЗ входить (рис. 7.4): передавач оптичної потужності (ПОМ) з вихідною потужністю *Ps*, приймач оптичної потужності (ПрОМ), що забезпечує при вхідної оптичної потужності *Pr* прийом і перетворення оптичного сигналу з заданим коефіцієнтом помилок BER, і волоконно-оптичний лінійний тракт (ВОЛТ), що має довжину *L* і загасання α. Приймально-передавальна пара ПОМ-ПрОМ має енергетичний потенціал *E*, який залежить від потужності ПОМ, спектральної щільності шуму, чутливості промити і швидкості передачі В. Заданий енергетичний потенціал Е обмежує довжину волоконно-оптичного тракту *L*, загасання якого (з урахуванням експлуатаційного запасу) не повинно перевищувати енергетичний потенціал *E*.

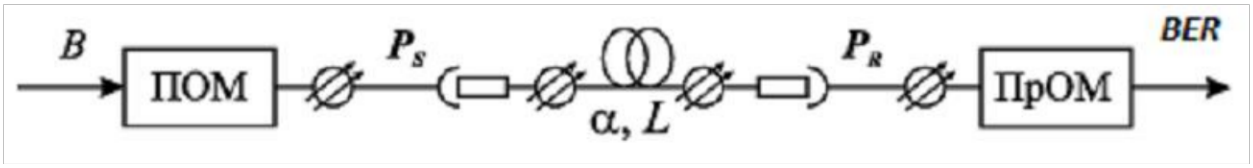


Рисунок 7.4 – Структурна схема ВОЛЗ

Вразливими до зловмисних дій компонентами ВОЛЗ вважаються:

– кабельні сегменти;

– вузли з'єднання будівельних відрізків оптичного кабелю в захисних оптичних муфтах.

Протягом усього лінійного тракту і на його елементах зловмисник може здійснювати тривалий несанкціонований доступ до інформації, що практично не виявляється за допомогою спеціальних засобів доступу до цифрового кодового потоку і здійснювати вивід на запис, прослуховування або ретрансляцію несанкціоновано отриманих даних.

У зв'язку з цим актуальним і закономірним є завдання захисту лінійного тракту ВОЛЗ.

Відомо, що в хвилевідній структурі оптоволокна оптичне випромінювання поширюється по закону повного внутрішнього відбиття. Проте, навіть після формування статичного розподілу поля в волокні, невелика частина розсіяного випромінювання все ж проникає за межі відбиває оболонки і може бути каналом витоку інформації, що передається.

Можливість існування побічних оптичних випромінювань з бічної поверхні ОВ обумовлена низкою конструктивних і технологічних факторів, наведених на рис. 7.5.

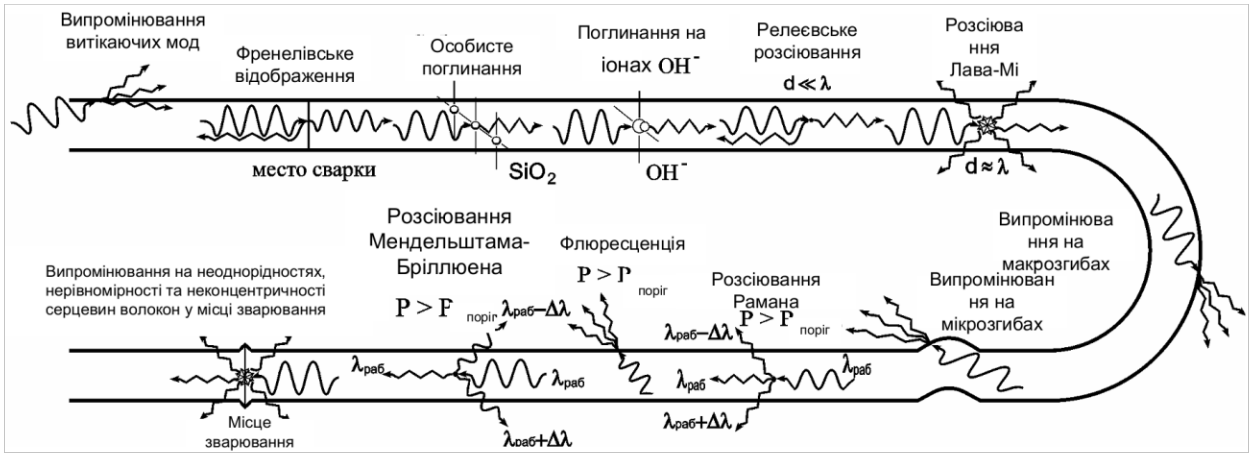


Рисунок 7.5 – Причини випромінювання і розсіювання світла в ОВ

7.2. Методи несанкціонованого з’йому інформації з волоконно-оптичних ліній зв'язку

На жаль, несанкціонований доступ (НСД) до ВОЛЗ, незважаючи на складність і витратність такої операції, все ж таки можливий. Способи знімання, які можуть бути використані для перехоплення інформації з ВОЛЗ, можна розділити на дві групи:

– за способом з'єднання: безконтактний, контактний, локальний, протяжний;

– за способом реєстрації і підсилювання: пасивні – реєстрація випромінювання з бічної поверхні оптоволокна; активні – реєстрація випромінювання, що виводиться через бічну поверхню оптоволокна за допомогою спеціальних засобів, що змінюють параметри сигналу.

На відміну від всіх інших середовищ передачі інформації, для формування каналів витоку на ділянках ВОЛЗ, як правило, вимагають прямого доступу до оптоволокну і спеціальних заходів відведення частини випромінювання з оптоволокна або реєстрації проходження випромінювання. Основні фізичні принципи формування каналів витоку в ВОЛЗ можна розділити на наступні типи:

– порушення повного внутрішнього відбиття;

– реєстрація розсіяного випромінювання на довжинах хвиль основного інформаційного потоку і комбінаційних частотах;

– параметричні методи реєстрації випромінювання.

Основні методи несанкціонованого з'єму інформації з ОВ представлені в табл. 7.2.

7.2.1. Порушення повного внутрішнього відбиття

Порушення повного внутрішнього відбиття, що приводить до витоку інформації може здійснюватися наступними способами:

– зміна кута падіння – використання зовнішнього впливу для зменшення кута падіння до значення, меншого значення граничного кута падіння, при якому починає спостерігатися повне внутрішнє відбиття;

– зміна ставлення кута заломлення оболонки до показника заломлення серцевини оптоволокна – використання зовнішнього впливу для збільшення кута повного внутрішнього відбиття до значень, великих характерних кутів падіння в світловоді;

– оптичне тунелювання – полягає в проходженні випромінювання через оболонку оптоволокна з показником заломлення меншим, ніж у серцевини, при кутах падіння великих кута повного внутрішнього відбиття тощо.

Таблиця 7.2 – Способи зняття інформації з ОВ

Порушення повного внутрішнього відображення	Макрозгиб, мікрозгиб, механічний вигин, скручування, розтягнення, вплив акустичних полів, оптичне тунелювання, вплив статичних електромагнітних полів
Реєстрація розсіяного випромінювання на довжинах хвиль основного інформаційного потоку і комбінаційних частотах	Пряма зміна розсіяного випромінювання на довжинах хвиль носія інформації
	Зміна розсіяного випромінювання на комбінаційних частотах
	Реєстрації випромінювання на основі спеціальної обробки ОВ зовнішніми полями, такими як теплове, електромагнітне, радіаційне
Параметричні методи реєстрації проходження випромінювання	Використання низьких температур
	Розрив оптоволокна
	Лінзове фокусування
	Компенсаційний спосіб

7.2.2. Реєстрація розсіяного випромінювання

Оптичні волокна мають малі втрати (0,2-0,18 дБ/км на довжині хвилі 1,55 мкм), що дозволяє передавати інформацію на великі відстані без ретрансляції сигналу. Ретрансляційні ділянки становлять понад 100 км. Це вимагає створення світлових імпульсів великої величини. Значна величина потужності, що вводиться в оптичне волокно, створює підвищене розсіювання на близький до ретранслятору ділянці, що може бути використане для знімання інформації. Сучасні фотоприймачі дозволяють вимірювати світлові потоки дуже малої величини.

Розсіяне випромінювання дозволяє сформувати канали витоку інформації, засновані на наступних фізичних принципах:

– пряма зміна розсіяного випромінювання на довжинах хвиль носія інформації;

– зміна розсіяного випромінювання на комбінаційних частотах;

– реєстрацію випромінювання на основі спеціальної обробки оптоволокна зовнішніми полями, такими як теплове, електромагнітне, радіаційне, з метою збільшення інтенсивності розсіяного випромінювання.

Таким чином, за допомогою зовнішнього впливу можна посилити втрати в світловоді на локальних ділянках, забезпечуючи формування каналів витоку інформації.

7.2.3. Параметричні методи реєстрації випромінювання, що проходить по оптоволокну

При поширенні по оптоволокну оптичного випромінювання, що є носієм інформації, воно викликає зміну фізичних властивостей середовища передачі інформації.

Модуляцію властивостей оптоволокна в залежності від інтенсивності світлових імпульсів можливо реєструвати спеціальними високочутливими пристроями.

Зміна властивостей оптоволокна є основою для формування каналу витоку інформації.

Наступні параметри оптоволокна піддаються модуляції світловим потоком:

– показник заломлення;

– показник поглинання світлового потоку оптоволокна при проходженні світла;

– малі зміни геометричних розмірів внаслідок фотопружного ефекту;

– реєстрація модуляції властивостей поверхні оптоволокна.

Сучасна техніка вимірювань дозволяє реєструвати незначні, дуже малі зміни фізичних властивостей оптоволокна. Так використання спектроскопії

втрат дозволяє реєструвати зміну показника поглинання, що викликає при проходженні по оптоволокну інформаційного потоку світла.

Вплив низьких температур

Цікавим є також протяжне безрозривне знімання інформації, яке можна здійснити на прямому волокні під впливом низьких температур. Справа в тому, що при низьких температурах відбувається зміна коефіцієнтів заломлення скла, в результаті чого в серцевині може підвищитися рівень розсіювання.

Розрив оптоволокна

Пристрої розривного НСД дозволяють здійснювати більш надійне знімання інформації. Однак розривне підключення вимагає тимчасового виключення лінії, що може сигналізувати про наявність самого доступу. Ймовірно, «для маскування», паралельно з підключенням можуть бути здійснені і навмисні пошкодження кабелю.

Спосіб лінзового фокусування

Основним і найбільш популярним способом безрозривного локального НСД є спосіб лінзового фокусування сингулярних (випливаючих) мод на вигині волокна. Цей спосіб знайшов застосування в апаратах для зварювання ОВ (і юстирування).

Очевидно, що для того, щоб здійснити НСД до інформації, необхідно дістатися до самого волокна ВОЛЗ і будь-яким чином зчитати інформацію, знявши частину оптичної потужності через оптичний розгалужувач.

Компенсаційний спосіб

Компенсаційні способи принципово поєднують в собі переваги перших двох груп – скритність і ефективність, але пов'язані з технічними труднощами при їх реалізації. Вивід випромінювання, формування і зворотне введення через бічну поверхню повинні здійснюватися з коефіцієнтом передачі, близьким до одиниці. Однак статистичний характер розподілу параметрів ОВ по довжині (діаметрів, показників заломлення серцевини і оболонки та ін.), спектральної смуги напівпровідникового лазера і характеристик пристрою знімання призводить до того, що різниця між виведеним і введенням назад рівнями

потужності носить імовірнісний характер. Тому коефіцієнт передачі може приймати різні значення. Здійснення знімання інформації цим способом можливо за допомогою спліттерів.

