МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

VPN-ІНФРАСТРУКТУРА ДЛЯ МАЛОГО ОФІСУ З РІЗНИМИ РІВНЯМИ ДОСТУПУ

Виконав: студент групи 1К-22
спеціальності
123 «Комп’ютерна інженерія»
Даніїл БУРТОВИЙ
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____Наталя ФАЛЬЧЕНКО

(підпис)

«_____» _____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Буртовому Даніїлу Костянтинович

1. Тема кваліфікаційної роботи «VPN-інфраструктура для малого офісу з різними рівнями доступу»

   Керівник роботи Медолиз Маргарита Миколаївна, викладач вищої категорії, затверджені наказом закладу передвищої освіти від «06». жовтня 2025 року № 84/1у
2. Строк подання студентом кваліфікаційної роботи 08.06.2026
3. Вихідні дані до кваліфікаційної роботи: нормативні документи та стандарти, джерела з VPN та мережевої безпеки, наукові статті та електронні ресурси, практичні ресурси та платформи моделювання
4. Зміст кваліфікаційної роботи (питання, що необхідно розглянути): VPN-технології та їх класифікація; протоколи тунелювання; сегментація мережі; контроль доступу в мережі; моделювання корпоративних мереж
5. Дата видачі завдання 15.10.2025 р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Основи VPN-технологій	09.12.2025	
3	Розділ 2 VPN-інфраструктура для малого офісу	10.03.2026	
4	Розділ 3 Реалізація та налаштування VPN-інфраструктури	28.04.2026	
5	Розділ 4 Оцінка ефективності та безпеки системи	12.05.2026	
6	Висновки	20.05.2026	
7	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
8	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	05.06.2026	
9	Подання кваліфікаційної роботи на затвердження завідувачу ЦК (за 7 днів до захисту)	08.06.2026	

Студент _____ Даніїл БУРТОВИЙ
(підпис)

Керівник роботи _____ Маргарита МЕДОЛИЗ
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота присвячена проєктуванню та моделюванню VPN-інфраструктури для малого офісу з різними рівнями доступу користувачів. У роботі розглянуто теоретичні засади функціонування віртуальних приватних мереж.

На основі аналізу потреб малого офісу сформовано вимоги до VPN-інфраструктури з урахуванням безпеки, масштабованості, відмовостійкості та простоти адміністрування. Розроблено структуру мережі, яка передбачає використання VPN-тунелю, сегментацію мережі, застосування списків контролю доступу та рольову модель керування доступом для адміністраторів, співробітників, віддалених і гостьових користувачів.

Практична частина роботи реалізована в середовищі Cisco Packet Tracer. Створено модель мережі малого офісу, налаштовано VPN-тунель між локальним і віддаленим сегментами мережі, реалізовано політики розмежування доступу та виконано тестування працездатності запропонованого рішення.

Результати дослідження підтвердили можливість забезпечення захищеного віддаленого доступу до корпоративних ресурсів із дотриманням принципів інформаційної безпеки та контролю прав користувачів.

Ключові слова: VPN, ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, МЕРЕЖЕВА ІНФРАСТРУКТУРА, МАЛИЙ ОФІС, ВІДДАЛЕНИЙ ДОСТУП, ІНФОРМАЦІЙНА БЕЗПЕКА, WIREGUARD, OPENVPN, ACL, МАРШРУТИЗАЦІЯ, СЕГМЕНТАЦІЯ МЕРЕЖІ, CISCO PACKET TRACER.

ABSTRACT

The qualification work is devoted to the design and modeling of a VPN infrastructure for a small office with different levels of user access. The work considers the theoretical principles of the functioning of virtual private networks.

Based on the analysis of the needs of a small office, requirements for the VPN infrastructure were formed, taking into account security, scalability, fault tolerance and ease of administration. A network structure was developed, which involves the use of a VPN tunnel, network segmentation, the use of access control lists and a role-based access control model for administrators, employees, remote and guest users.

The practical part of the work was implemented in the Cisco Packet Tracer environment. A small office network model was created, a VPN tunnel was configured between the local and remote network segments, access separation policies were implemented and the performance of the proposed solution was tested.

The results of the study confirmed the possibility of providing secure remote access to corporate resources while adhering to the principles of information security and user rights control.

Keywords: VPN, VIRTUAL PRIVATE NETWORK, NETWORK INFRASTRUCTURE, SMALL OFFICE, REMOTE ACCESS, INFORMATION SECURITY, WIREGUARD, OPENVPN, ACL, ROUTING, NETWORK SEGMENTATION, CISCO PACKET TRACER.

ЗМІСТ

ВСТУП

У сучасних умовах функціонування малого офісу значна частина робочих процесів залежить від стабільного та захищеного доступу до інформаційних ресурсів. Працівники використовують файлові сховища, бази даних, системи електронного документообігу, бухгалтерські програми, внутрішні сервіси та адміністративні панелі мережевого обладнання. При цьому доступ до таких ресурсів дедалі частіше здійснюється не лише з локальної мережі офісу, а й віддалено: з дому, з іншого міста, під час відрядження або з мобільних пристроїв.

За таких умов актуальним є створення VPN-інфраструктури, яка забезпечує захищений канал передавання даних між користувачем і корпоративною мережею. VPN дає змогу зменшити ризики перехоплення трафіку, несанкціонованого доступу до внутрішніх ресурсів і неконтрольованого використання службових даних. Особливого значення набуває розмежування прав користувачів, оскільки адміністратор, штатний працівник, віддалений користувач і гість не повинні мати однаковий рівень доступу до мережевих ресурсів.

Актуальність теми зумовлена потребою малого офісу в поєднанні безпеки, доступності, економічності та простоти адміністрування мережевої інфраструктури. На відміну від великих підприємств, малий офіс зазвичай має обмежений бюджет і не завжди може використовувати дорогі корпоративні рішення. Тому розробка VPN-інфраструктури з різними рівнями доступу є практично важливим завданням, спрямованим на підвищення захищеності та керованості офісної мережі.

Мета роботи – проєктування VPN-інфраструктури для малого офісу з різними рівнями доступу користувачів, що забезпечує захищене віддалене підключення, контроль доступу до внутрішніх ресурсів і стабільну роботу мережевого середовища.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Охарактеризувати поняття VPN-технологій, їх призначення та особливості функціонування.
2. Проаналізувати типи VPN-з’єднань і сучасні VPN-протоколи.
3. Визначити потреби малого офісу щодо захищеного віддаленого доступу.
4. Сформувати вимоги до VPN-інфраструктури з урахуванням безпеки, масштабованості, відмовостійкості та простоти адміністрування.
5. Розробити структуру мережі малого офісу з використанням VPN-тунелю, firewall, ACL-політик і логічної сегментації.
6. Побудувати модель рівнів доступу для адміністраторів, співробітників, гостьових і віддалених користувачів.
7. Оцінити продуктивність, захищеність та економічну доцільність запропонованої VPN-інфраструктури.

Об’єктом дослідження є мережева інфраструктура малого офісу, що потребує організації захищеного локального та віддаленого доступу до корпоративних інформаційних ресурсів.

Предметом дослідження є принципи, засоби та методи побудови VPN-інфраструктури малого офісу з різними рівнями доступу користувачів, зокрема VPN-тунелювання, автентифікація, ACL-політики, firewall, маршрутизація та сегментація мережі.

Практичне значення роботи полягає в розробці моделі VPN-інфраструктури, яку можна використовувати як основу для організації захищеної мережевої взаємодії в малому офісі. Використання віртуальних приватних мереж дає змогу забезпечити віддалений доступ працівників до службових ресурсів, обмежити права користувачів відповідно до їхніх функціональних ролей і знизити ризик несанкціонованого доступу до внутрішніх сегментів мережі.

РОЗДІЛ 1 ОСНОВИ VPN-ТЕХНОЛОГІЙ

1.1. Поняття та призначення VPN

VPN, або віртуальна приватна мережа, є технологією створення захищеного логічного каналу зв’язку між користувачем і корпоративною мережею через відкриту або потенційно незахищену мережу, зокрема Інтернет. Її сутність полягає в тому, що передавання даних здійснюється не у відкритому вигляді, а через спеціальний захищений тунель. Такий підхід дає змогу малому офісу організувати безпечний віддалений доступ до внутрішніх ресурсів без використання дорогих виділених каналів зв’язку.

Основний принцип роботи VPN ґрунтується на тунелюванні, шифруванні та автентифікації. Тунелювання передбачає інкапсуляцію мережевих пакетів, тобто передавання внутрішнього трафіку офісної мережі всередині зовнішнього з’єднання. Завдяки цьому користувач може отримувати доступ до серверів, баз даних, файлових сховищ або службових застосунків так, ніби його пристрій фізично підключений до локальної мережі підприємства. У документації Cisco VPN розглядається як засіб захищеної передачі трафіку в IP-мережах із використанням механізмів тунелювання та криптографічного захисту [8].

Важливим елементом VPN є шифрування, яке забезпечує конфіденційність переданих даних. Навіть у разі перехоплення трафіку стороння особа не може прочитати його зміст без відповідного ключа. Це особливо актуально для працівників малого офісу, які підключаються до корпоративної мережі з дому, публічної Wi-Fi-мережі або під час відрядження. Для реалізації захищеного обміну даними можуть використовуватися різні протоколи, зокрема IPsec, OpenVPN і WireGuard. Наприклад, OpenVPN підтримує роботу із сертифікатами, ключами та захищеним клієнт-серверним з’єднанням [9].

Автентифікація у VPN виконує функцію перевірки користувача або пристрою перед наданням доступу до мережі. Вона може здійснюватися за

допомогою паролів, цифрових сертифікатів, ключів або багатофакторної перевірки. Для малого офісу це має практичне значення, оскільки різні категорії користувачів повинні мати різний рівень доступу: адміністратор – до мережевого обладнання, працівник – до робочих сервісів, гість – лише до Інтернету. Такий підхід узгоджується з принципами Zero Trust, відповідно до яких доступ має надаватися не автоматично, а після перевірки ролі, прав і контексту підключення [2].

Отже, VPN є ключовою технологією для побудови безпечної інфраструктури малого офісу. Вона забезпечує захищене передавання даних, віддалений доступ до корпоративних ресурсів, автентифікацію користувачів і можливість поділу доступу за ролями. Саме тому VPN доцільно розглядати не лише як засіб шифрування трафіку, а як основу для організації контрольованої та захищеної офісної мережі.

1.2 Типи VPN-з’єднань

VPN-з’єднання класифікують за способом організації доступу, типом учасників мережевої взаємодії та технологією захисту трафіку. У межах малого офісу це питання має не лише теоретичне, а й прикладне значення, оскільки різні типи VPN розв’язують різні завдання: підключення віддалених працівників, об’єднання філій, захист доступу до вебсервісів, сегментацію прав користувачів або створення захищеного каналу між маршрутизаторами. Правильний вибір типу VPN дає змогу поєднати безпеку, економічність і простоту адміністрування.

Найпоширенішим варіантом для малого офісу є Remote Access VPN. Такий тип з’єднання використовується тоді, коли окремий користувач підключається до корпоративної мережі ззовні: з дому, іншого міста, коворкінгу або під час відрядження. На пристрої користувача встановлюється VPN-клієнт, який після автентифікації створює захищений тунель до VPN-сервера офісу. Працівник отримує доступ не до всієї мережі автоматично, а

лише до тих ресурсів, які дозволені його роллю: файлового сервера, CRM-системи, бухгалтерської бази або внутрішнього порталу. У рекомендаціях NSA та CISA підкреслюється, що віддалені VPN-рішення мають бути належно захищені, регулярно оновлюватися та використовувати надійні механізми автентифікації [12].

Site-to-Site VPN застосовується для об’єднання двох або більше локальних мереж. Наприклад, якщо підприємство має головний офіс і невелику філію, цей тип VPN дає змогу з’єднати їх через Інтернет так, ніби вони є частинами єдиної корпоративної мережі. Зазвичай таке з’єднання встановлюється між маршрутизаторами або міжмережевими екранами, тому користувачам не потрібно вручну запускати VPN-клієнт. Для малого бізнесу Site-to-Site VPN доцільний у разі наявності кількох офісів, складу, торгової точки або віддаленого серверного майданчика. Cisco розглядає такі VPN-рішення як один із базових способів організації захищеного зв’язку між мережевими вузлами через IP-інфраструктуру [7].

Client-to-Site VPN за змістом близький до Remote Access VPN, однак акцент у ньому робиться саме на підключенні окремого клієнтського пристрою до мережі організації. У такій моделі ноутбук, смартфон або робоча станція виступає клієнтом, а маршрутизатор, firewall або окремий сервер виконує роль VPN-шлюзу. Для малого офісу цей тип є практичним, оскільки дозволяє швидко надати працівнику контрольований доступ до внутрішніх сервісів без фізичної присутності в офісі. Наприклад, системний адміністратор може отримати доступ до панелі керування сервером, менеджер – до CRM, а бухгалтер – до фінансової бази. Безпека такого підключення залежить від поєднання VPN, правил firewall, ACL і політик доступу.

Окремо виділяють MPLS VPN, який використовується переважно в корпоративних мережах провайдерського рівня. MPLS VPN ґрунтується на технології багатопротокольної комутації міток і дає змогу створювати

ізольовані віртуальні мережі для різних клієнтів у межах інфраструктури оператора зв’язку. Його перевагами є стабільність, керованість, можливість гарантування якості обслуговування та зручність для великих територіально розподілених компаній. Водночас для малого офісу MPLS VPN часто є менш доцільним через вищу вартість і залежність від послуг провайдера. У невеликих організаціях частіше використовують OpenVPN, WireGuard, IPsec або SSL VPN, оскільки вони дешевші, простіші для розгортання і краще відповідають обмеженому бюджету.

Важливе місце серед VPN-рішень займають SSL VPN та IPsec VPN. SSL VPN використовує криптографічні механізми, пов’язані із захистом вебз’єднань, і часто застосовується для доступу до окремих корпоративних сервісів через браузер або спеціальний клієнт. Такий варіант зручний для користувачів, яким не потрібен повний доступ до всієї локальної мережі. Наприклад, працівнику можна надати доступ тільки до внутрішнього вебпорталу або конкретної службової системи. IPsec VPN, навпаки, частіше використовується для глибшого мережевого захисту, зокрема для Site-to-Site-з’єднань або повноцінного тунелювання IP-трафіку. У документації Cisco IPsec описується як набір механізмів для захисту IP-пакетів, що забезпечує конфіденційність, цілісність і автентифікацію даних [8].

Як видно з таблиці 1.1, для малого офісу найбільш практичними є Remote Access VPN, Client-to-Site VPN, SSL VPN та IPsec VPN. Вони дають змогу організувати захищений доступ без значних витрат на провайдерські корпоративні канали. Site-to-Site VPN доцільний тоді, коли офіс має філію або окремий віддалений майданчик. MPLS VPN є технічно надійним, однак у більшості випадків він економічно виправданий для середніх і великих організацій, а не для малого офісу.

Таблиця 1.1 – Порівняльна характеристика основних типів VPN-з’єднань

Тип VPN-з’єднання	Основне призначення	Типовий приклад використання	Переваги	Обмеження
Remote Access VPN	Віддалений доступ окремого користувача до офісної мережі	Працівник підключається до файлового сервера з дому	Зручний для дистанційної роботи, підтримує індивідуальні права доступу	Потребує захисту клієнтських пристроїв і надійної автентифікації
Site-to-Site VPN	Об’єднання кількох локальних мереж	Головний офіс з’єднується з філією або складом	Не потребує запуску VPN-клієнта на кожному ПК, зручний для філій	Складніше налаштування маршрутизації та firewall
Client-to-Site VPN	Підключення конкретного пристрою до мережі організації	Ноутбук адміністратора підключається до серверної мережі	Гнучке керування доступом окремих користувачів	Залежить від налаштування клієнтського ПЗ і політик безпеки
MPLS VPN	Ізольована корпоративна мережа через інфраструктуру провайдера	Об’єднання багатьох офісів великої компанії	Стабільність, керованість, підтримка якості обслуговування	Висока вартість, залежність від провайдера
SSL VPN	Доступ до окремих сервісів через захищене з’єднання	Доступ до внутрішнього вебпорталу або службової системи	Зручність для користувача, можливість обмеженого доступу	Не завжди підходить для повного доступу до локальної мережі
IPsec VPN	Захист IP-трафіку між вузлами або мережами	Захищений тунель між маршрутизаторами офісів	Високий рівень захисту, придатність для Site-to-Site	Може бути складнішим у налаштуванні

Отже, тип VPN-з’єднання потрібно обирати не формально, а відповідно до реальних потреб організації. Якщо головне завдання полягає у підключенні працівників з дому, доцільним є Remote Access або Client-to-Site VPN. Якщо потрібно об’єднати кілька офісів, варто застосовувати Site-to-Site VPN на основі IPsec. Якщо доступ має бути обмежений лише окремими вебсервісами, зручним варіантом є SSL VPN. Для проєктованої інфраструктури малого офісу оптимальним є поєднання Client-to-Site VPN для віддалених працівників із

політиками розмежування доступу, що дозволяє забезпечити безпеку, контроль і гнучкість адміністрування.

1.3 Протоколи VPN

Протоколи VPN визначають спосіб створення захищеного каналу, порядок автентифікації користувача, методи шифрування та особливості передавання трафіку між клієнтом і сервером. Для малого офісу вибір протоколу має практичне значення, оскільки від нього залежать швидкість роботи, рівень захисту, складність налаштування та сумісність із клієнтськими пристроями. Найчастіше в практиці використовують PPTP, L2TP/IPsec, OpenVPN, WireGuard і SSTP.

PPTP є одним із найстаріших VPN-протоколів. Його перевагою є просте налаштування та підтримка в багатьох операційних системах. Проте з погляду сучасної інформаційної безпеки PPTP вважається застарілим, оскільки має слабші механізми захисту порівняно з новішими рішеннями. Тому в інфраструктурі малого офісу його доцільно розглядати лише як історичний або резервний варіант, але не як основний протокол для захисту корпоративного трафіку.

L2TP/IPsec поєднує тунелювання L2TP із криптографічним захистом IPsec. Сам по собі L2TP не забезпечує шифрування, тому на практиці використовується разом з IPsec, який відповідає за конфіденційність, цілісність і автентифікацію даних. Такий протокол може застосовуватися для віддаленого доступу або об’єднання мереж, однак потребує уважного налаштування ключів, політик безпеки та параметрів firewall. У документації Cisco IPsec подається як технологія захисту IP-трафіку, що використовується для створення безпечних VPN-з’єднань [8].

OpenVPN є поширеним відкритим VPN-рішенням, яке підтримує роботу із сертифікатами, ключами, різними режимами шифрування та клієнт-серверною моделлю. Його перевагою є гнучкість налаштування, підтримка різних операційних систем і можливість використання як у малих офісах, так

і в більших корпоративних мережах. Для проєктування офісної VPN-інфраструктури OpenVPN є зручним варіантом, оскільки дозволяє поєднати захищений доступ із розмежуванням прав користувачів [9].

WireGuard є сучасним VPN-протоколом, який орієнтований на простоту конфігурації, високу продуктивність і використання сучасних криптографічних механізмів. Його часто застосовують у рішеннях MikroTik, pfSense та інших мережевих платформах. Для малого офісу WireGuard є привабливим через меншу складність налаштування порівняно з деякими традиційними VPN-рішеннями та добру швидкодію. У документації MikroTik WireGuard розглядається як сучасний інструмент для створення захищених тунелів між пристроями [13].

SSTP використовує захищене з’єднання через SSL/TLS і часто асоціюється з екосистемою Microsoft. Його перевагою є можливість роботи через порт 443, який зазвичай використовується для HTTPS-трафіку. Це може бути корисно тоді, коли інші VPN-протоколи блокуються мережею або firewall. Водночас SSTP менш універсальний порівняно з OpenVPN або WireGuard, тому в малому офісі його доцільно використовувати переважно у середовищах, де основними клієнтськими пристроями є комп’ютери з Windows.

Таблиця 1.2 визначає порівняльну характеристику VPN-протоколів, які можуть бути використані для побудови захищеної мережевої інфраструктури малого офісу.

Таблиця 1.2 – Порівняльна характеристика VPN-протоколів

Протокол	Основне призначення	Переваги	Обмеження	Доцільність для малого офісу
PPTP	Базове VPN-з’єднання	Просте налаштування, широка сумісність	Застарілий рівень безпеки	Небажаний як основний протокол
L2TP/IPsec	Захищене тунелювання з використанням IPsec	Кращий захист, ніж PPTP; підтримка багатьма ОС	Складніше налаштування, залежність від коректних IPsec-політик	Можливий для типових VPN-з’єднань

Продовження таблиці 1.2

OpenVPN	Гнучкий віддалений доступ	Сертифікати, кросплатформність, надійне шифрування	Потребує окремого клієнта та налаштування конфігурацій	Доцільний для малого офісу
WireGuard	Сучасні швидкі VPN-тунелі	Висока продуктивність, простіша конфігурація	Потребує правильного керування ключами	Дуже доцільний для малого офісу
SSTP	VPN через SSL/TLS	Може працювати через HTTPS-порт 443	Менша універсальність, орієнтація на Windows-середовище	Доцільний для Windows-інфраструктури

Отже, для сучасної VPN-інфраструктури малого офісу найдоцільніше використовувати OpenVPN або WireGuard. OpenVPN забезпечує гнучкість і широкі можливості налаштування, тоді як WireGuard має переваги у швидкодії та простоті конфігурації. L2TP/IPsec може застосовуватися як альтернативне рішення, SSTP – для середовищ із переважанням Windows-клієнтів, а PPTP не варто використовувати як основний протокол через застарілі механізми захисту.

1.4 Аналіз сучасних рішень для малого офісу

Для побудови VPN-інфраструктури малого офісу можуть використовуватися різні програмні та апаратні рішення, які відрізняються вартістю, складністю налаштування, рівнем безпеки та можливостями адміністрування. Найпоширенішими варіантами є MikroTik, Cisco, pfSense, OpenVPN Access Server та SoftEther VPN.