Слід зазначити, що захисні оболонки і елементи конструкції кабелю істотно послаблюють бічне випромінювання. Тому перехоплення інформації будь-яким їх перерахованих вище способів можливий тільки при порушенні цілісності зовнішньої захисної оболонки кабелю і безпосередньому доступі до оптичних волокон.

7.3. Способи захисту оптичного лінійного тракту від несанкціонованого доступу

Вищенаведені способи знімання інформації з оптичного волокна спростовують припущення про неможливість зняття інформації шляхом формування каналів витоку. У зв'язку з цим необхідно ознайомлення з можливими методами захисту інформації, що передається з використанням волоконно-оптичних ліній зв'язку.

Основні способи захисту ВОЛТ представлено у табл. 7.3.

7.3.1. Захист ВОЛТ на рубежі оптичного волокна

Для знімання інформації з ОВ необхідно здійснити фізичний контакт з його поверхнею. Правильний вибір конструкції ОВ дозволяє підвищити захищеність ВОЛЗ від НСД, оскільки ускладнює фізичний контакт з поверхнею, що відбиває волокна.

7.3.1.1 Оптичне волокно з поверхневою металізацією

Металізоване покриття ОВ підвищує температурний діапазон використання волокна до 700-800 °С. Поверхневий шар дозволяє збільшити апертурне число для одномодового випромінювання.

Металева плівка, нанесена на поверхню кварцового волокна, має високу адгезію і міцність до розчавлення чи навантажень, хорошу радіаційну стійкість і хімічну стійкість до агресивних середовищ, температуростійкість

визначається властивостями металу і можливо адаптувати волокно до заданих температурних умов.

Таблиця 7.3 – Способи захисту ВОЛТ від НСД

Захист оптичного волокна	Поверхнева металізація
	Багатошаровість ОВ
	Використання одномодового волокна з ненульовою дисперсією
Захист волоконно-оптичного кабелю	Наявність як захисних, так і допоміжних оболонок
	Використання ВОК без кольорового маркування ОВ
	ВОК з ненульовою зміщеною дисперсією
Спосіб прокладки волоконно-оптичного кабелю	Прокладка ВОК у ґрунт, по дну океану, підвіс кабелів разом з лініями електропередачі тощо
Перетворення інформації, що передається	Скремблювання, надлишкове кодування, спектральне розділення двох каналів
Додаткові засоби захисту	Маскування лінійного коду
Моніторинг	Рефлектометрія та відеоспостереження

Металізоване покриття є відбиваючою оболонкою ОВ і не допускає випромінювання з його поверхні. У разі порушення металізованого покриття істотно зростають втрати, що може бути виявлено відомими методами протидії НСД з ВОЛЗ.

7.3.1.2 Багатошарове оптичне волокно

Відомий метод захисту з використанням багатошарового оптичного волокна зі спеціальною структурою відображаючих і захисних оболонок. Конструкція такого волокна має 4-шарову структуру з одномодовою серцевиною.

Оптичне волокно складається з чотирьох шарів: центральної світлопровідної серцевини, внутрішньої відбиваючої оболонки, світлопровідної оболонки і зовнішньої відбиваючої оболонки.

Спроби проникнути до серцевини виявляються зі зміни рівня контрольного (шумового) сигналу або по змішуванню його з інформаційним сигналом. Місце НСД визначається з високою точністю за допомогою рефлектометра.

На рис. 7.6 позначено: 1 – центральна світлопровідна серцевина; 2 – внутрішня відбиваюча оболонка; 3 – світлопровідна оболонка; 4 – зовнішня відбиваюча оболонка.

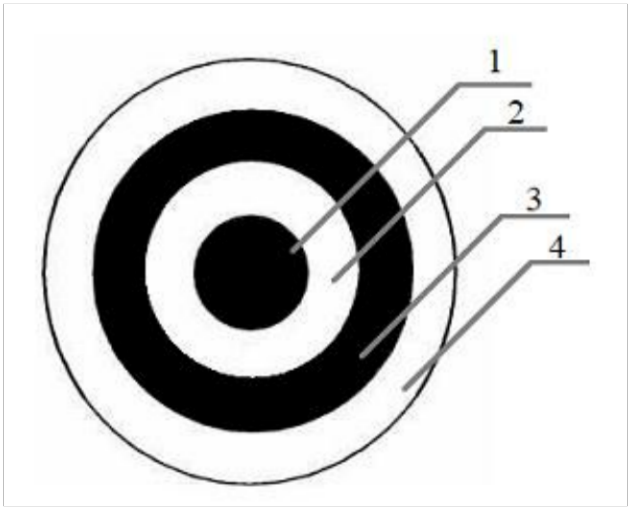


Рисунок 7.6 – Чотиришарове оптичне волокно

7.3.1.3 Вторинні захисні покриття волоконних світловодів

При виробництві волоконно-оптичного кабелю (ВОК) застосовується кілька видів вторинних покриттів, кожне з яких оптимізовано для виконання певного завдання. Варіанти конструктивного виконання вторинних захисних

покриттів волоконних світловодів подано на рис. 7.7, де а) щільне буферне покриття із зовнішнім діаметром 0,9 мм; б) щільне буферне покриття із зовнішнім діаметром 0,6 мм; в) двошарове захисне покриття із зовнішнім діаметром 0,9 мм і внутрішнім м'яким шаром; г) модульна конструкція (трубчасте покриття); д) мікромодульна конструкція (волокно укладено вільно в трубку, заповнену гелієм); е) типу mini-breakout.

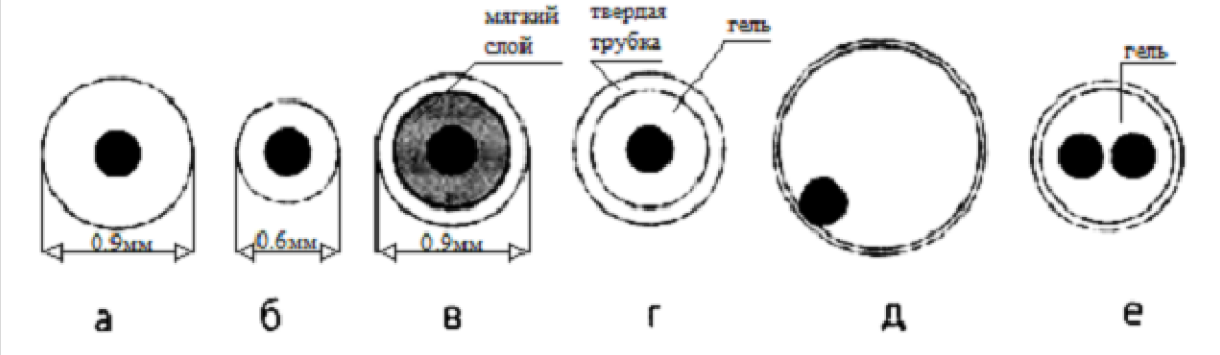


Рисунок 7.7 – Варіанти конструктивного виконання вторинних захисних покриттів волоконних світловодів

Аналіз конструкцій шести варіантів захисних покриттів ОВ, дозволяє зробити наступні висновки.

1. Конструкції ОВ варіантів «д» і «е» характеризуються найменшої захищеністю від НСД, тому що волокна вільно укладені в трубці, що є їх захисним покриттям. Видалення цього захисного покриття легко здійснюється без контакту зі світловодами, що не вимагає спеціальних заходів для збереження їх цілісності.

2. Конструкція ОВ варіанту «г» також недостатньо захищена від фізичного контакту з відбиваючою оболонкою. Світловод вільно покладений в трубку із зовнішнім діаметром 0,9 мм. Решта внутрішнього простору вільна або може бути заповнена гелем. Така конструкція ОВ дозволяє легко встановити контакт з відбиваючою оболонкою ОВ після розтину трубки і видалення гелю.

3. Конструкція ОВ варіанту «в» теж недостатньо захищена в зв'язку з тим, що після розтину трубки вторинне м'яке покриття можна видалити, хоча

виконати це складніше ніж у варіанті «г». Про це свідчить те, що за один технологічний цикл обробки ОВ може бути видалено захисне покриття на ділянці 1-2 метра.

4. Найбільш захищеними від НСД є конструкції ОВ варіантів «а» і «б», в яких застосовують щільне вторинне буферне покриття, яке без зазору укладено на первинне захисне покриття і відбиваючу оболонку. Завдяки такій конструкції ОВ максимальна довжина, що знімається за один технологічний цикл щільного покриття, становить 5 сантиметрів, що значно ускладнює встановлення фізичного контакту з відображає оболонкою світловоду.

Підвищеної захищеністю від доступу до відбиваючої оболонці мають волокна в стрічкової конструкції в якій кілька волокон укладені в один ряд і залиті загальним захисним покриттям. У такій конструкції оброблення вторинного покриття одного ОВ і його витяг з стрічки перешкоджають поруч розташовані волокна, які можуть бути пошкоджені.

7.3.2. Захист інформації на рубежі волоконно-оптичного кабелю

При виборі волоконно-оптичного кабелю (ВОК) для реалізації захисту від НСД лінії зв'язку, слід звертати увагу на конструкцію самого кабелю. До складу ВОК має входити якомога більше (в межах можливості прокладки) як захисних, так і допоміжних оболонок. Наявність таких оболонок значно ускладнює НСД з ОВ для зловмисника. Структура ВОК з різними оболонками представлена на рис. 7.8.

Використання ВОК без кольорового маркування ОВ ускладнює зловмисникові визначення оптоволокна, з конфіденційною інформацією, що передається по ньому. При використанні ВОК, що містять велику кількість ОВ перехоплювачеві необхідно робити НСД з певного волокна за яким передається необхідна йому конфіденційна інформація. Так як зазвичай ОВ в ВОК мають кольорове забарвлення захисних оболонок або кільцеве маркування і волокна при з'єднанні будівельних довжин ВОК з'єднуються між собою з позначенням цього маркування, то це може полегшити перехоплювачі знаходження нульового волокна, якщо він заздалегідь знає його маркування. Відсутність

маркування змушує перехоплювача послідовно проводити підключення до великої кількості ОВ в ВОК; досліджувати трафік в них і методом перебору знаходити потрібне ОВ з якого необхідно робити НСД. Така операція є трудомісткою і тривалою і може посприяти виявленню НСД службою захисту лінії зв'язку. Саме за рахунок цих особливостей конструкції і способів передачі інформації в ВОК виникає можливість у захисників інформації вибрати такий тип кабелю, який би став серйозним рубежем захисту від НСД, використовуючи особливості передачі інформації, які розкриває волоконна оптика в системах зв'язку.