MikroTik є зручним рішенням для малого офісу завдяки доступній вартості обладнання, підтримці маршрутизації, firewall, VLAN та VPN-протоколів. Особливо важливою є підтримка WireGuard, що дає змогу створювати швидкі й відносно прості VPN-тунелі для віддалених користувачів або з’єднання між офісами [13]. Cisco орієнтований на більш професійну мережеву інфраструктуру. Його перевагами є висока надійність, розвинені

механізми ACL, IPsec VPN, маршрутизації та централізованого адміністрування. Водночас для малого офісу Cisco може бути дорожчим і складнішим у налаштуванні, ніж MikroTik або pfSense [1].

pfSense є популярним рішенням на базі firewall-шлюзу, яке підтримує різні VPN-технології, зокрема IPsec, OpenVPN і WireGuard. Його доцільно використовувати тоді, коли малому офісу потрібне поєднання VPN-сервера, firewall, маршрутизатора та системи контролю доступу в одному середовищі [3]. OpenVPN Access Server є спеціалізованим рішенням для організації віддаленого доступу. Його перевага полягає у зручному керуванні користувачами, сертифікатами та клієнтськими підключеннями. Таке рішення підходить для офісу, де основним завданням є безпечне підключення працівників із дому або з інших локацій [10].

SoftEther VPN є гнучким програмним VPN-рішенням, яке підтримує кілька протоколів і може використовуватися як альтернатива OpenVPN або IPsec. Його перевагою є універсальність, однак для навчального або малого офісного проєкту воно потребує уважного налаштування політик доступу та контролю безпеки.

На основі аналізу програмно-апаратних рішень для побудови VPN-інфраструктури та захисту мережі малого офісу, які надані в таблиці 1.3, для малого офісу найбільш практичними є MikroTik, pfSense та OpenVPN Access Server. MikroTik доцільний за обмеженого бюджету, pfSense – коли потрібен повноцінний firewall і VPN-шлюз, а OpenVPN Access Server – коли головним завданням є керований віддалений доступ працівників.

Таблиця 1.3 – Порівняння сучасних VPN-рішень для малого офісу

Рішення	Основне призначення	Переваги	Обмеження
MikroTik	Маршрутизація, firewall, VPN	Доступна ціна, підтримка WireGuard, VLAN	Потребує знання RouterOS
Cisco	Корпоративна мережева інфраструктура	Надійність, ACL, IPsec, масштабованість	Вища вартість і складність

Продовження таблиці 1.3

pfSense	Firewall і VPN-шлюз	OpenVPN, IPsec, WireGuard в одному рішенні	Потребує окремого пристрою або сервера
OpenVPN Access Server	Віддалений доступ користувачів	Зручне керування клієнтами й сертифікатами	Орієнтація переважно на OpenVPN
SoftEther VPN	Універсальний програмний VPN	Підтримка різних протоколів	Потребує точного налаштування безпеки

У даному розділі визначено теоретичні основи VPN-технологій як засобу захищеної мережевої взаємодії в малому офісі. Встановлено, що VPN забезпечує тунелювання, шифрування, автентифікацію користувачів і контрольований доступ до внутрішніх ресурсів.

Аналіз типів VPN-з’єднань показав, що для малого офісу найбільш доцільними є Remote Access VPN, Client-to-Site VPN, SSL VPN та IPsec VPN, оскільки вони відповідають потребам віддаленої роботи й розмежування доступу. Порівняння протоколів засвідчило переваги OpenVPN і WireGuard, які поєднують належний рівень безпеки, продуктивність і практичну зручність налаштування. Отже, вибір VPN-рішення має ґрунтуватися на вимогах безпеки, вартості, масштабованості та простоти адміністрування.

РОЗДІЛ 2 VPN-ІНФРАСТРУКТУРА ДЛЯ МАЛОГО ОФІСУ

2.1 Аналіз потреб малого офісу

Проєктування VPN-інфраструктури малого офісу потребує попереднього визначення організаційних, технічних і безпекових вимог, оскільки саме ці параметри впливають на вибір архітектури мережі, типу VPN-з’єднання, моделі автентифікації та засобів контролю доступу. У межах цієї роботи малий офіс розглядається як організаційне середовище з обмеженою кількістю користувачів, локальними інформаційними ресурсами, потребою у віддаленому доступі та відносно невеликим бюджетом на розгортання мережевої інфраструктури.

Кількість користувачів є одним із базових параметрів проєктування. Для малого офісу характерною є наявність приблизно 10-20 робочих місць, які можуть охоплювати адміністративний персонал, бухгалтерію, менеджерів, технічного спеціаліста та тимчасових або гостьових користувачів. Така структура потребує не лише забезпечення доступу до мережі, а й розмежування прав між різними категоріями користувачів. Зокрема, адміністратор має отримувати доступ до мережевого обладнання та серверних ресурсів, штатні працівники – до робочих сервісів, а гостьові користувачі – лише до зовнішнього Інтернету без можливості взаємодії з внутрішніми сегментами мережі.

Потреба у віддаленому доступі зумовлена поширенням дистанційної та змішаної форми роботи. Для малого офісу це означає необхідність забезпечити захищене підключення працівників до внутрішніх ресурсів поза межами локальної мережі. Такими ресурсами можуть бути файловий сервер, система електронного документообігу, база клієнтів, бухгалтерська система або внутрішні адміністративні сервіси. У цьому контексті VPN виконує функцію контрольованого каналу доступу, який має поєднувати шифрування трафіку, автентифікацію користувача та перевірку його прав. Застосування такого підходу узгоджується з принципами Zero Trust, відповідно до яких факт

підключення до мережі не повинен автоматично означати повний доступ до всіх ресурсів [2].

Захист корпоративних ресурсів є центральною вимогою до проєктованої інфраструктури. Основними об’єктами захисту виступають службові документи, облікові записи користувачів, конфігурації мережевого обладнання, внутрішні бази даних і канали передавання інформації. Для зниження ризику несанкціонованого доступу VPN має поєднуватися з міжмережевим екраном, списками контролю доступу, VLAN-сегментацією та політиками ролей. Така модель дає змогу обмежити доступ користувача лише тими ресурсами, які необхідні для виконання його службових функцій.

Важливим обмеженням є бюджет малого офісу. На відміну від великих корпоративних структур, мале підприємство часто не має можливості впроваджувати дорогі ліцензійні рішення або утримувати окремий штат мережевих адміністраторів. Тому доцільним є використання рішень, які поєднують прийнятну вартість, достатній рівень захисту та відносну простоту адміністрування. До таких рішень належать MikroTik, pfSense та OpenVPN Access Server, які можуть виконувати функції VPN-шлюзу, firewall і засобу керування доступом у межах невеликої мережі [3, 10, 13] (див. рис.2.1).

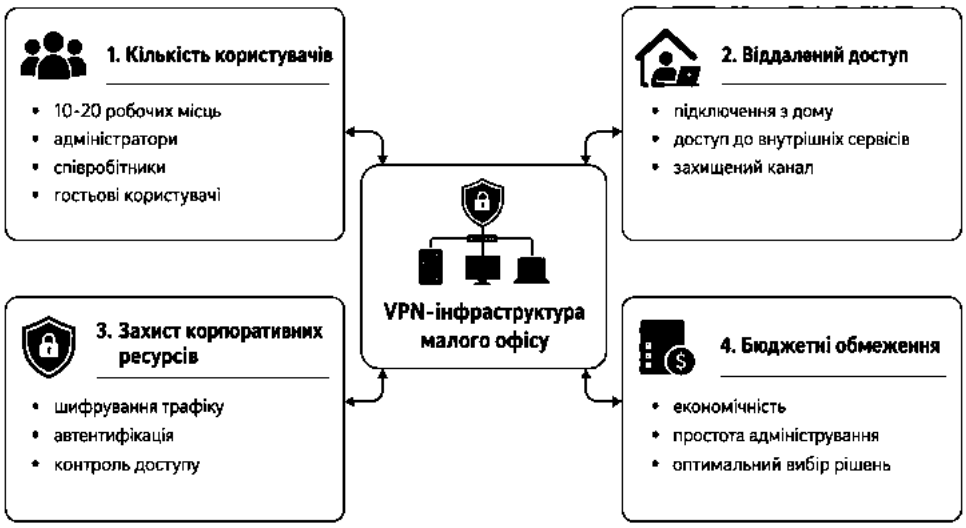

Рисунок 2.1 – Структура потреб малого офісу під час проєктування VPN-інфраструктури

Отже, аналіз потреб малого офісу свідчить, що VPN-інфраструктура має забезпечувати не лише захищене віддалене підключення, а й кероване розмежування доступу, захист внутрішніх ресурсів і відповідність фінансовим можливостям організації. Саме ці потреби формують основу для подальшого визначення вимог до системи та вибору її технічної архітектури.

2.2 Формування вимог до системи

Формування вимог до VPN-інфраструктури малого офісу є необхідним етапом проєктування мережевої системи, оскільки саме на цьому етапі визначаються функціональні характеристики, параметри безпеки, особливості мережевої взаємодії та принципи адміністрування майбутньої інфраструктури. Для малого офісу характерними є обмежена кількість мережевого обладнання, потреба у віддаленому доступі працівників до корпоративних ресурсів, відсутність складних центрів обробки даних і необхідність мінімізації витрат на підтримку мережі. У зв’язку з цим система повинна забезпечувати достатній рівень захисту інформації, підтримку стабільного VPN-з’єднання та можливість централізованого управління доступом користувачів.

Однією з ключових вимог до системи є забезпечення мережевої безпеки. Передавання корпоративного трафіку через публічні мережі створює ризики перехоплення даних, несанкціонованого доступу та компрометації службової інформації. Тому VPN-інфраструктура повинна реалізовувати механізми захищеного тунелювання трафіку між локальною мережею офісу та віддаленими користувачами. Крім захисту каналу передавання даних, система повинна підтримувати контроль доступу до внутрішніх ресурсів мережі шляхом використання ACL та розмежування ролей користувачів. Реалізація різних рівнів доступу дозволяє обмежити доступ звичайних співробітників або гостьових користувачів до критичних мережевих ресурсів і серверів адміністрування [6]. Додатково сучасні підходи до захисту VPN-інфраструктур передбачають застосування принципів Zero Trust, у межах яких

доступ користувача до мережі не повинен надаватися автоматично лише на підставі факту підключення до VPN [2].

Наступною вимогою є масштабованість системи. Навіть для малого офісу необхідно враховувати можливість подальшого розширення мережі, збільшення кількості користувачів, підключення нових сегментів або інтеграції додаткових серверів і служб. Архітектура мережі повинна дозволяти зміну структури адресації та додавання нових вузлів без необхідності повного перепроєктування інфраструктури. З цією метою доцільним є використання окремих підмереж для локального та віддаленого сегментів мережі, а також централізованої маршрутизації між ними. Такий підхід спрощує керування трафіком, дозволяє реалізовувати політики доступу між сегментами мережі та забезпечує подальший розвиток системи без значних змін базової топології [4].

Важливою вимогою до VPN-інфраструктури є відмовостійкість. Для малого офісу втрата доступу до внутрішніх ресурсів або порушення роботи VPN-з’єднання може призвести до зупинки окремих бізнес-процесів, неможливості віддаленої роботи співробітників та втрати доступу до корпоративних серверів. У зв’язку з цим система повинна підтримувати стабільну маршрутизацію трафіку, контроль стану мережевих інтерфейсів і можливість оперативного тестування доступності вузлів мережі. У процесі проєктування також необхідно враховувати резервування логічних маршрутів і можливість швидкого відновлення VPN-з’єднання після порушення мережевої взаємодії. Використання тунельних механізмів маршрутизації та контроль таблиць маршрутів дозволяє забезпечити більш стабільну роботу міжмережевого обміну даними [7].

Окрему увагу під час формування вимог було приділено простоті адміністрування системи. Для малого офісу недоцільним є впровадження надмірно складної інфраструктури, яка потребує великої кількості спеціалізованого обладнання або постійного обслуговування окремими мережевими адміністраторами. У зв’язку з цим система повинна підтримувати централізовану конфігурацію маршрутизаторів, зрозумілу структуру адресації

та прості механізми налаштування ACL і VPN-тунелів. Важливою вимогою також є можливість швидкого моніторингу стану мережі та перевірки функціонування VPN-з’єднання за допомогою стандартних засобів діагностики маршрутизаторів Cisco IOS XE [11]. Крім того, використання Cisco Packet Tracer як тестового середовища дозволяє моделювати VPN-інфраструктуру, маршрутизацію та політики доступу без використання фізичного обладнання, що є доцільним для невеликих організацій і навчальних проєктів [5].

Таким чином, сформовані вимоги до системи охоплюють забезпечення мережевої безпеки, підтримку масштабованості, відмовостійкості та простоти адміністрування. Сукупність зазначених вимог створює основу для подальшого проєктування структури VPN-інфраструктури малого офісу та реалізації системи багаторівневого доступу користувачів до корпоративних ресурсів.

2.3 Побудова структури мережі

Розробка структури мережі передбачає визначення топології, принципів логічного поділу користувачів, схеми IP-адресації та механізмів маршрутизації між локальним і віддаленим сегментами. Для малого офісу обґрунтованою є централізована модель, у якій офісна мережа з корпоративними серверами з’єднується з віддаленим сегментом через тунельне VPN-з’єднання. Така побудова дає змогу відокремити службовий трафік від звичайної міжмережевої взаємодії та забезпечити керований доступ до внутрішніх ресурсів [7].

У запропонованій структурі виокремлено три основні компоненти: офісний сегмент, віддалений сегмент і проміжний маршрутизатор провайдера. Офісний сегмент містить робочі станції користувачів, файловий сервер, адміністративний сервер, комутатор і маршрутизатор Router-Office. Віддалений сегмент представлений робочими станціями PC-Remote-Employee та PC-Remote-Admin, які взаємодіють з офісною мережею через Router-

Remote. Для перевірки працездатності цієї моделі використано Cisco Packet Tracer, що дозволяє моделювати маршрутизатори, комутатори, тунельні інтерфейси, таблиці маршрутизації та ACL без застосування фізичного обладнання [5].

Сегментація мережі здійснюється на основі функціональних ролей користувачів. У межах проєкту виділено адміністратора, співробітника, гостьового користувача та віддаленого користувача. Адміністратор отримує повний доступ до серверних ресурсів, співробітник - обмежений доступ до робочих сервісів, а гостьовий користувач не повинен мати доступу до критичних ресурсів. Технічно така модель реалізується через ACL, які фільтрують трафік за адресою джерела, адресою призначення та типом протоколу [6]. Це відповідає принципу мінімально необхідних привілеїв, за яким кожний користувач має отримувати лише той рівень доступу, який потрібний для виконання його функцій [2].

Схема адресації побудована з використанням окремих приватних підмереж. Для офісного сегмента застосовано мережу 192.168.10.0/24, для віддаленого сегмента - 192.168.20.0/24, а для тунельного з’єднання - 10.10.10.0/30. Такий поділ спрощує ідентифікацію джерел трафіку, налаштування правил доступу та діагностику помилок. Маршрутизацію між сегментами реалізовано через статичні маршрути, що є доцільним для малої мережі зі сталою кількістю вузлів і передбачуваною структурою трафіку [4]. Отже, запропонована структура мережі забезпечує логічне розмежування користувачів, контрольований доступ до серверів і технічну можливість перевірки роботи VPN-з’єднання засобами мережевої діагностики.

2.4 Розробка моделі рівнів доступу

Розробка моделі рівнів доступу є необхідною складовою проєктування VPN-інфраструктури малого офісу, оскільки саме механізми розмежування привілеїв визначають рівень захисту корпоративних ресурсів та контроль

мережевої взаємодії між користувачами. У межах досліджуваної мережевої моделі було реалізовано рольовий підхід до організації доступу, відповідно до якого права користувачів визначаються їхньою функціональною роллю в системі [2].

У структурі мережі виділено чотири основні категорії користувачів: адміністратори, співробітники, гостьові користувачі та віддалені користувачі. Адміністратори мають повний доступ до серверних ресурсів, таблиць маршрутизації, VPN-з’єднань та механізмів конфігурації мережевого обладнання. Саме ця категорія користувачів виконує функції управління інфраструктурою та контролю мережевої безпеки.

Співробітники офісу отримують доступ лише до корпоративних сервісів, необхідних для виконання службових функцій. Для цієї категорії користувачів передбачено обмеження доступу до адміністративних ресурсів і мережевих параметрів системи. Гостьові користувачі мають мінімальний рівень привілеїв та не повинні взаємодіяти із внутрішніми серверами або службовими сегментами мережі. Віддалені користувачі підключаються до локальної інфраструктури через VPN-тунель і отримують доступ відповідно до визначеної ролі користувача.

Для реалізації моделі доступу використовувалися ACL, які дозволяють фільтрувати трафік за IP-адресами джерела та призначення, а також контролювати доступ до окремих серверних вузлів [6] (див. рис.2.2). Такий підхід забезпечує сегментацію мережевого трафіку та дозволяє обмежити несанкціоновану взаємодію між користувачами різних категорій.

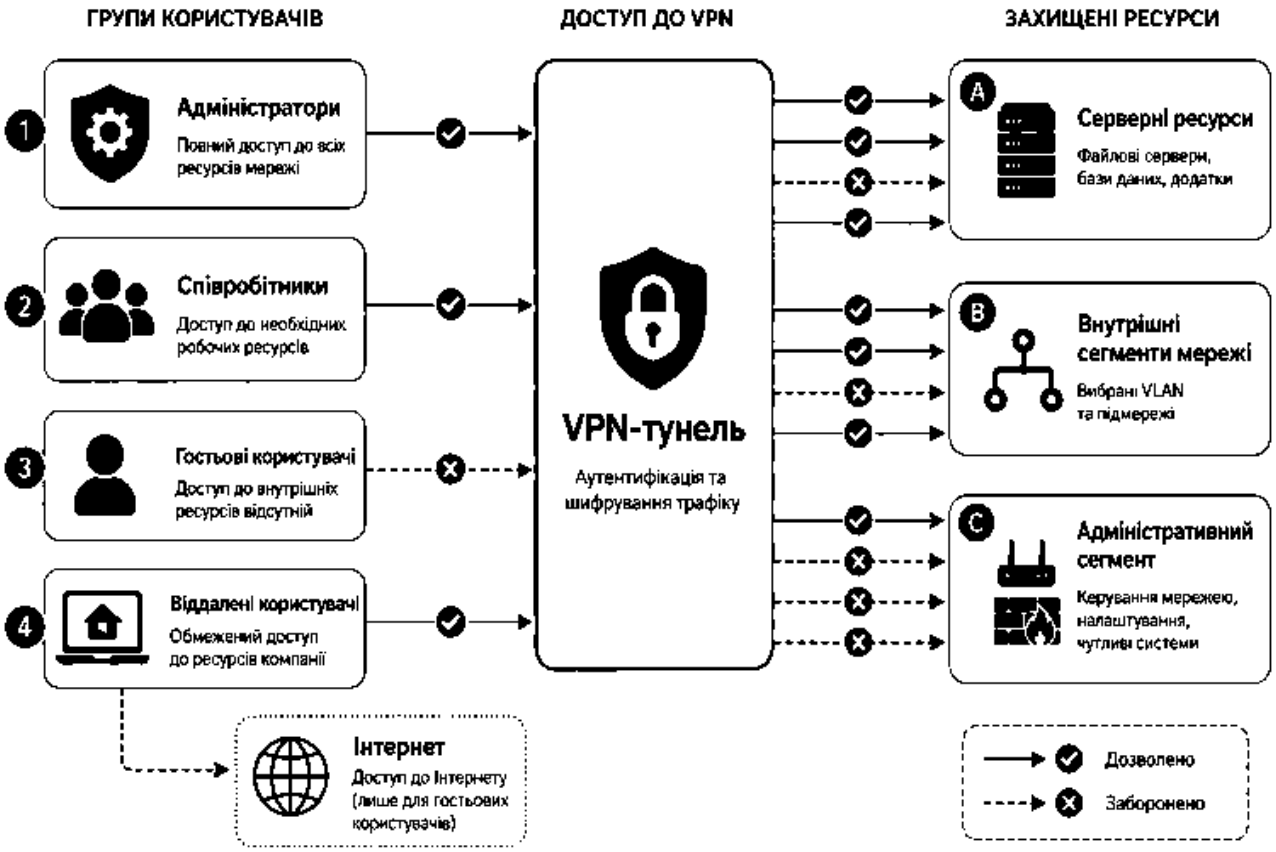

Рисунок 2.2. – Модель рівнів доступу користувачів у VPN-інфраструктурі малого офісу

Отже, розроблена модель рівнів доступу забезпечує контрольовану взаємодію між користувачами та корпоративними ресурсами, зменшує ризик несанкціонованого доступу й створює основу для реалізації політик мережевої безпеки в межах VPN-інфраструктури малого офісу.

2.5 Вибір програмного та апаратного забезпечення

Вибір програмного та апаратного забезпечення для VPN-інфраструктури малого офісу здійснювався з урахуванням вимог мережевої безпеки, підтримки віддаленого доступу, можливостей сегментації користувачів та обмежень бюджету. Для побудови тестового середовища було використано Cisco Packet Tracer, оскільки це програмне середовище дозволяє моделювати маршрутизатори, комутатори, таблиці маршрутизації, ACL та VPN-тунелі без застосування фізичного обладнання [5].

Як основний мережевий вузол використовувалися маршрутизатори Cisco, які забезпечують підтримку статичної маршрутизації, тунельних інтерфейсів та механізмів контролю доступу. Використання обладнання Cisco є доцільним для навчального та тестового моделювання VPN-інфраструктури, оскільки Cisco IOS XE підтримує реалізацію ACL, сегментацію мережевого трафіку та конфігурацію захищених VPN-з’єднань [4].

Для реалізації контролю доступу використовувалися ACL, що виконують функції базового мережевого firewall і дозволяють обмежувати доступ користувачів до окремих серверів або сегментів мережі [6]. Такий підхід забезпечує розмежування привілеїв між адміністраторами, співробітниками та віддаленими користувачами без необхідності використання окремого апаратного міжмережевого екрана.

У межах теоретичного аналізу також було розглянуто сучасні VPN-рішення MikroTik, pfSense, OpenVPN та WireGuard як альтернативні платформи для практичного впровадження VPN-інфраструктури малого офісу [3]. Зокрема, WireGuard характеризується спрощеною конфігурацією та високою продуктивністю VPN-з’єднання [14], тоді як OpenVPN забезпечує підтримку різних механізмів автентифікації та клієнтських підключень [9]. Обране програмне та апаратне забезпечення забезпечує можливість моделювання VPN-інфраструктури, реалізації багаторівневого доступу та перевірки політик мережевої безпеки в умовах малого офісу.