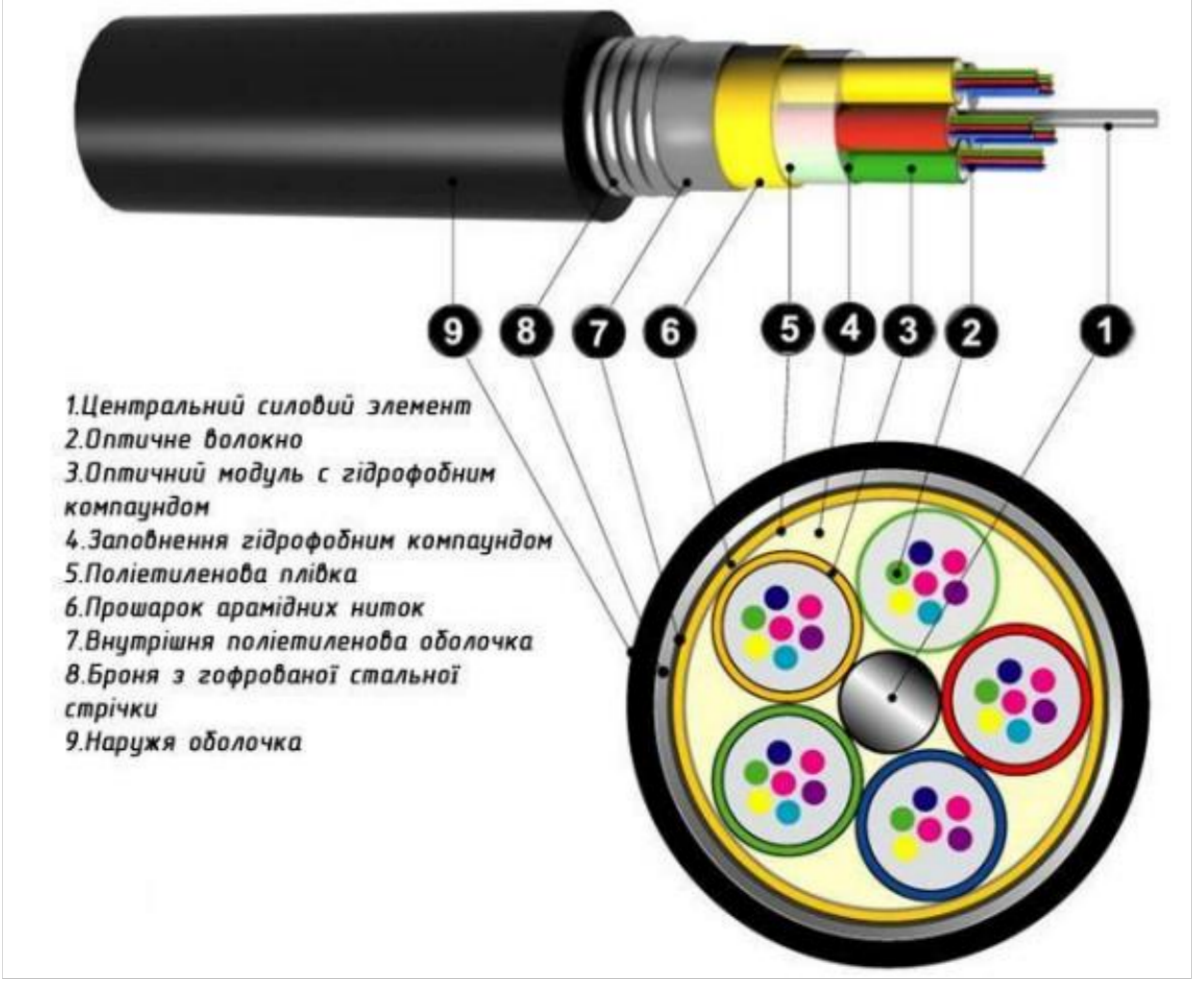


Рисунок 7.8 – Структура ВОК

При використанні в ВОК оптичного волокна з ненульовою зміщеною дисперсією по одному ОВ можлива передача великих потоків інформації на високих швидкостях на різних довжинах хвиль. При цьому конфіденційна

інформація передається на одній довжині хвилі, а на інших довжинах хвиль передається маскуюча інформація, що ускладнює зловмисникові знайти потрібне ОВ в багатоволоконному ВОК, а потім знайти потрібну довжину хвилі з конфіденційним трафіком серед великої кількості довжин хвиль з маскуючим трафіком.

7.3.3. Захист ВОЛЗ на рубежі прокладки ВОК

Прокладка ВОК у важкодоступних місцях є важливим аспектом в захисті інформації у ВОЛЗ. Підвіс кабелів разом з лініями електропередачі, прокладка ВОК у ґрунт і каналізацію, підводна прокладка, чи прокладка у нестандартних місцях – все це ускладнює задачу зловмисника дістатися до кабелю, а потім до оптичної серцевини та спробувати зняти інформацію. Правильний підбір ВОК згідно з місцем прокладення кабелю, розрахунок його параметрів та передбачення допоміжних опорних конструкцій є одним з рубежів захисту від НСД.

7.3.4. Захист ВОЛЗ методами перетворювання інформації

7.3.4.1 Захист лінійного тракту за допомогою скремблювання

Перемішування даних скремблером перед передачею їх у лінію за допомогою потенційного коду являється способом логічного кодування. Методи скремблювання полягають в побітному обчисленні результуючого коду на основі бітів початкового коду та отриманих у попередніх тактах бітів результуючого коду.

7.3.4.2 Захист ВОЛЗ за допомогою надлишкового кодування

Надлишкові коди засновані на розбитті вихідної послідовності біт на порції, які часто називають символами. Далі кожен вихідний символ замінюється на новий, який має більшу кількість біт, ніж вихідний. Надмірність інформації при надлишковому кодуванні дозволяє виявляти в навіть автоматично виправляти певну кількість помилкових бітів.

7.3.4.3 Спектральне розділення двох каналів

Відомий спосіб захисту інформації в оптичному тракті, який використовує спектральне розділення каналів. З цією метою на стику між лінійним і станційним оптичним кабелем (ОК) на вході в лінійний оптичний тракт впроваджується оптичний мультиплексор, один з входів якого підключений до станційного кабелю, з виходу якого надходить інформаційний сигнал (ІС) з робочою довжиною хвилі λ_1, а на другий вхід подається додатковий сигнал (сигнал перешкоди) з робочою довжиною хвилі λ_2. Оптичний мультиплексор забезпечує об'єднання двох сигналів з різними довжинами хвиль λ_1, λ_2 , для передачі по одному оптичному волокну (ОВ). У зв'язку з тим, що фотоприймач являє собою широкосмуговий пристрій знімання інформації з ОВ без застосування складних оптичних фільтрів, заздалегідь налаштованих на довжину хвилі ІС, стає практично неможливим. На виході оптичного тракту встановлюється демультиплексор, що забезпечує розподіл сигналів з різними довжинами хвиль λ_1, λ_2. Інформаційний сигнал на довжині хвилі λ_1 подається на фотоприймач, а сигнал маскуючої перешкоди з довжиною хвилі λ_2 відкидається.

7.3.4.4 Методи квантової криптографії

Методи квантової криптографії забезпечують високий ступінь захисту від перехоплення інформації на лінії зв'язку за рахунок передачі даних у вигляді окремих фотонів, оскільки неруйнуюче вимірювання їх квантових станів в каналі зв'язку перехоплювачем неможливо, а факт перехоплення фотонів з каналу може бути виявлений по зміні імовірнісних характеристик послідовності фотонів.

7.3.5. Маскування інформації способом багаторазового спектрального розподілу

Під маскуванням розуміють зміну форми переданої інформації по оптичній лінії, що ускладнює її розпізнавання при несанкціонованій зміні.

Недоліком способу спектрального розподілу двох каналів є передача всієї інформації, що захищається, на одній довжині хвилі, а маскуючого сигналу на інший довжині хвилі.

Подальше підвищення захищеності інформації в оптичному тракті методом спектрального розподілення можна досягти багаторазовим розподілом переданого повідомлення на частини і передача цих частин на різних довжинах хвиль і маскуванням цих частин на кожній довжині хвилі.

Приклад реалізації запропонованого способу захисту ВОЛЗ полягає у використанні структурної схеми, поданої на рис. 7.9.

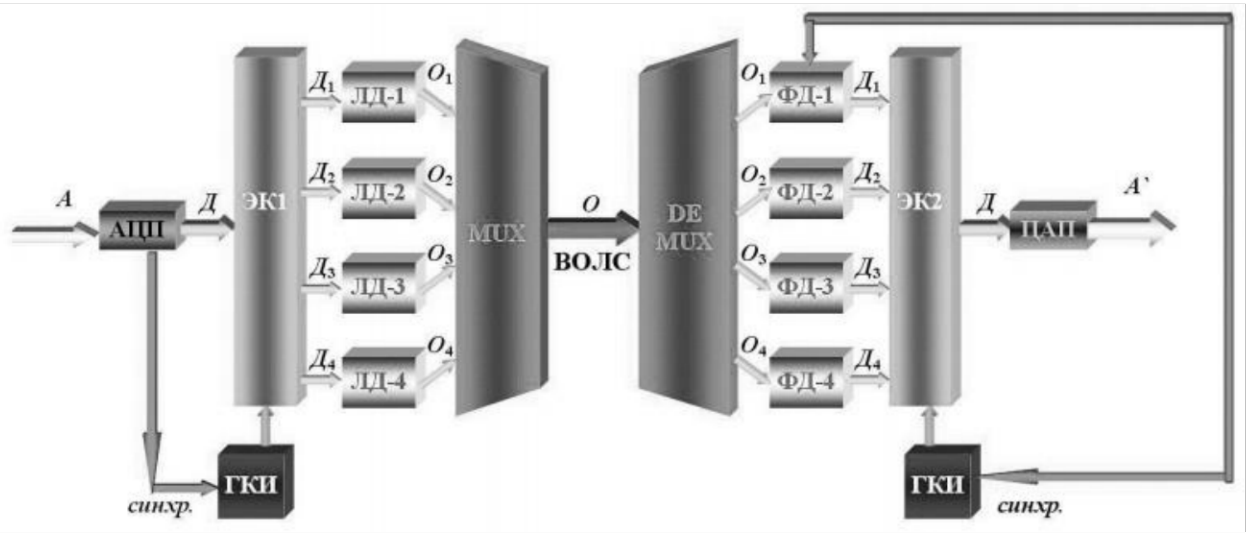


Рисунок 7.9 – Структурна схема маскування інформації шляхом її розподілу і передачі частин на різних довжинах хвиль

Аналогова інформація повідомлення А в електронному вигляді перетворюється в аналого-цифровому перетворювачі (АЦП) в цифровий потік даних, який поділяється в електронному комутаторі (ЕК) на кілька частин – в пакети $Д_1 \div Д_4$. Перший пакет $Д_1$ є опорним, і несе в собі інформацію про синхронізацію. Пакети $Д_1 \div Д_4$ надходять на електронно-оптичні перетворювачі, де перетворюються з електричних в оптичні сигнали лазерних діодів (ЛД), причому кожен на різній довжині хвилі випромінювання $\lambda_1 \div \lambda_4$. Окремі оптичні сигнали подаються на мультиплексор, де проводиться їх мультиплексування в загальний потік О на різних довжинах хвиль $\lambda_1 \div \lambda_4$ і їх

передача по ВОЛЗ в спільному оптичному волокні. В результаті проведених перетворень по ВОЛЗ передається не вся інформація на одній довжині хвилі, а тільки її частина, решта ж інформації передаються на інших довжинах хвиль. На протилежному кінці лінійного тракту виконуються зворотні перетворення: загальний сигнал з ВОЛЗ надходить на демультиплексор оптичних сигналів, на виході якого загальний потік розподіляється і формуються оптичні сигнали на різних довжинах хвиль $\lambda_1 \div \lambda_4$, які надходять на селективні оптичні фотоприймачі – фотодіоди (ФД). Оптичні сигнали в оптичних фотоприймачах перетворюються в електричні сигнали. Отримані сигнали надходять на входи електронного комутатора, який синхронізований з комутатором, і в якому збирається весь цифровий потік. В цифро-аналоговому перетворювачі (ЦАП) узагальнений цифровий потік перетвориться в аналоговий. Таким чином, якщо на ділянці прокладки ВОЛЗ зловмисник намагається зняти інформацію, підключивши пристрій несанкціонованого з'йому інформації, то ймовірність того, що він виявить весь потік інформації, що передається на різних довжинах хвиль дуже низька.