2.6 Схема взаємодії компонентів системи

Схема взаємодії компонентів системи визначає логіку обміну даними між мережевими вузлами VPN-інфраструктури малого офісу та відображає механізми взаємодії між локальним сегментом, віддаленими користувачами, маршрутизаторами, серверними ресурсами та засобами контролю доступу. Формування такої схеми є необхідним етапом проєктування, оскільки вона дозволяє встановити порядок передавання мережевого трафіку, визначити

точки застосування політик безпеки та забезпечити контроль доступу до корпоративних ресурсів.

У структурі системи центральним елементом виступає офісний маршрутизатор Router-Office, який забезпечує маршрутизацію трафіку між локальною мережею, VPN-тунелем і проміжним сегментом провайдера. До локального сегмента підключаються робочі станції користувачів, файловий сервер і адміністративний сервер. Віддалений сегмент мережі взаємодіє з локальною інфраструктурою через Router-Remote, між яким і Router-Office формується тунельне VPN-з'єднання. Передавання трафіку між сегментами здійснюється через проміжний маршрутизатор Router-ISP, який виконує функцію моделювання публічної мережі.

Контроль доступу до ресурсів реалізується через ACL, які застосовуються до мережевого трафіку на маршрутизаторах і дозволяють фільтрувати доступ користувачів відповідно до їхньої ролі [6]. У межах системи адміністративні користувачі мають доступ до критичних серверних ресурсів, тоді як для співробітників і віддалених користувачів передбачено обмеження доступу до окремих сегментів мережі. Такий підхід забезпечує логічне розмежування трафіку та зменшує ризик несанкціонованої взаємодії між компонентами інфраструктури [2, с. 17].

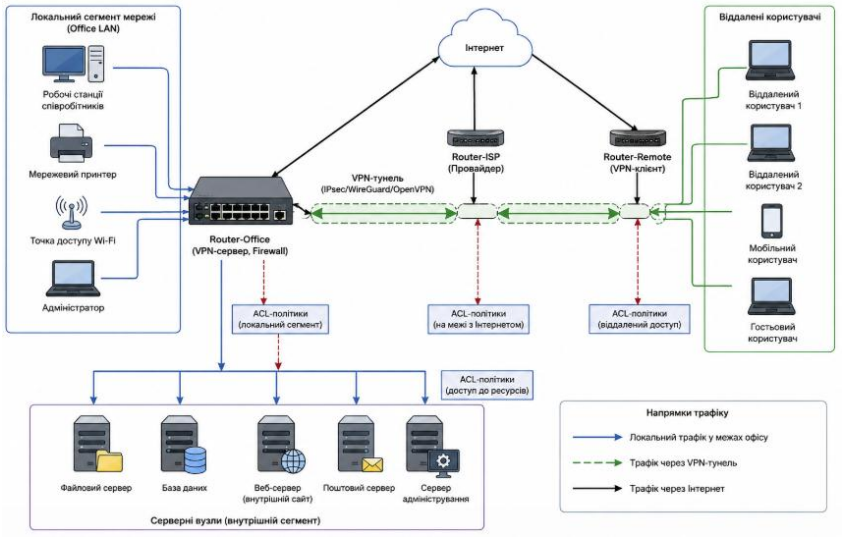

Рисунок 2.3 – Схема взаємодії компонентів VPN-інфраструктури малого офісу

Отже, схема взаємодії компонентів системи формує логічну основу функціонування VPN-інфраструктури та забезпечує централізований контроль мережевої взаємодії між користувачами, серверами та мережевими сегментами малого офісу.

У другому розділі обґрунтовано проєктні засади побудови VPN-інфраструктури для малого офісу. Визначено, що ключовими потребами такого середовища є захищений віддалений доступ, розмежування прав користувачів, захист внутрішніх ресурсів і врахування бюджетних обмежень.

Сформовано основні вимоги до системи, серед яких пріоритетними є безпека, масштабованість, відмовостійкість і простота адміністрування. Розроблена структура мережі передбачає поділ користувачів за ролями, застосування VPN-тунелю, використання firewall, ACL-політик і логічної сегментації мережі.

Запропонована модель рівнів доступу дає змогу обмежити взаємодію користувачів із ресурсами відповідно до їхніх функціональних повноважень. Отже, спроєктована VPN-інфраструктура створює технічну основу для безпечного, керованого й економічно доцільного функціонування мережі малого офісу.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ VPN-ІНФРАСТРУКТУРИ

3.1 Розгортання тестового середовища

Розгортання тестового середовища виконано в Cisco Packet Tracer, що дозволило сформувати емуляційну модель VPN-інфраструктури малого офісу та перевірити її функціонування без використання фізичного мережевого обладнання. Вибір цього середовища є методично обґрунтованим, оскільки Cisco Packet Tracer підтримує моделювання маршрутизаторів, комутаторів, клієнтських вузлів, серверів, IP-адресації, статичної маршрутизації та базових механізмів перевірки мережевої доступності [5].

На рисунку 3.1 представлено логічну топологію тестового середовища.

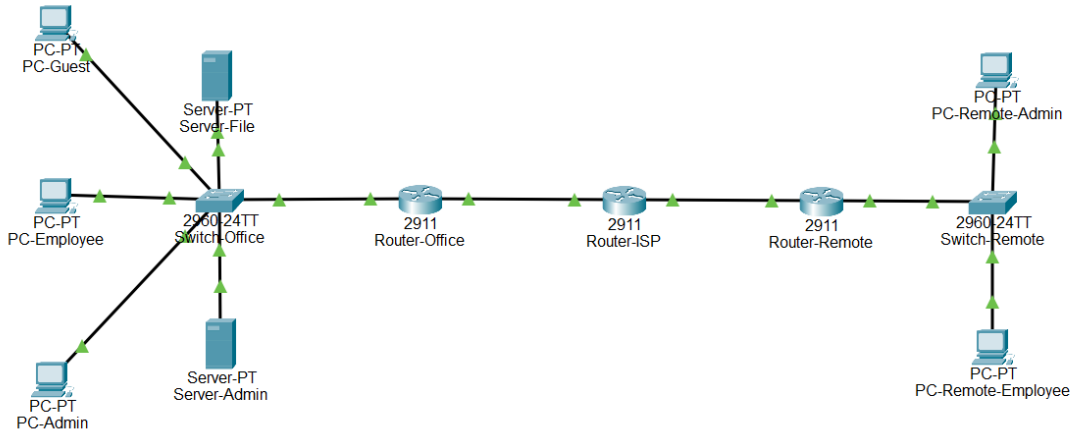

Рисунок 3.1 – Топологія тестового середовища VPN-інфраструктури малого офісу

Модель складається з двох функціональних сегментів: локальної офісної мережі та віддаленої мережі користувачів. Локальний сегмент містить робочі станції PC-Guest, PC-Employee і PC-Admin, файловий сервер Server-File, адміністративний сервер Server-Admin, комутатор Switch-Office та маршрутизатор Router-Office. Віддалений сегмент охоплює робочі станції PC-Remote-Admin і PC-Remote-Employee, комутатор Switch-Remote та

маршрутизатор Router-Remote. Між Router-Office і Router-Remote розміщено Router-ISP, який виконує роль транзитного вузла та імітує зовнішню мережу провайдера.

Запропонована топологія є доцільною для дослідження VPN-доступу, оскільки вона відтворює типову ситуацію малого офісу: внутрішні серверні ресурси розташовані в локальній мережі, а віддалені користувачі повинні отримувати до них доступ через контрольований міжмережевий канал. Наявність окремого транзитного маршрутизатора унеможливлює трактування моделі як простої локальної мережі та дозволяє показати зміну роботи системи після налаштування тунельного з'єднання.

На рисунку 3.2 наведено конфігурацію Router-ISP, який забезпечує міжмережеву взаємодію між офісним і віддаленим сегментами.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 100.0.0.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)#
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 200.0.0.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.10.0 255.255.255.0 100.0.0.2
Router(config)#ip route 192.168.20.0 255.255.255.0 200.0.0.2
Router(config)#
Router(config)#end
Router#write
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
```

Рисунок 3.2 – Налаштування транзитного маршрутизатора Router-ISP

На інтерфейсі GigabitEthernet0/0 встановлено адресу 100.0.0.1 255.255.255.252, що відповідає каналу зв'язку з Router-Office. На інтерфейсі

GigabitEthernet0/1 встановлено адресу 200.0.0.1 255.255.255.252, що забезпечує з’єднання з Router-Remote. Для забезпечення маршрутизації задано два статичні маршрути: до мережі 192.168.10.0/24 через 100.0.0.2 та до мережі 192.168.20.0/24 через 200.0.0.2.

З технічної точки зору така конфігурація забезпечує базову IP-зв’язність між крайовими маршрутизаторами та створює умови для подальшого налаштування VPN-тунелю. Водночас Router-ISP не виконує функції захисту доступу до корпоративних ресурсів, а лише передає трафік між мережевими сегментами. Це важливо для логіки дослідження: захищений доступ і розмежування прав користувачів реалізуються не на транзитному вузлі, а на рівні крайових маршрутизаторів, тунельної маршрутизації та ACL-політик [6].

Отже, розгорнуте тестове середовище забезпечує необхідну основу для подальшої реалізації VPN-інфраструктури. Воно дозволяє окремо перевірити базову маршрутизацію, працездатність тунельного з’єднання, доступність серверних ресурсів та ефективність політик обмеження доступу для різних категорій користувачів.

3.2 Налаштування VPN-сервера

Налаштування VPN-сервера у змодельованій інфраструктурі виконано на базі крайових маршрутизаторів Router-Office та Router-Remote, між якими сформовано тунельний канал передавання трафіку. У межах Cisco Packet Tracer реалізація виконувалася через інтерфейс Tunnel0, що дозволило логічно поєднати офісну мережу 192.168.10.0/24 із віддаленою мережею 192.168.20.0/24. Такий підхід є доцільним для демонстраційної моделі, оскільки дає змогу перевірити принцип роботи VPN-доступу, маршрутизацію між сегментами та доступність ресурсів без застосування фізичного обладнання [5].

На рисунку 3.3 показано результат команди show ip interface brief. Із наведених даних видно, що інтерфейси GigabitEthernet0/0, GigabitEthernet0/1 та Tunnel0 перебувають у стані up/up. Це підтверджує фізичну й логічну

працездатність мережевих інтерфейсів, а також активний стан тунельного інтерфейсу.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.20.1    YES manual up                    up
GigabitEthernet0/1     200.0.0.2       YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Tunnel0                10.10.10.2      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Рисунок 3.3 – Перевірка стану інтерфейсів віддаленого маршрутизатора

Адреса 10.10.10.2, призначена інтерфейсу Tunnel0, використовується як тунельна адреса віддаленої сторони VPN-з’єднання. Отже, цей скрін підтверджує, що тунель не лише налаштований, а й перебуває в робочому стані.

На рисунку 3.4 наведено конфігурацію Router-Office. Спочатку налаштовано локальний інтерфейс GigabitEthernet0/0 з адресою 192.168.10.1/24, який виконує функцію шлюзу для офісного сегмента.

Далі інтерфейсу GigabitEthernet0/1 призначено адресу 100.0.0.2/30, що забезпечує зв’язок із транзитним маршрутизатором Router-ISP. Основним елементом VPN-конфігурації є створення interface tunnel 0 з адресою 10.10.10.1/30, джерелом тунелю GigabitEthernet0/1 та призначенням 200.0.0.2. Також додано маршрут до віддаленої мережі 192.168.20.0/24 через тунельну адресу 10.10.10.2.

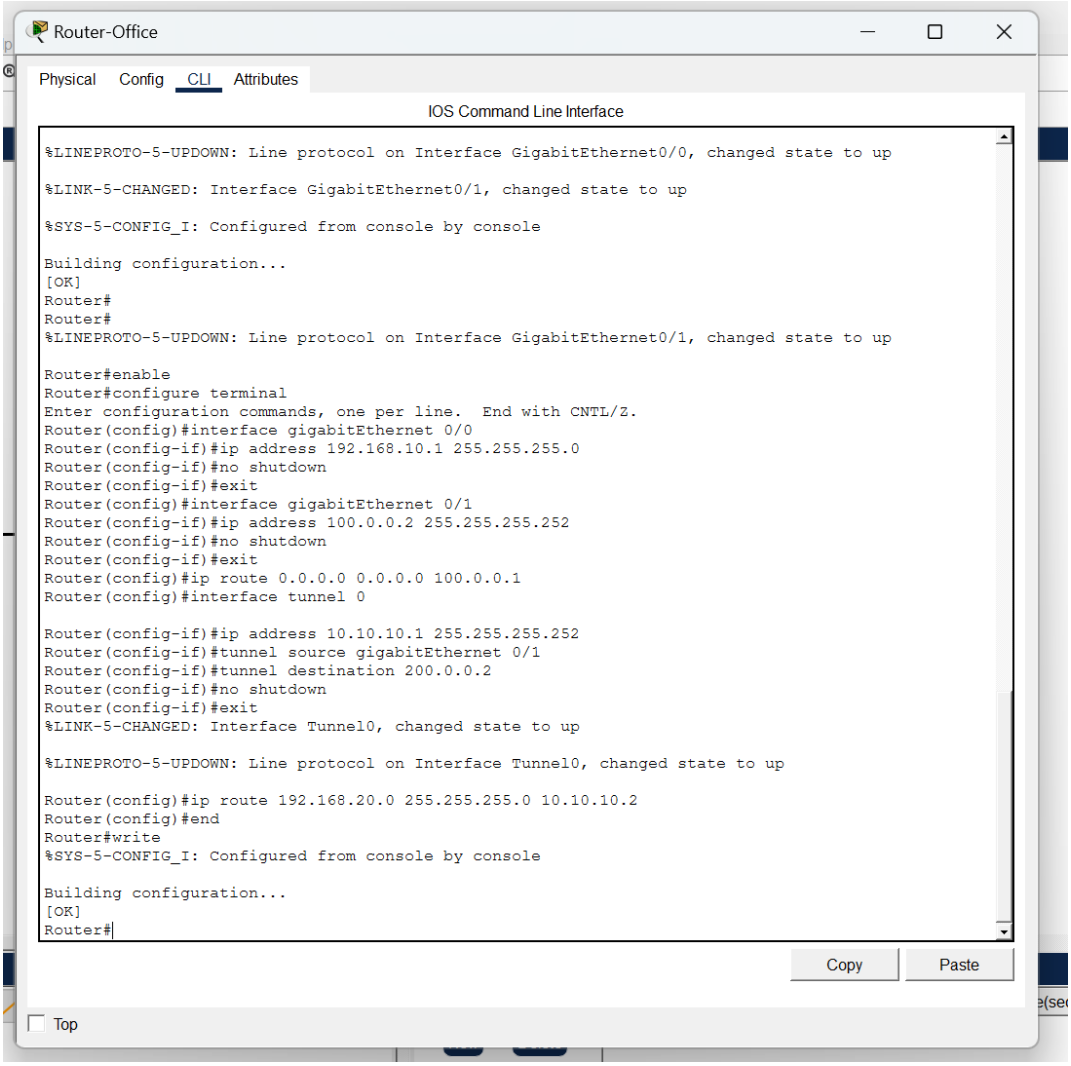

Рисунок 3.4 – Налаштування тунельного інтерфейсу на Router-Office

На рисунку 3.5 показано конфігурацію Router-Remote. Локальний інтерфейс маршрутизатора має адресу 192.168.20.1/24 і виконує роль шлюзу для віддаленого сегмента. Зовнішній інтерфейс GigabitEthernet0/1 отримав адресу 200.0.0.2/30, що забезпечує підключення до Router-ISP. Для формування зворотної сторони VPN-тунелю створено Tunnel0 з адресою 10.10.10.2/30, джерелом GigabitEthernet0/1 та призначенням 100.0.0.2. Статичний маршрут 192.168.10.0/24 via 10.10.10.1 спрямовує трафік до офісної мережі через VPN-тунель.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 200.0.0.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1
Router(config)#interface tunnel 0

Router(config-if)#ip address 10.10.10.2 255.255.255.252
Router(config-if)#tunnel source gigabitEthernet 0/1
Router(config-if)#tunnel destination 100.0.0.2
Router(config-if)#no shutdown
Router(config-if)#exit
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Router(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.1
Router(config)#end
Router#write
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Рисунок 3.5 – Налаштування тунельного інтерфейсу на Router-Remote

Отже, налаштування VPN-сервера в межах тестової моделі реалізовано як двостороннє тунельне з’єднання між Router-Office і Router-Remote. Конфігурація підтверджує наявність логічного каналу між двома приватними мережами, а стан Tunnel0 up/up засвідчує його працездатність.

3.3 Реалізація системи рівнів доступу

Реалізація системи рівнів доступу в межах змодельованої VPN-інфраструктури здійснювалася через застосування списків контролю доступу ACL на маршрутизаторі офісного сегмента. Такий підхід дозволяє формалізувати політики доступу не лише на рівні загальної мережевої зв’язності, а й на рівні конкретних взаємодій між вузлами. У проєкті адміністративний сервер 192.168.10.200 розглядається як критичний ресурс, доступ до якого має бути обмежений для користувачів із нижчим рівнем привілеїв. Застосування ACL у Cisco IOS є базовим механізмом фільтрації

трафіку за IP-адресами джерела, адресами призначення та типами протоколів [6].

```
Router#
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 deny ip host 192.168.10.10 host 192.168.10.200
Router(config)#access-list 110 permit ip any any
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
Router(config)#end
Router#write
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Рисунок 3.6 – Первинне налаштування ACL для обмеження доступу до адміністративного сервера