Для подальшого підвищення захищеності переданої інформації від НСД в схему вносяться додаткові елементи: суматори імпульсів і віднімаючі пристрої, а також генератор маскуючих імпульсів (рис. 7.10).

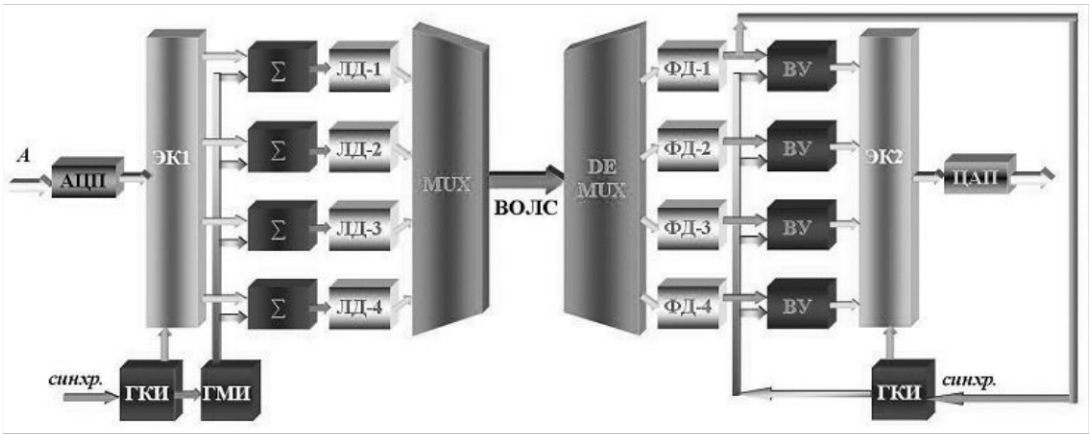


Рисунок 7.10 – Структурна схема маскування шляхом заповнення порожніх часових інтервалів псевдовипадковими імпульсами

Часові інтервали, які виникають після розподілу початкового потоку інформації на кілька частин, заповнюються маскуючими псевдовипадковими сигналами. При цьому в загальному потоці в ВОЛЗ після їх мультиплексування створюються суцільні оптичні потоки на різних довжинах хвиль $\lambda_1 \div \lambda_4$, що складаються з суми інформаційних і маскуючих сигналів, які утворюють додаткові перешкоди для відбору пакетів, що несуть корисну інформацію. На приймальному кінці ВОЛЗ ці сигнали розділяються по довжинах хвиль на демультиплексорі, перетворюються з оптичних в електричні, з яких за допомогою віднімаючих пристроїв, синхронізованих з суматорами виключаються із загального потоку інформації маскуючі сигнали. Решта пакетів, що несуть корисну інформацію, за допомогою електронного комутатора збирають в загальний цифровий потік, перетворений з допомогою ЦАП в аналогову інформацію.

7.3.6. Аналіз відбитого сигналу (рефлектометрія)

Для контролю величини потужності сигналу зворотного розсіяння в ОВ використовується різні методи, основані на використані рефлектометрії. В досліджуване ОВ надсилається зондуючий оптичний сигнал, наприклад, потужний короткий імпульс. Потім на цьому ж боці реєструється відбите випромінювання, що виникає на різних неоднорідностях та спрямовано в зворотному напрямі. По інтенсивності даного випромінювання можна судити про втрати в ОВ, місця виникнення яких розподілені по довжині ВОК на відстанях до 100-120 км. Початкові, тобто тестові рефлектограми конкретної волоконно-оптичної лінії фіксуються при різних динамічних параметрах зондуючого сигналу в пам'яті комп'ютера. Потім, під час функціонування ВОЛЗ в ОВ надсилається такий самий зондуючий сигнал; отримані рефлектограми порівнюються з тестовими рефлектограмами. Відхилення рефлектограми більш ніж на 0,1 дБ свідчить про можливу спробу несанкціонованого доступу до ОВ.

Метод рефлектометрії має вагомі переваги порівняно з іншими методами контролю параметрів ВОЛЗ:

– виміри проводяться на одному кінці лінії (або з одного кінця оптичного волокна);

– є можливість визначення довжини відрізка волокна (кабелю) до місця пошкодження (неоднорідностей, тріщин ОВ, мікро вигинів);

– вимірює втрати на з’єднаннях;

– вимірює коефіцієнт зворотного відбиття;

– проводить оцінку стану системи з плином часу, порівнянням первинних та отриманих поточних рефлекторам (можна також порівняти рефлекторами на різних довжинах хвиль (звичайно, на 1310 нм та 1550), що дозволяє визначити характер виявленої неоднорідності, наприклад, ідентифікувати згини або зрощення ОВ).

До недоліків підходу на основі рефлектометрів можна віднести наступне:

– залежність роздільної здатності від довжині ВОЛТ. При точному виявленні локальних неоднорідностей (для фіксації НСД) значно знижується динамічний діапазон і, відповідно, зменшується контрольована ділянка ВОЛТ;

– потужні зондуючі імпульси ускладнюють штатну роботу ВОЛЗ з передачі інформації, що знижує можливості рефлектомерта, або ускладнює і здорожує систему;

– джерела потужних зондуючих імпульсів мають обмежений ресурс використання, недостатній для тривалого безперервного контролю ВОЛЗ;

– спеціалізовані джерела зондуючого оптичного випромінювання, широкосмугова і швидкодіюча апаратура приймального блоку рефлектометрів значно здорожує систему.

Існують наступні методи рефлектометрії:

– імпульсна (optical time domain reflectometer, OTDR);

– частотна (optical frequency domain reflectometer, OFDR);

– брілюеновська (optical frequency domain reflectometer, OFDR);

– когерентна (coherent optical time domain reflectometer, C-OTDR);

– поляризаційна (polarization optical time domain reflectometer, P-OTDR).

Дільниці поблизу відбиваючих елементів, в котрих не можна достовірно проводити виміри, називають *мертвими зонами рефлектометра*. Дільницю поблизу відбиваючої події, в межах якої неможливо виявити іншу відбиваючу подію, називають мертвою зоною відбиття. Ділянка поблизу відбиваючої події, в межах котрої неможливо достовірно виміряти рівень потужності зворотного розсіювання, називається мертвою зоною загасання.

7.4. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи, розв'язати задачі.

7.4.1. Задача 1

Розглянути та дослідити метод або спосіб організації несанкціонованого доступу до даних, що передаються оптоволокном ВОЛЗ згідно свого варіанту (табл. 7.1). Відповісти на питання: в чому полягає сутність даного методу / способу. Складові, які він містить (якщо є). Які фізичні явища або особливості оптоволоконної передачі інформації він використовує.

Таблиця 7.1 – Варіанти завдань до Задачі 1 Лабораторної роботи 7

№ з/п	Номер підпункту в опису лаб. роб.	Способи зняття інформації з оптичного волокна
1.	7.2.2.	Реєстрація розсіяного випромінювання
2.	7.2.1.	Порушення повного внутрішнього відбиття
3.	7.2.3.	Реєстрація випромінювання, що проходить по оптоволокну шляхом зміни параметрів оптоволокна
4.	7.2.3.	Методи, що засновані на зміни фізичних властивостей оптоволокна
5.	7.2.3.	Компенсаційний спосіб
6.	7.2.2.	Реєстрація розсіяного випромінювання
7.	7.2.1.	Порушення повного внутрішнього відбиття
8.	7.2.3.	Методи, що засновані на зміни фізичних властивостей оптоволокна
9.	7.2.3.	Реєстрація випромінювання, що проходить по оптоволокну шляхом зміни параметрів оптоволокна
10.	7.2.3.	Компенсаційний спосіб

7.4.2. Задача 2

Розглянути та дослідити метод (засіб або підхід) захисту ВОЛЗ (ВОЛТ) згідно свого варіанту (табл. 7.2). Відповісти на питання: в чому полягає сутність даного методу. Складові, які він містить (якщо є). За рахунок чого підвищується захищеність ВОЛЗ / ВОЛТ даним методом. Чи можна сформулювати переваги та недоліки даного методу. В яких випадках доречно використовувати даний метод захисту волоконно-оптичного каналу зв'язку.

Таблиця 7.2 – Варіанти завдань до Задачі 2 Лабораторної роботи 7

№ з/п	Номер підпункту в опису лаб. роб.	Метод захисту волоконно-оптичного каналу зв'язку
1.	7.3.5.	Маскування інформації способом багаторазового спектрального розподілу
2.	7.3.6.	Аналіз відбитого сигналу (рефлектометрія)
3.	7.3.4.	Захист ВОЛЗ методами перетворювання інформації
4.	7.3.1.	Захист ВОЛТ на рубежі оптичного волокна
5.	7.3.2., 7.3.3.	Захист інформації на рубежі волоконно-оптичного кабелю та на рубежі його прокладки
6.	7.3.5.	Маскування інформації способом багаторазового спектрального розподілу
7.	7.3.4.	Захист ВОЛЗ методами перетворювання інформації
8.	7.3.1.	Захист ВОЛТ на рубежі оптичного волокна
9.	7.3.2., 7.3.3.	Захист інформації на рубежі волоконно-оптичного кабелю та на рубежі його прокладки
10.	7.3.6.	Аналіз відбитого сигналу (рефлектометрія)

7.5. Питання до самоконтролю

1. Назвіть кілька відомих переваг ВОЛЗ (в тому числі переваг в сенсі захисту інформації), які на вашу думку обумовлені тим фактом, що по ВОК не тече електричний струм (внаслідок чого відсутні відповідні магнітні явища).

2. Наведіть приклади механічних маніпуляцій з ОВ, які може здійснити зловмисник для НСД шляхом порушення повного внутрішнього відбиття?

3. Які переваги в сенсі підвищення інформаційної безпеки надає металева плівка, нанесена на поверхню оптичного волокна?

4. Чому відсутність кольорового маркування ОВ у ВОК ускладнює зловмисникові виконання НСД?

5. Наведіть приклади захисту ВОЛЗ шляхом особливої прокладки ВОК.

6. В чому полягає основний недолік способу захисту ВОЛЗ шляхом спектрального розподілу двох каналів? Який підхід дозволяє позбутися цього недоліку

7. В чому полягає суть методів на основі рефлектометрії?

7.6. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

7.7. Література до Лабораторної роботи 7

Рекомендовані літературні джерела до виконання Лабораторної роботи 7: [1, 2, 15].

ЛАБОРАТОРНА РОБОТА 8. РОБОТА З ГРІД-СЕРТИФІКАТОМ

Мета роботи: набуття навичок захисту інформації у розподілених обчислювальних мережах та поводження з грід-сертифікатами.

8.1. Теоретичний матеріал до лабораторної роботи

Узагальнено кажучи, можна вважати, що якщо інтернет є мережею, що дозволяє розподіляти інформацію, то грід-середовище є мережею, що дозволяє розподіляти обчислювальні ресурси, тобто завантажувати свої завдання і дані на віддалений грід-вузол та запускати необхідні обчислювальні процеси. При цьому використовуватимуться потужні та коштовне обчислювальне обладнання: грид-середовище, по суті, є розподіленою суперкомп'ютерною мережею.