На рисунку 3.6 показано створення списку доступу 110, у якому задано правило deny ip host 192.168.10.10 host 192.168.10.200. Це означає, що вузлу з IP-адресою 192.168.10.10 забороняється IP-взаємодія з адміністративним сервером 192.168.10.200. Наступне правило permit ip any any виконує функцію дозволу всього іншого трафіку, який не підпадає під попередню заборону. Така логіка є принципово важливою, оскільки ACL обробляє правила послідовно: спочатку перевіряється заборона для конкретної пари вузлів, а після цього дозволяється інший трафік. Команда ip access-group 110 in, застосована на інтерфейсі GigabitEthernet0/0, вказує, що фільтрація виконується для вхідного трафіку з боку локального офісного сегмента.

```
Router#
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no ip access-group 110 in
Router(config-if)#exit
Router(config)#no access-list 110
Router(config)#access-list 110 deny icmp host 192.168.10.10 host 192.168.10.200
Router(config)#access-list 110 permit ip any any
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
Router(config)#end
Router#write
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Рисунок 3.7 – Уточнення ACL-політики для контролю ICMP-трафіку

На рисунку 3.7 подано уточнену конфігурацію ACL, у якій попередній список доступу було вилучено командою no access-list 110, після чого створено нове правило deny icmp host 192.168.10.10 host 192.168.10.200. На відміну від первинного варіанта, це правило блокує не весь IP-трафік, а лише ICMP-запити між користувацьким вузлом і адміністративним сервером. Такий варіант є методично коректним для експериментальної перевірки політики доступу, оскільки команда ping використовує ICMP і дозволяє наочно підтвердити факт блокування доступу.

З позиції мережевої безпеки реалізована ACL-політика відображає принцип мінімально необхідних привілеїв: користувач не отримує доступу до адміністративного ресурсу, якщо такий доступ не відповідає його ролі в системі [2]. У межах цієї моделі адміністратор має розширений доступ до серверної інфраструктури, тоді як звичайний або гостьовий користувач обмежується у взаємодії з критичними вузлами.

3.4 Налаштування клієнтських підключень

Налаштування клієнтських підключень у змодельованій VPN-інфраструктурі виконувалося шляхом статичного призначення IP-параметрів

робочим станціям локального офісного сегмента. Такий підхід є доцільним для тестового середовища, оскільки він забезпечує передбачувану адресацію вузлів, спрощує перевірку маршрутизації та дозволяє коректно застосовувати ACL-політики до конкретних IP-адрес. У межах моделі клієнтські пристрої не отримують адреси автоматично через DHCP, а налаштовуються вручну, що підвищує контрольованість експериментальної конфігурації в Cisco Packet Tracer [5].

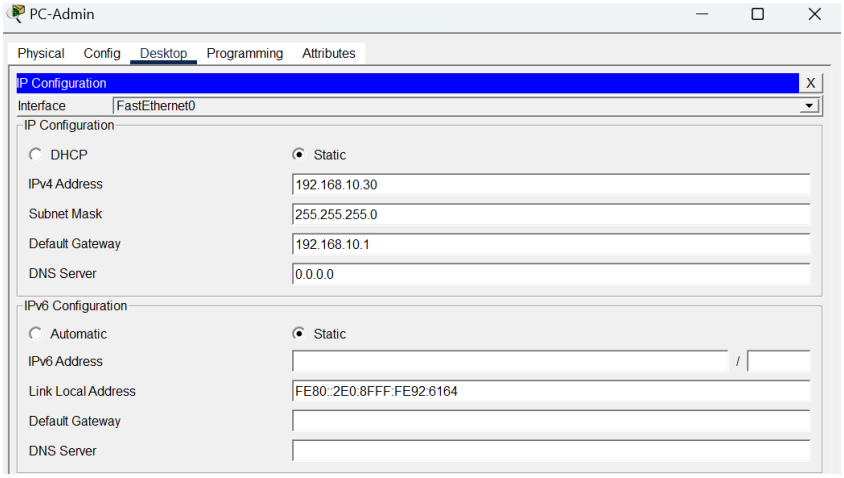

Рисунок 3.8 – Налаштування IP-параметрів робочої станції PC-Admin

На рисунку 3.8 показано налаштування клієнтського вузла PC-Admin. Робочій станції призначено IP-адресу 192.168.10.30, маску підмережі 255.255.255.0 та шлюз за замовчуванням 192.168.10.1. Така конфігурація вказує, що PC-Admin належить до офісної підмережі 192.168.10.0/24, а передавання трафіку до інших сегментів мережі здійснюється через Router-Office. З технічної позиції PC-Admin є вузлом із підвищеним рівнем доступу, тому його адресація повинна бути сталою для коректного застосування політик маршрутизації та контролю доступу.

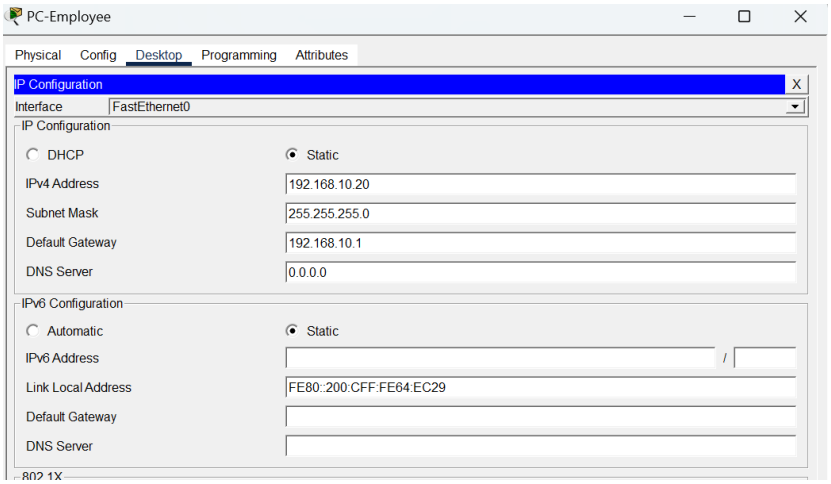

Рисунок 3.9 – Налаштування IP-параметрів робочої станції PC-Employee

На рисунку 3.9 наведено конфігурацію робочої станції PC-Employee. Для цього клієнта встановлено IP-адресу 192.168.10.20, маску 255.255.255.0 та основний шлюз 192.168.10.1. Це означає, що PC-Employee також розміщується в офісному сегменті, однак його функціональна роль відрізняється від адміністративного вузла. У подальшому така фіксована адресація дозволяє відокремлювати звичайних співробітників від адміністраторів і застосовувати до них різні правила доступу.

Отже, на цьому етапі було забезпечено базову клієнтську конфігурацію для роботи в офісній мережі, перевірки доступності віддаленого сегмента через VPN-тунель і подальшого тестування політик розмежування доступу. Статичне налаштування клієнтів у цьому випадку є методично виправданим, оскільки дозволяє однозначно пов’язати кожний вузол із відповідною роллю користувача та перевірити коректність реалізованої моделі доступу.

3.6 Тестування системи

Тестування розробленої VPN-інфраструктури було спрямоване на перевірку трьох взаємопов’язаних параметрів: доступності мережевих ресурсів, працездатності тунельного з’єднання та коректності політик розмежування доступу. У межах емуляційної моделі Cisco Packet Tracer основним діагностичним інструментом використано ICMP-запити, оскільки

вони дають змогу зафіксувати факт проходження пакетів між вузлами, рівень втрат і орієнтовний час відповіді мережевого сегмента [5].

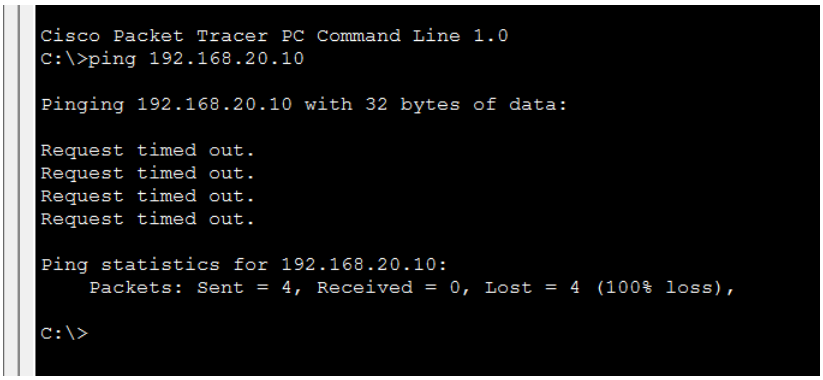

Рисунок 3.11 – Перевірка недоступності віддаленого сегмента до встановлення VPN-з’єднання

На рисунку 3.11 наведено результат первинної перевірки доступу до вузла 192.168.20.10, який належить до віддаленої мережі. Усі чотири ICMP-запити завершилися повідомленням Request timed out, а показник втрат становив 100%. Такий результат свідчить про відсутність сталої міжмережевої взаємодії між офісним сегментом 192.168.10.0/24 і віддаленим сегментом 192.168.20.0/24 до налаштування тунельного маршруту. Отже, вихідний стан мережі підтверджує, що віддалений ресурс не був доступний без спеціально організованого VPN-каналу.

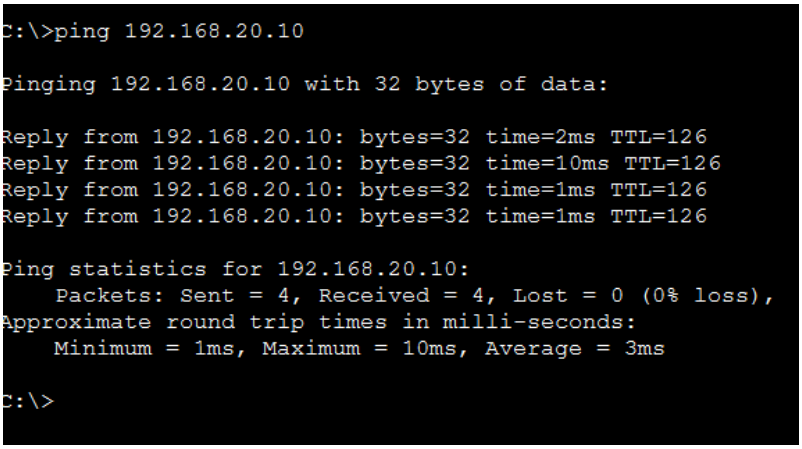

Рисунок 3.12 – Перевірка доступності віддаленого сегмента після налаштування VPN

На рисунку 3.12 показано повторну перевірку доступу до того самого вузла 192.168.20.10 після налаштування тунельного інтерфейсу та статичної маршрутизації. Усі чотири пакети отримали відповідь, втрати становили 0%, а середній час відповіді дорівнював 3 ms. Це підтверджує, що після активації VPN-тунелю трафік між локальною та віддаленою мережами почав проходити коректно. Відсутність втрат пакетів у цьому тесті засвідчує працездатність логічного тунельного каналу та коректність маршрутів між сегментами.

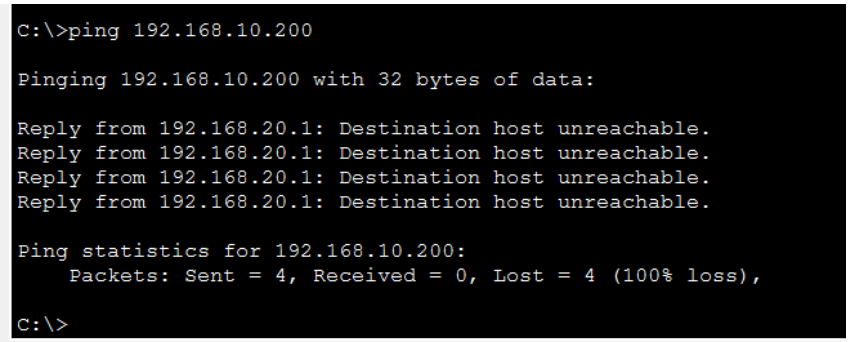

Рисунок 3.13 – Перевірка блокування доступу до адміністративного сервера

На рисунку 3.13 зафіксовано спробу доступу до адміністративного сервера 192.168.10.200. Відповідь Destination host unreachable від шлюзу 192.168.20.1 і втрата 100% пакетів показують, що трафік до захищеного ресурсу був заблокований. Цей результат підтверджує практичну дію ACL-політики, яка обмежує доступ окремого користувача або групи користувачів до адміністративного сегмента. Тобто система не лише забезпечує з’єднання між мережами, а й виконує вибіркову фільтрацію трафіку відповідно до заданих правил доступу [6].

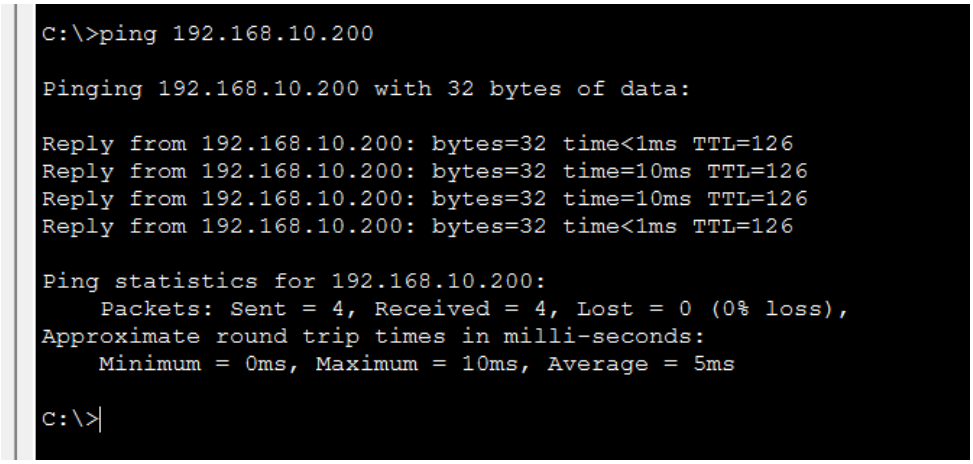

Рисунок 3.14 – Перевірка дозволеного доступу до адміністративного сервера

На рисунку 3.14 наведено результат перевірки доступу до адміністративного сервера з авторизованого вузла. У цьому випадку всі чотири ICMP-пакети були доставлені успішно, втрати становили 0%, а середній час відповіді дорівнював 5 ms. Отриманий результат має принципове значення, оскільки демонструє не загальне блокування адміністративного сервера, а саме рольове розмежування доступу. Неавторизований запит блокується, тоді як дозволений трафік проходить без порушення мережевої зв’язності.

Таким чином, результати тестування підтвердили функціональну завершеність змодельованої VPN-інфраструктури. Порівняння стану до та після налаштування тунелю показало зміну доступності віддаленого сегмента з 100% втрат до повністю успішної передачі пакетів. Додаткова перевірка ACL засвідчила, що система підтримує не лише міжмережеву взаємодію, а й контрольований доступ до критичних ресурсів. Отже, реалізована модель відповідає завданню побудови VPN-інфраструктури малого офісу з різними рівнями доступу користувачів.

У третьому розділі було реалізовано тестову модель VPN-інфраструктури малого офісу в Cisco Packet Tracer. Створена топологія охоплює офісний сегмент, віддалений сегмент, серверні ресурси, клієнтські вузли та транзитний маршрутизатор. У процесі налаштування сформовано

тунельне з’єднання між Router-Office і Router-Remote, що забезпечило передавання трафіку між мережами 192.168.10.0/24 та 192.168.20.0/24. Працездатність тунелю підтверджено успішним проходженням ICMP-пакетів після його активації.

Також реалізовано базову систему розмежування доступу за допомогою ACL. Тестування показало, що неавторизований доступ до адміністративного сервера блокується, тоді як дозволений користувач зберігає доступ до ресурсу.

Отже, практична реалізація підтвердила працездатність запропонованої VPN-моделі та її придатність для малого офісу з різними рівнями доступу користувачів.

РОЗДІЛ 4 ОЦІНКА ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ СИСТЕМИ

4.1 Аналіз продуктивності VPN

Оцінювання продуктивності VPN-інфраструктури здійснювалося шляхом аналізу швидкості передавання пакетів, мережевих затримок та навантаження на маршрутизатори під час функціонування тунельного з'єднання. Результати тестування засвідчили стабільну передачу даних між локальним і віддаленим сегментами мережі без критичних втрат пакетів після встановлення VPN-тунелю. Передавання ICMP-пакетів відбувалося коректно, що підтверджує працездатність маршрутизації та належний рівень пропускної здатності в межах змодельованої мережевої інфраструктури.

Аналіз затримок показав, що середній час відгуку перебував у межах 1-10 мс, що є прийнятним показником для малого офісного середовища. Незначні короткочасні затримки спостерігалися лише під час ініціалізації тунельних інтерфейсів та оновлення маршрутів, після чого VPN-з'єднання функціонувало стабільно. Відсутність повторних розривів каналу свідчить про коректне налаштування тунелю та міжмережевої взаємодії.