Тому виконання операцій в грід-середовищі є потенційно більш небезпечною дією, порівняно з користуванням Глобальною мережею. Тому питанням кібербезпеки в гріді приділяється набагато більше уваги. Зокрема, кожний користувач грід-мережі (а також кожний програмний процес, що виконується в грід-середовищі) повинен мати засіб підтвердження своїх повноважень. На практиці в якості такого засобу використовується механізм сертифікації, який базується на використанні криптографічних методів. Тобто, кожний грід-користувач повинен мати персональний сертифікат (а кожний грід-процес – сертифікат хоста/вузла), який ідентифікує суб'єкт грід-обчислень та надає відповідні повноваження.

8.1.1. Інфраструктура відкритого ключа

Криптографія є галуззю прикладної математики, яка займається питаннями безпеки передачі даних. У криптографії відправник переводить незахищену інформацію (звичайний текст) у закодований текст (цифровий текст). Одержувач використовує засоби криптографії для переведення отриманого цифрового тексту назад у звичайний текст, а також для перевірки особистості відправника, цілісності даних або кількох із названих показників

одночасно. Криптографічні технології можна використовувати для забезпечення повного спектру послуг з безпеки.

Цифровий підпис є одним із механізмів, які можна застосовувати для захисту автентичності і цілісності електронних документів. Його можна використовувати для документу будь-якої форми, який обробляється в електронному вигляді. Цифровий підпис реалізується за допомогою методу криптографії на основі унікальної зв‘язаної пари ключів, в якій один з них використовується для створення підпису (приватний ключ), а другий – для перевірки підпису (відкритий ключ). Приватний ключ повинен зберігатися у таємниці, оскільки будь-хто, хто має до нього доступ, може підписувати документи. На доповнення до цього, захист цілісності відкритого ключа також є важливим. Такий захист здійснюється шляхом використання сертифіката відкритого ключа.

В грід системах існує спеціальна підсистема безпеки для забезпечення безпечного доступу до ресурсів в незахищених мережах загального доступу (Інтернет) з урахуванням прав даного користувача і правил обслуговування користувачів даним ресурсним центром (такі правила часто називають «локальною політикою»). Практично у всіх великих грід-системах робота цієї підсистеми заснована на інфраструктурі безпеки гріду (Grid Security Infrastructure, GSI), яка розроблена Globus Alliance.

Підсистема надає такі сервіси, як автентифікація, конфіденційність передачі інформації і делегування прав. Під делегуванням прав мається на увазі, що користувачеві потрібно лише один раз пройти процедуру автентифікації, а далі система сама забезпечить його автентифікацію на всіх ресурсах, які він планує використовувати. GSI, у свою чергу, заснована на надійній і широко використовуваній технології відкритих криптографічних ключів (Public Key Infrastructure, PKI).

Термін «інфраструктура відкритого ключа» (ІВК) походить від криптографії відкритого ключа. Інфраструктура відкритого ключа є поєднанням програмного забезпечення, шифрувальних технологій і послуг, які допомагають

забезпечити безпеку комунікацій і бізнес-операцій у мережах загального доступу. Інфраструктура відкритого ключа об‘єднує цифрові сертифікати, криптографію відкритого ключа і органи сертифікації та забезпечує побудову загальної архітектури безпеки організації.

Типова ІВК включає в себе видачу цифрових сертифікатів індивідуальним користувачам і серверам, програмне забезпечення з реєстрації кінцевого користувача; інтеграцію із сертифікатами; інструменти для управління, оновлення та скасування сертифікатів, а також інші послуги і підтримки, пов‘язані з ними.

До функціональних елементів інфраструктури відкритого ключа відносяться органи сертифікації, органи реєстрації, сховища та архіви:

- орган сертифікації як нотаріус видає або скасовує сертифікати;
- орган реєстрації – організація, якій ОС довіряє зареєструвати або яка ручається перед ОС за зв‘язок між відкритими ключами та ідентифікацією власників сертифікатів;
- сховище – це база даних активних сертифікатів і список анульованих сертифікатів – САС (Certificate Revocation List – CRL) для системи ОС;
- архів є базою даних, яку використовують при вирішенні майбутніх спорів;
- користувачі ІВК – це організації або фізичні особи, які використовують ІВК, але не видають сертифікати.

8.1.2. Ідентифікація користувачів і грід-вузлів

В якості ідентифікаторів користувачів і ресурсів в GSI (Grid Security Infrastructure) використовуються цифрові сертифікати стандарту X.509 (стандарт міжнародної організації International Telecommunication Union, ITU). У роботі з сертифікатами X.509 і в процедурі видачі/отримання сертифікатів задіяне три сторони:

1. Центр сертифікації (Certificate Authority, CA) – спеціальна організація, яка володіє повноваженнями видавати (підписувати електронним способом) цифрові сертифікати. Різні CA зазвичай незалежні між собою. Стосунки між

CA і його клієнтами регулюються спеціальним документом і довіра до сертифіката будується на довірі до центру сертифікації, який підписав цей сертифікат.

2. Власник сертифіката – користувач грід або грід-ресурс, який користується сертифікаційними послугами центру сертифікації. Центр сертифікації включає в сертифікат дані, які надаються власником (ім'я, організація і іншу інформацію) і завіряє його своїм цифровим підписом. Зокрема, власникові сертифіката надається унікальне ім'я (Distinguished Name, DN), наприклад, "O=Grid/O=Globus/OU=itso.grid.com/CN=Sergiy Petrov"

3. Користувачі або ресурси, які виконують автентифікацію інших грід-об'єктів – вони покладаються на інформацію з сертифікатів при отриманні його від об'єктів, який ідентифікуються. Вони можуть приймати або відмовляти в прийомі сертифікатів, які підписані певним CA.

В GSI використовуються два типи сертифікатів X.509:

1. Сертифікат користувача (User Certificate), який повинен мати кожен користувач, що працює з грід-системою. Сертифікат користувача містить інформацію про ім'я користувача, організацію, до якої він належить, і центр сертифікації, який видав даний сертифікат.

2. Сертифікат вузла (Host Certificate) повинен мати кожен вузол (грід-сервіс або ресурс) грід-системи. Сертифікат вузла аналогічний сертифіката користувача, але в ньому замість імені користувача вказується доменне ім'я конкретного грід-вузла.

Сертифікат стандарту X.509 GSI (Grid Security Infrastructure) включає такі основні елементи, показані на рис. 8.1.

Дійсні сертифікати зберігаються в спеціальному репозиторії центру сертифікації; там же зберігається список відкликаних сертифікатів (Certificate Revocation List, CRL). Центр сертифікації засвідчує приналежність сертифіката даному користувачеві або грід-вузлу, які ідентифікуються своїми унікальними іменами (Distinguished Name, DN).

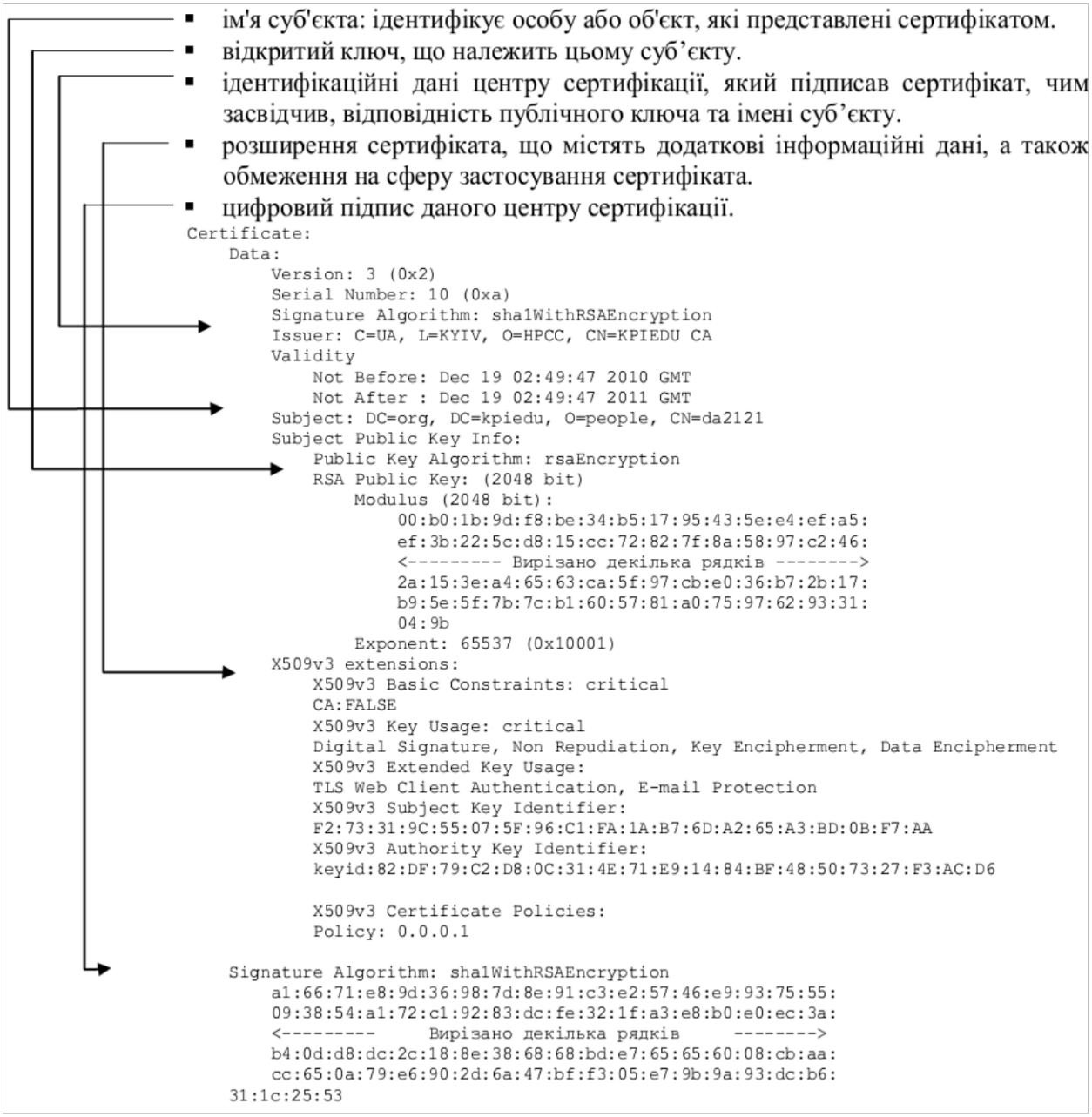


Рисунок 8.1 – Структура сертифіката

Для генерації сертифіката використовується в основному несиметричний алгоритм шифрування. При цьому в режимі шифрування відкритий ключ використовується для шифрування, закритий ключ – для розшифровки. У випадку використання цифрового підпису: закритий ключ – для шифрування, відкритий ключ – для розшифровки. Цифровий підпис може створити лише власник закритого (приватного) ключа. Тому важливою вимогою є безпечне зберігання закритого ключа.

8.1.3. Делегування прав і використання довіреності

Важливою умовою для ефективної роботи розподілених систем є можливість делегування прав користувача грід-сервісам. Річ у тому, що практично будь-який запит користувача проходить через декілька сервісів. І якби не було механізму делегування, користувачеві було б необхідно автентифікуватися на кожному сервісі в ланцюжку, що обробляє даний запит. Це означає, що користувач після відправлення завдання має невідривно бути біля свого комп'ютера і відповідати на запити про свою автентифікацію від кожного сервісу в ланцюжку. Фактично це робить роботу в грід-середовищі неможливою – в усякому разі, при запуску великого набору завдань. Делегування прав дозволяє уникнути цієї проблеми.

Для забезпечення безпеки в грід-системах та делегування прав користувача грід - сервісам використовується спеціальне доручення (Proxy Certificate, проксі-сертифікат), з коротким (зазвичай – кілька годин) терміном дії. Цю довіреність «виписує» (виконує відповідну команду користувацького інтерфейсу) сам користувач за допомогою свого постійного сертифіката, діючи в цьому випадку як «сертифікаційний центр» для самого себе. За допомогою цього проксі-сертифіката грід-сервіси виконують дії від імені користувача – власника сертифіката, наприклад, запускають завдання на обчислювальному ресурсі.

8.2. Отримання сертифіката майбутнім користувачем грід-системи

8.2.1. Український центр грід-сертифікації

Будь-який потенційний користувач технології грід-обчислень має отримати відповідний цифровий персональний сертифікат міжнародного зразка. В Україні такий сертифікат можна отримати лише в авторизованому Центрі сертифікації, розташованому в ЗВО Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Нижче наведено покрокову інструкцію отримання грід-сертифіката, а також інструкцію з перетворення сертифіката у формат, придатний для використання у будь-якому веб-браузері.

8.2.2. Отримання нового персонального сертифіката

8.2.2.1. В будь-якому браузері зайти на сторінку Центра сертифікації: https://ca.ugrid.org/ (рис. 8.2).

8.2.2.2. В лівому верхньому куті обрати зручну мову інтерфейсу.

8.2.2.3. Ознайомитися з поточною політикою видачі сертифікатів за посиланням https://ca.ugrid.org/docs/current_policy_ugrid.pdf (англ. мовою).

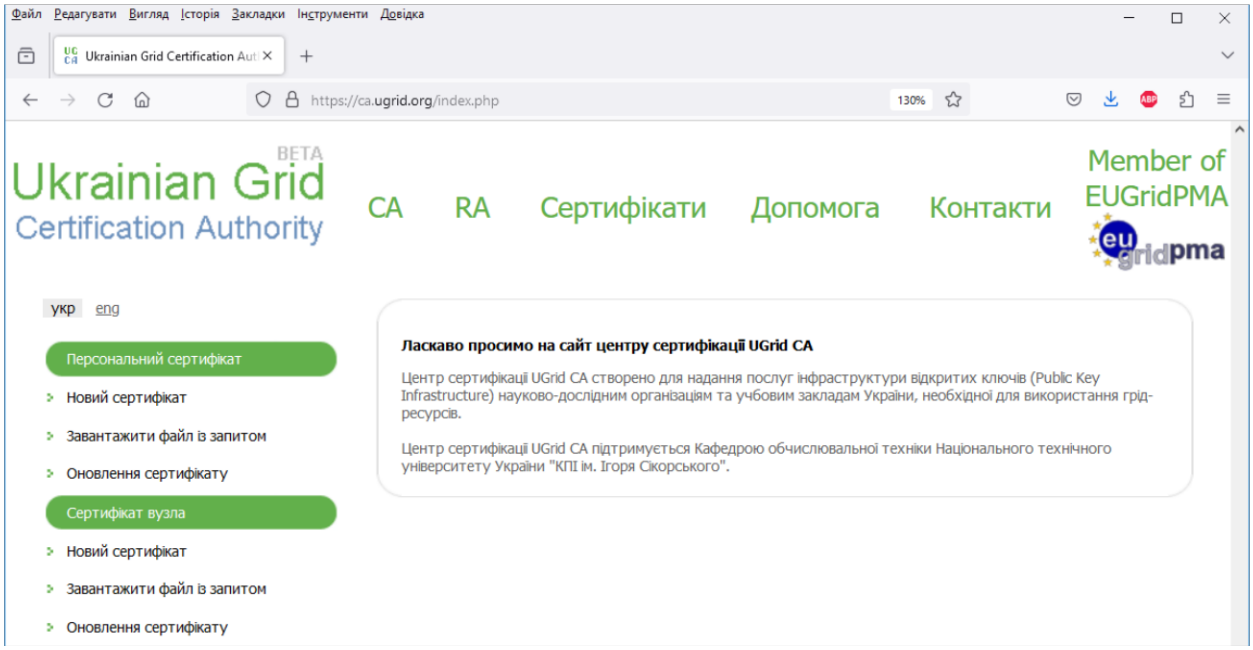


Рисунок 8.2 – Веб-сайт українського Центру сертифікації

8.2.2.4. В інтерфейсі Центра сертифікації обрати пункт меню "Персональний сертифікат / Новий сертифікат".

8.2.2.5. Заповнити відповідну форму (рис. 8.3).

Поля "Ім'я" та "Прізвище" заповнюються за правилами транслітерації української мови латиницею (https://zakon.rada.gov.ua/laws/show/55-2010-%D0%BF#Text) або так, як записано в закордонному паспорті, причому перші

літери імені та прізвища мають бути великими (у верхньому регістрі), а всі інші - малими (у нижньому регістрі).

Примітка: Ці два поля утворюють атрибут CN (Common Name) сертифіката.

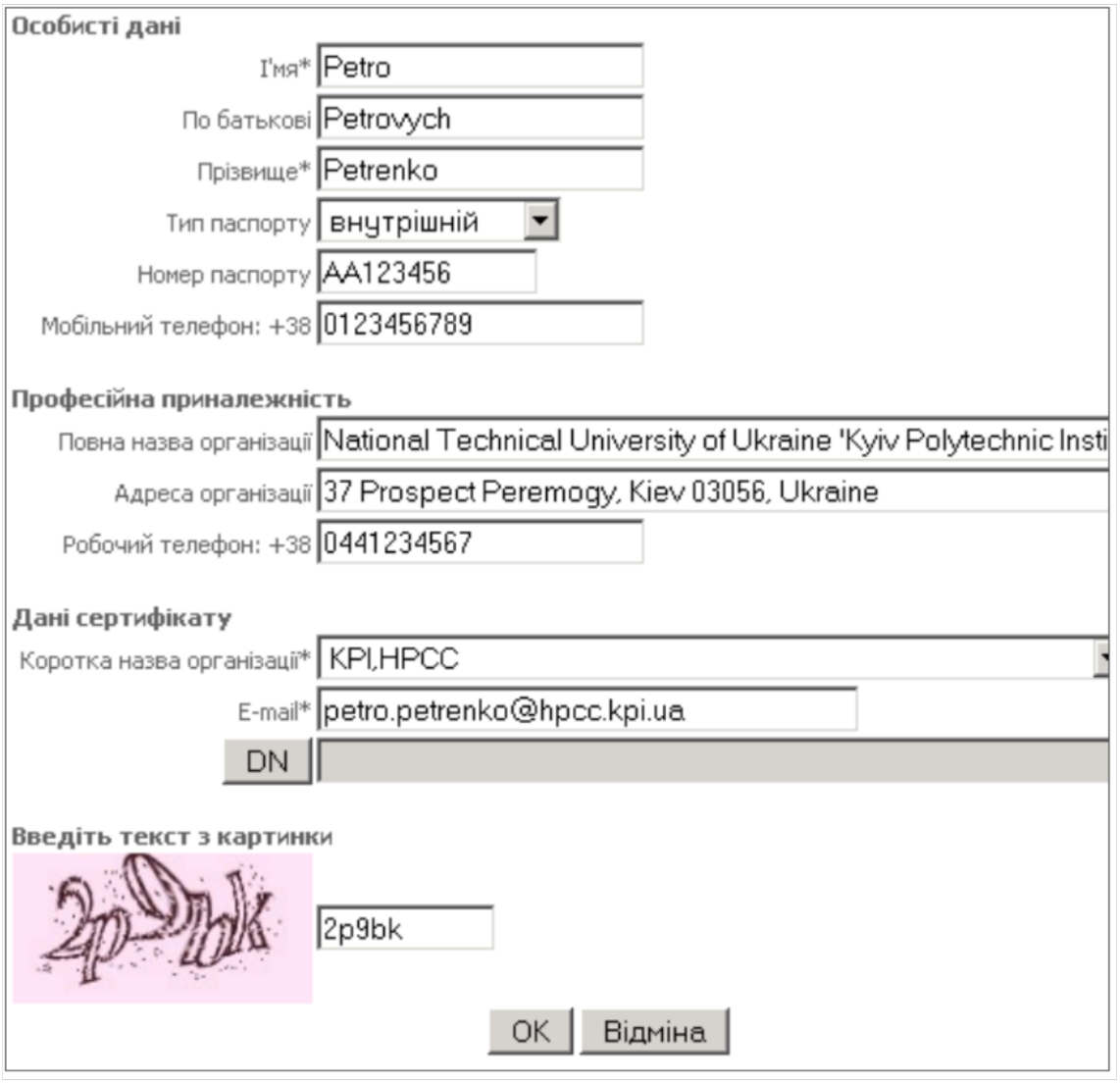


Рисунок 8.3 – Реєстраційна форма "Особисті дані"

8.2.2.6. Натиснувши на кнопку OK, отримати посилання для скачування скрипту генерації запиту на сертифікат, а також серійний номер, під яким зберігається цей запит (рис. 8.4).

8.2.2.7. Записати або запам'ятати номер запита.

8.2.2.8. Натиснувши на посилання "Скачати скрипт", завантажити файл скрипту **user_ca_ugrid.sh** на свій комп'ютер.

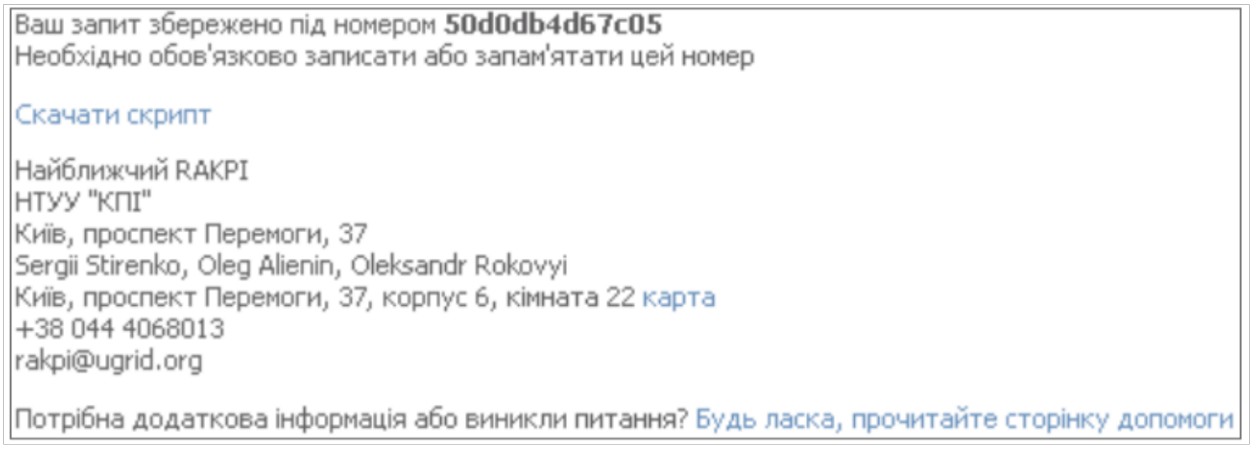


Рисунок 8.4 – Запрошення до скачування скрипту генерації запиту на сертифікат

8.2.2.9. Знайти окремий комп'ютер (або запустити віртуальну машину) з встановленою операційною системою Linux.

8.2.2.10. В командному рядку Linux-середовища запустити на виконання цей скрипт наступною командою:

```
[petro@computer ~]$ sh ./user_ca_ugrid.sh
```

8.2.2.11. Після того, як скрипт згенерує закритий ключ користувача і просить ввести пароль:

```
Generating a 2048 bit RSA private key
...+++
.....................+++
writing new private key to '/home/petro/.globus/userkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

двічі ввести пароль для шифрування закритого ключа (не відображається на екрані). УВАГА! Довжина пароля не менше 15 літер.

8.2.2.12. Далі скрипт генерує закритий ключ і запит на отримання сертифіката, інформує про це:

```
All done. Your private key is stored in the file
/home/petro/.globus/userkey.pem
Now you should upload the message, contained in the file
  /home/petro/.globus/userreq.mail
to  https://ca.ugrid.org
```

та виводить на екран модуль відкритого ключа користувача:

```
C5F29C0A24 856620084B734F077599F64ED2A7D5869EFE8686CC6F9B7F1
45ED2A78A48947FDCB29D46B8C1A6293D66B71123DFE013A62E2EBCE232C
66DE33FE5AC297972A4B7D5053DFD6BE29BF90DFE6D889853C3413D961B9
BD8BCF610D654A1B984111D12401D2AE634E66318D5719A854BC347CB666
A950B1B51B751E79B4814DFD6D3608D087A4CD0F4CCD77FCC882A3F87B3E
AB86F00A5DA428F8EA42CC147D52588F9DC273268B95A742EBD8A664E4A3
D1832831F9C4C0ED4A5863BCC2CCFBB1F763CA6755A4166723309AAC161B
1A468E5917E5B56B813AD30CF23ECB163DC98A0CAEBAF862575F002BC105
C16A9D24E8BFC1EC068CAEE 4923283385
```

8.2.2.13. Скопіювати у надійне місце закритий ключ користувача в зашифрованому вигляді, тобто файл **userkey.pem**, який був збережений скриптом у папку **/home/petro/.globus/** на локальному Linux-комп'ютері (тут **petro** – це назва домашньої папки користувача системи Linux, від імені якого запускався скрипт), а також запит на отримання грід-сертифіката, тобто файл **userreq.mail**, який був збережений скриптом у ту ж саму папку.

8.2.2.14. На своєму комп'ютері на сайті Центра сертифікації обрати пункт меню "Персональний сертифікат / Завантажити файл із запитом".

8.2.2.15. Вказати серійний номер запиту (збережений на кроці 8.2.2.7) та шлях до файлу із запитом у формі, що з'явиться:

8.2.2.16. Отримати на адресу електронної пошти, вказану на кроці 8.2.2.5, лист від Центру сертифікації про те, що запит прийнято до розгляду.

8.2.2.17. Роздрукувати у двох примірниках, заповнити та підписати паперову форму запиту на отримання сертифіката користувача (https://ca.ugrid.org/docs/request.pdf).

8.2.2.18. Особисто звернутися в Центр Сертифікації або в один з офіційних Реєстраційних центрів, перелік яких наведено за посиланням https://ca.ugrid.org/ra.php.

Під час звернення при собі мати:

– внутрішній паспорт;

– копію першої сторінки та сторінки з останньою фотографією внутрішнього паспорта (у двох примірниках);

– закордонний паспорт (якщо є);

– документ, що засвідчує причетність особи до досліджень в області грід-обчислень (наприклад, офіційний лист від керівника закладу / дослідницького проєкту, в якому працює/навчається користувач);

– дві копії заповненого і підписаного запиту на отримання сертифіката користувача, підписаного на кроці 8.2.2.17.

8.2.2.19. Центр Сертифікації підпише сертифікат протягом п'яти робочих днів і надішле подальші інструкції як його отримати.

8.2.2.20. Отримати на адресу електронної пошти, вказану на кроці 8.2.2.5, лист від Центру сертифікації про те, як отримати грід-сертифікат (файл з назвою **usercert.pem**), який має бути створений та підписаний в Центрі протягом п'яти робочих днів після звернення.

Зауважимо, що грід-сертифікат видається терміном на один рік. До закінчення цього терміну сертифікат можна продовжити без особистого звернення в Центр сертифікації або Реєстраційний центр, використовуючи ще діючий сертифікат, для чого потрібно обрати на сайті Центра сертифікації спочатку пункт меню "Персональний сертифікат / Оновлення сертифікату", а потім – "Персональний сертифікат / Завантажити файл із запитом". Докладні інструкції стосовно отримання та продовження терміну дії грід-сертифіката можна знайти на сторінці сайту "Допомога": https://ca.ugrid.org/help.php.

8.2.3. Перетворення персонального сертифіката з формату X509 у формат PK12

На початковій стадії розвитку грід-технологій користувачі для виконання своїх завдань були вимушені працювати у недружному оточенні UNIX-подібних операційних систем в пакетному режимі, надсилаючи в грід-середовище окремі команді з командного рідка. Делегування сертифікаті від

грід-користувача до грід-процеса шляхом створення тимчасових проксі-сертифікатів також здійснювалося вручну.

Згодом з'явилося багато більш зручних сервісів, внаслідок чого сучасні користувачі майже не використовують командний рядок, а свої завдання формують та запускають на виконання завдяки різноманітним сервісам, реалізованим зазвичай у вигляді веб-застосунків. Делегування повноважень також відбувається веб-сервісам, доступ до яких користувачам надають звичайні веб-браузери. Крім того в грід-сегменті традиційного Інтернету існує багато спеціалізованих веб-ресурсів, доступ до яких регламентується наявністю персонального грід-сертифіката.

Але традиційні веб-технології в переважній більшості використовують сертифікати у форматі, що він є не сумісним зі стандартом X509, в якому створюються сертифікати для гряд-середовища, зокрема ті, про які мова йшла вище (тобто pem-файли). Тому грід-користувач часто-густо повинен перетворювати свій грід-сертифікат з формату **PEM** у формат, придатний для використання у будь-якому веб-браузері. Найпростіше для цього використовувати формат **PKCS12** (тобто сертифікат у вигляді файлу з розширенням **.p12**).

Нижче наведено покрокову інструкцію з перетворення грід-сертифіката з формату PEM у формат PKCS12.

8.2.3.1. Знайти окремий комп'ютер (або запустити віртуальну машину) з встановленою операційною системою Linux. Скопіювати на нього файл сертифіката **usercert.pem** і файл закритого (приватного) ключа **userkey.pem**.

8.2.3.2. В командному рядку Linux-середовища запустити на виконання команду:

```
openssl pkcs12 -in usercert.pem -inkey userkey.pem -export -out usercert.p12
```

8.2.3.3. В процесі виконання команди буде виданий спочатку запит місця розташування файлу userkey.pem, потім – usercert.pem, якщо ці файли не розташовані в поточній папці. В такому випадку необхідно ввести повні шляхи до файлів.

8.2.3.4. Після цього буде виданий запит на введення пароля шифрування закритого ключа (той, що був визначений на кроці 8.2.2.11 попередньої інструкції).

8.2.3.5. Потім необхідно двічі ввести пароль, який буде використовуватися для шифрування PKCS12-файлу. Цей пароль потім потрібно буде вводити в програмі, в яку імпортується сертифікат (зокрема, у веб-браузері). УВАГА! Довжина пароля не менше 15 літер.

8.2.3.6. Сертифікат у форматі PKCS12, тобто файл **usercert.p12**, який буде згенеровано командою у випадку її успішного виконання, скопіювати у надійне місце.

8.3. Порядок виконання практичної роботи

Ознайомитись з теоретичним матеріалом до лабораторної роботи та виконати наступну послідовність дій.

8.3.1. Завантажити з середовища Teams на свій комп’ютер тестовий файл сертифіката **usercert.p12** (Команди /ЗК / Файли / Документи / General / Навчальні матеріали / 2. Завдання для лабораторних робот / usercert.p12).

Зауваження. Якщо вказаний файл відсутній в зазначеному місці, завантажити звідти файл **usercert.xxx** та перейменувати його на **usercert.p12**.

8.3.2. Встановити на свій комп’ютер (якщо потрібно) та відкрити браузер **Google Chrome**.

8.3.3. В правому верхньому куті натиснути символ "три крапки" (рис. 8.5).

8.3.4. Послідовно обрати пункти меню: "Налаштування" (у випадаючому меню) / Конфіденційність і безпека / Безпека / Керування сертифікатами.

8.3.5. У відкритому вікні "Сертифікати" послідовно обрати пункти меню: Імпорт / Далі / Ім'я файлу / Огляд (обрати папку з файлом usercert.p12; праворуч від поля "Ім'я файлу" обрати тип сертифіката: "Файли обміну приватною інформацією (*.pfx;*.p12)") / Далі / Пароль: (ввести пароль

"RS<21LjyYNE2023") / Далі / Автоматично обирати сховище на основі типу сертифіката / Далі / Готово.

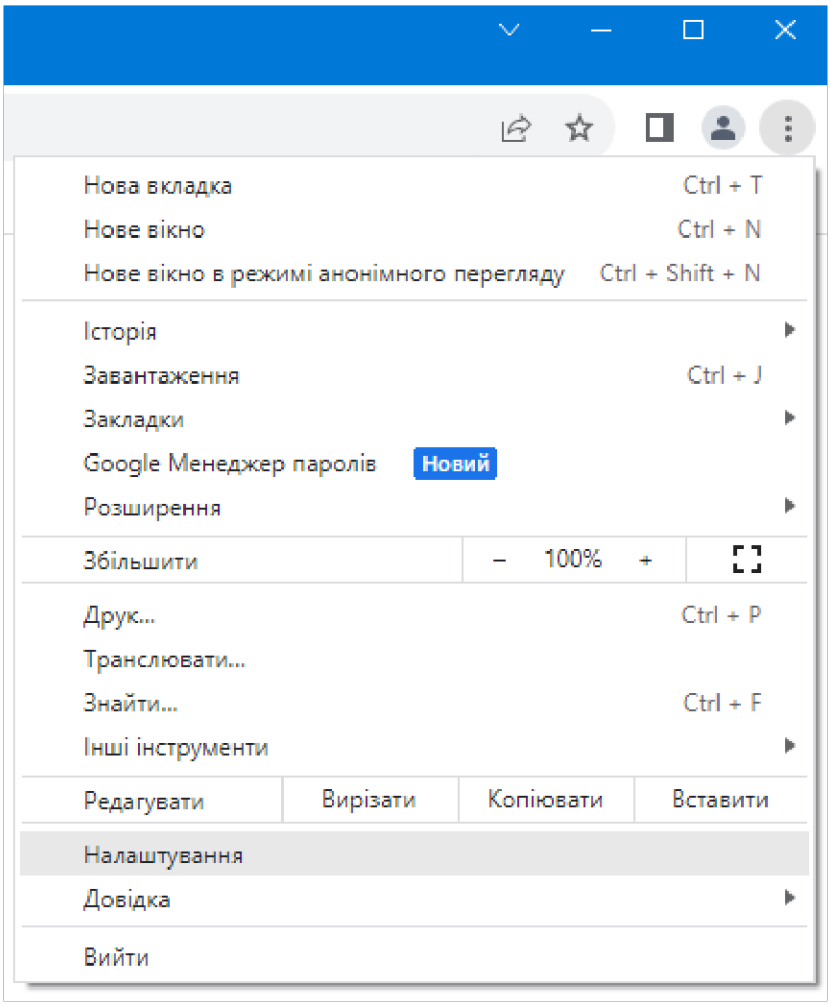


Рисунок 8.5 – Службове меню браузера Google Chrome

8.3.6. Зробити скріншот відкритого вікна "Сертифікати".

8.3.7. У відкритому вікні "Сертифікати" обрати рядок, що починається з "Sergiy Gilgurt…"; натиснути кнопку "Перегляд". На вкладинках "Загальні" та "Склад" продивитися інформацію про сертифікат (рис. 8.6).

8.3.8. Закрити вікно "Сертифікати". У адресному рядку браузера ввести адресу Сервісу ARGO моніторингу доступності/надійності європейської грід-інфраструктури (EGI): https://argo-mon.egi.eu/

8.3.9. Подивитися на реакцію браузера. Спробувати зрозуміти її причини. Зробити скріншот.

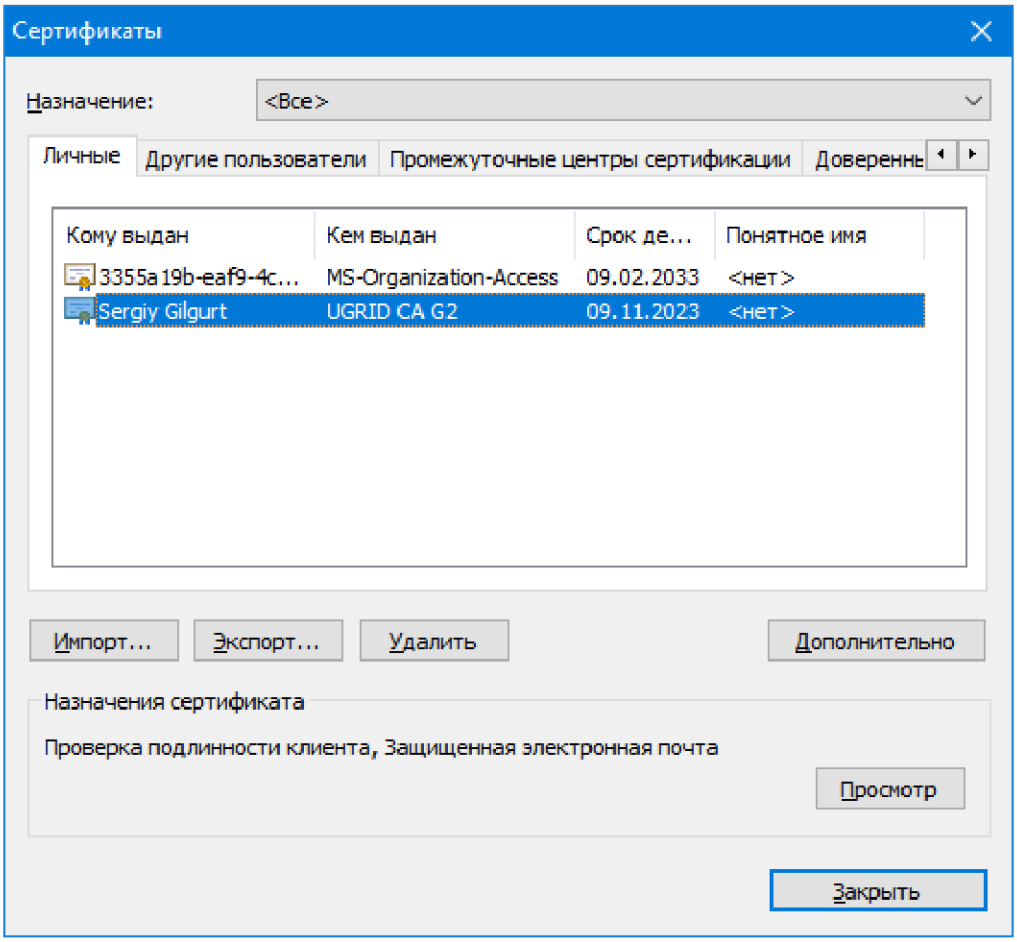


Рисунок 8.6 – Вікно "Сертифікати"

8.3.10. Встановити на свій комп’ютер (якщо потрібно) та відкрити браузер **Mozilla FireFox**.

8.3.11. В налаштуваннях браузера самостійно знайти вікно керування сертифікатами (Менеджер сертифікатів).

8.3.12. Виконати на цьому браузері послідовність дій, аналогічних пп. 8.3.5 - 8.3.7.

8.3.13. Підготувати звіт. В розділі про практичну частину записати послідовність команд, необхідних для відкриття вікна керування сертифікатами в браузері Mozilla FireFox, записану у формі, подібній до п. 8.3.4.

8.3.14. Додати до звіту три скріншоти:

- створений в п. 8.3.6;
- створений в п. 8.3.9;

– скрін-шот, подібний до такого, що зроблений в п. 8.3.6, але для браузера Mozilla FireFox.

8.4. Питання до самоконтролю

1. Який розділ прикладної математики використовується при створенні цифрових сертифікатів?

2. Які персональні дані про користувача містяться у грід-сертифікаті?

3. Який механізм використовується для делегування повноважень сертифікованого користувача грід-процесам, що вони на віддалених обчислювальних вузлах виконують його завдання без його безпосередньої участі та контролю з його боку?

4. Чому, на вашу думку, в п. 8.3.9 ви отримали саме таку реакцію браузера?

5. Чи вважаєте ви достатньо надійним пароль, який вводили в п. 8.3.5?

6. В будь-якому текстовому редакторі переключіть клавіатуру в режим введення кириличних символів (українська розкладка), послідовно натисніть клавіші клавіатури з латинськими символами **RS<21LjyYNE2023** та наведіть послідовність символів, які отримали в результаті.

7. Чи змінилася ваша думка стосовно надійності згаданого паролю?

8.5. Вимоги до оформлення звіту

Звіт з лабораторної роботи подається у вигляді текстового файлу (у форматі .doc, .docx або .pdf) та має містити наступні складові:

1) титульний лист (див. Додаток А);

2) короткі теоретичні відомості;

3) практична частина із зазначенням завдань згідно варіанту, докладним описом послідовності дій щодо його виконання та наведенням отриманих результатів;

4) відповіді на питання до самоконтролю (із зазначенням самих питань);

5) висновки щодо виконаної лабораторної роботи.

8.6. Література до Лабораторної роботи 8

Рекомендовані літературні джерела до виконання Лабораторної роботи 8: [1, 2, 16].

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII із змінами та доповненнями [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12# Text. – Назва з екрана.

2. Основи інформаційної безпеки [Електронний ресурс] : навч. посіб. / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с. – Режим доступу: http://ir.lib.vntu.edu.ua//handle/123456789/21843. – Назва з екрана.

3. Безпека програм та даних [Електронний ресурс] : навч. посіб. / В. І. Горбенко, А. О. Лісняк. – Запоріжжя : ЗНУ, 2022. – 72 с. – Режим доступу: https://dspace.znu.edu.ua/jspui/bitstream/12345/11649/1/HORBENKOLISNIAK.doc. – Назва з екрана.

4. Служба підтримки Microsoft. Мережевий захист у службі "Безпека у Windows" [Електронний ресурс] // Microsoft. – Режим доступу : https://support.microsoft.com/uk-ua/windows/мережевий-захист-у-службі-безпека-у-windows-aef9838b-d081-fd75-3b1b-e5fa794c003b. – Назва з екрана.

5. Посібник з налаштування брандмауера в Windows 10 [Електронний ресурс]. – Режим доступу : https://uk.soringpcrepair.com/firewall-settings-in-windows-10/. – Назва з екрана.

6. Налаштування брандмауера у Windows 7/8/10 [Електронний ресурс] / /ComEL. – Режим доступу: https://www.comelzv.net/index.php?option=com_content&view=article&id=73&Itemid=103. – Назва з екрана.

7. Віртуальні локальні мережі VLAN : методичні вказівки [Електронний ресурс] / уклад. С. І. Приходько, О. С. Жученко, М. А. Штомпель, С. В. Сколота. – Харків : УкрДУЗТ, 2018. – 41 с. – Режим доступу:

http://lib.kart.edu.ua/bitstream/123456789/1362/3/Методичні%20вказівки.pdf. – Назва з екрана.

8. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко. – Харків: НТУ «ХПІ», 2019. – 194 с. – Режим доступу: https://core.ac.uk/download/pdf/333611355.pdf. – Назва з екрана.

9. Методичні вказівки до лабораторних робіт з дисципліни «Бездротові технології» для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання. Мережі WiFi. Частина 2 [Електронний ресурс] / уклад. Г. Г. Киричек. – Запоріжжя : Національний університет «Запорізька політехніка», 2019. – 34 с. – Режим доступу: http://eir.zp.edu.ua/bitstream/123456789/4924/1/ M07292.pdf. – Назва з екрана.

10.Обзор Wi-Fi роутера TP-LINK TL-WR940N/TL-WR941ND [Електронний ресурс] // TopNet. – Режим доступу: https://topnet.com.ua/instrukcii-po-nastrojke-routerov/ nastrojka-wi-fi-routera-tp-link-tl-wr940n-tl-wr941nd/. – Назва з екрана.

11. Захист інформації в телекомунікаційних системах [Електронний ресурс] : навч. посіб. / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов, В. М. Чуприн, О. О. Горбунов. – Київ : НАУ, 2009. – 380 с. – Режим доступу: https://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf. – Назва з екрана.

12. Методичні вказівки до лабораторних робіт з дисципліни "Програмно-апаратне забезпечення та захист мобільних пристроїв" [Електронний ресурс] / уклад. О. А. Лаптєв, Т. О. Гришанович, Я. В. Жолоб, О. К. Жигаревич. – Луцьк : ВНУ ім. Лесі Українки, 2022. – 99 с. – Режим доступу: https://evnuir.vnu.edu.ua/bitstream/123456789/21574/1/PAZZMP.pdf. – Назва з екрана.

13. Основи управління інформаційною безпекою [Електронний ресурс] : навч. посіб. / А. М. Гребенюк, Л. В. Рибальченко. – Дніпро : ДДУВС,

2020. – 144 с. – Режим доступу: http://er.dduvs.in.ua/xmlui/bitstream/handle/123456789/5717/ПОСІБНИК%20ОУІБ%20.pdf?sequence=1&isAllowed=y. – Назва з екрана.

14. Безпека і кібербезпека смартфонів [Електронний ресурс] // DATAMI, 25 серпня 2020. – Режим доступу: https://datami.ua/bezpeka-i-kiberbezpeka-smartfoniv/. – Назва з екрана.

15. Литовка Т. В. Пояснювальна записка до дипломного проекту магістра на тему «Розробка вдосконаленого способу маскування лінійного коду» // Інститут інформатики та радіоелектроніки. Факультет радіоелектроніки та телекомунікацій. Кафедра захисту інформації [Електронний ресурс]. – Запоріжжя: ЗНТУ, 2018. – 147 с. – Режим доступу: http://eir.zntu.edu.ua/bitstream/123456789/4876/1/ MR_Lytovka.pdf . – Назва з екрана.

16. Центр сертифікації Ukrainian Grid Certification Authority [Електронний ресурс] // Computer Engineering Department, KPI 2007-2024. – Режим доступу: https://ca.ugrid.org/. – Назва з екрана.

ДОДАТОК А. Приклад оформлення титульного листа лабораторної роботи

ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
Факультет комп'ютерно-інформаційних технологій та автоматизації
Кафедра прикладної математики та інформатики

ЗВІТ З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № ***N***

з дисципліни «Захист комп’ютерних мереж»

за темою: «***Назва лабораторної роботи***»

Виконав(ла):

Студент(ка) гр. ***КІБ-NN***

Ім'я ПРИЗВИЩЕ

Перевірив:

Сергій ГІЛЬГУРТ

Луцьк – 20**NN**