Навантаження на мережеве обладнання залишалося помірним навіть після застосування ACL-політик і фільтрації трафіку. Використання статичної маршрутизації та GRE-тунелю не спричинило суттєвого зростання затримок або деградації доступності ресурсів. Це дозволяє зробити висновок про достатню ефективність реалізованої VPN-інфраструктури для забезпечення захищеного обміну даними в умовах малого офісу.

4.2 Аналіз рівня захищеності

Проведений аналіз функціонування VPN-інфраструктури показав, що реалізована система забезпечує базовий рівень захисту мережевих ресурсів від несанкціонованого доступу. Основним механізмом обмеження доступу виступають ACL-політики, які дозволяють фільтрувати мережевий трафік відповідно до встановлених правил безпеки. У процесі тестування було

підтверджено коректне блокування ICMP-запитів до окремих вузлів мережі, що свідчить про ефективність реалізованої системи контролю доступу та сегментації мережевого середовища.

Аналіз потенційних загроз показав, що найбільшу небезпеку для VPN-інфраструктури становлять спроби несанкціонованого підключення, перехоплення трафіку, сканування внутрішніх ресурсів і порушення цілісності маршрутизації. У разі відсутності належної фільтрації трафіку можливе отримання доступу до внутрішніх сегментів мережі або серверних ресурсів сторонніми користувачами. Крім того, використання відкритих міжмережевих сервісів без додаткових механізмів автентифікації може створювати ризики компрометації мережевої інфраструктури.

Для підвищення рівня безпеки доцільним є впровадження багаторівневої системи захисту, що включає застосування ACL-політик, сегментацію мережі, використання захищених VPN-тунелів та постійний моніторинг мережевої активності. Додатково ефективність захисту може бути підвищена шляхом використання сучасних криптографічних алгоритмів, механізмів автентифікації користувачів і регулярного аналізу журналів мережевих подій. Отримані результати підтверджують, що реалізована VPN-інфраструктура забезпечує достатній рівень захищеності для використання в умовах малого офісу.

4.3 Економічна доцільність впровадження

Для оцінювання економічної ефективності впровадження VPN-інфраструктури було використано співвідношення між потенційними витратами на організацію окремого фізичного каналу зв’язку та витратами на реалізацію VPN-рішення на базі наявної мережевої інфраструктури.

Економічний ефект визначався за формулою 4.1.

$$E = \frac{S-C}{C} \times 100\% \quad (4.1)$$

де: E- економічна ефективність впровадження VPN; S- потенційно зекономлені витрати; C- витрати на реалізацію VPN-інфраструктури.

У межах дослідження було прийнято, що середні витрати на організацію окремого виділеного каналу зв'язку для малого офісу становлять близько 18000 грн на рік, тоді як використання VPN-інфраструктури на базі існуючого інтернет-з'єднання та маршрутизаторів потребує приблизно 6000 грн витрат на налаштування, адміністрування та підтримку системи.

Після підстановки значень отримано значення з формули 4.2

$$E = \frac{18000-6000}{6000} \times 100\% = 200\% \qquad (4.2)$$

Отриманий результат свідчить про те, що використання VPN-інфраструктури дозволяє суттєво зменшити витрати на організацію корпоративної мережевої взаємодії порівняно з використанням окремих фізичних каналів зв'язку.

Для оцінювання рівня використання мережевого каналу застосовувався коефіцієнт завантаження 4.3:

$$K_u = \frac{T_f}{T_c} \qquad (4.3)$$

де: K_u- коефіцієнт використання каналу; T_f- фактичний обсяг переданого трафіку; T_c- максимальна пропускна здатність каналу.

За умови передавання 45 Мбіт/с трафіку через канал із пропускною здатністю 100 Мбіт/с отримуємо 4.5

$$K_u = \frac{45}{100} = 0.45 \qquad (4.5)$$

Отримане значення свідчить про помірне навантаження на мережеву інфраструктуру та наявність резерву пропускної здатності для подальшого масштабування системи.

4.4 Рекомендації щодо модернізації системи

Проведений аналіз функціонування VPN-інфраструктури малого офісу дозволяє визначити низку напрямів подальшої модернізації системи з метою

підвищення рівня мережевої безпеки, продуктивності та відмовостійкості. У процесі дослідження було встановлено, що використання тунельного VPN-з’єднання та ACL забезпечує базовий рівень захисту мережевої взаємодії, однак подальший розвиток інфраструктури потребує впровадження більш сучасних механізмів автентифікації, шифрування та моніторингу мережевої активності.

Одним із пріоритетних напрямів модернізації є перехід від базової тунельної моделі до використання сучасних VPN-протоколів із підтримкою криптографічного захисту трафіку. Для малого офісу доцільним є впровадження OpenVPN або WireGuard, які забезпечують вищий рівень захисту даних, підтримку сучасних алгоритмів шифрування та більш гнучкі механізми конфігурації віддалених підключень [9]. Особливо перспективним є використання WireGuard, який характеризується спрощеною архітектурою, меншою кількістю програмного коду та нижчим рівнем мережевих затримок [14].

Важливим напрямом модернізації є вдосконалення системи контролю доступу. Реалізовані ACL забезпечують базову фільтрацію трафіку, однак для підвищення рівня безпеки доцільним є впровадження централізованої рольової моделі доступу та багатофакторної автентифікації користувачів. Використання принципів Zero Trust дозволяє мінімізувати ризики несанкціонованого доступу до корпоративних ресурсів навіть у випадку компрометації окремих облікових записів [2].

Окрему увагу доцільно приділити розвитку систем моніторингу та журналювання мережевої активності. У межах подальшої модернізації рекомендується впровадження засобів централізованого збору логів, автоматизованого аналізу подій безпеки та контролю мережевого навантаження. Це дозволить оперативно виявляти спроби несанкціонованого доступу, аналізувати стан VPN-з’єднань і забезпечувати контроль стабільності мережевої взаємодії.

Додатковим напрямом модернізації є впровадження VLAN-сегментації та резервування критичних мережевих вузлів. Використання окремих VLAN для адміністративного, серверного та гостьового сегментів дозволить підвищити рівень ізоляції мережевого трафіку та зменшити ризик поширення загроз між сегментами інфраструктури [1]. У свою чергу резервування маршрутизаторів або каналів зв’язку дозволить забезпечити безперервність функціонування мережі у випадку відмови окремих компонентів системи.

Отже, подальша модернізація VPN-інфраструктури повинна бути спрямована на впровадження сучасних VPN-протоколів, посилення механізмів автентифікації, розвиток систем моніторингу та поглиблення сегментації мережевого середовища. Реалізація зазначених заходів дозволить підвищити рівень захищеності, стабільності та масштабованості мережевої інфраструктури малого офісу.

У розділі здійснено оцінку продуктивності, захищеності та економічної доцільності впровадженої VPN-інфраструктури малого офісу. Встановлено, що реалізована система забезпечує стабільний обмін даними між локальним і віддаленим сегментами мережі, а рівень затримок залишається прийнятним для виконання типових офісних завдань.

Аналіз безпеки засвідчив, що застосування ACL-політик дає змогу обмежити доступ до окремих мережевих ресурсів і зменшити ризик несанкціонованої взаємодії між сегментами. Водночас подальше підвищення рівня захисту потребує використання сучасних VPN-протоколів, посиленої автентифікації, VLAN-сегментації та системного моніторингу мережевих подій.

Економічні розрахунки підтвердили доцільність застосування VPN як альтернативи виділеним фізичним каналам зв’язку. Отримані результати свідчать, що запропонована VPN-інфраструктура є придатною для малого офісу, оскільки поєднує достатню продуктивність, базову захищеність, керованість і можливість подальшої модернізації.

ВИСНОВКИ

У результаті виконання роботи було розроблено та перевірено модель VPN-інфраструктури для малого офісу з різними рівнями доступу користувачів. Отримані результати підтвердили, що запропонована мережева модель забезпечує не лише базову міжмережеву взаємодію між локальним і віддаленим сегментами, а й контрольований доступ до внутрішніх ресурсів відповідно до ролі користувача. Успішне проходження пакетів із показником 0% loss підтвердило працездатність сформованого тунелю та коректність маршрутизації між мережами 192.168.10.0/24 і 192.168.20.0/24.

Одержані результати довели, що використання VPN-моделі дає змогу змінити характер роботи мережі: замість ізольованих сегментів формується керований канал взаємодії між офісною та віддаленою частинами інфраструктури. При цьому доступ до ресурсів не надається автоматично всім користувачам, а регулюється через політики доступу. Це є принципово важливим для малого офісу, де одночасно існують адміністративні, робочі, гостьові та віддалені користувачі.

Реалізація ACL підтвердила ефективність розмежування прав доступу. Зокрема, було заблоковано доступ користувача з нижчим рівнем привілеїв до адміністративного сервера 192.168.10.200, що підтверджено результатом Destination host unreachable. Водночас авторизований адміністративний вузол отримав успішну відповідь від цього самого сервера. Отже, система продемонструвала вибіркову фільтрацію трафіку: заборонені запити блокуються, а дозволений трафік проходить без порушення загальної працездатності мережі.

Результати тестування також показали, що побудована VPN-інфраструктура має прийнятні показники стабільності для умов малого офісу. Після завершення налаштування тунелю передавання пакетів здійснювалося без критичних втрат, а час відповіді залишався у межах, достатніх для базових офісних сервісів. Це свідчить про функціональну придатність запропонованої

моделі для організації віддаленого доступу, обміну службовими даними та адміністрування ресурсів у невеликій корпоративній мережі.

Економічний результат полягає в тому, що запропонована модель дозволяє організувати віддалену взаємодію без побудови окремих фізичних каналів зв’язку. Використання програмної емуляції, статичної маршрутизації, тунельних інтерфейсів і ACL знижує витрати на попереднє проєктування та тестування мережевого рішення. Для малого офісу це є доцільним, оскільки забезпечує баланс між вартістю впровадження, рівнем безпеки та простотою адміністрування.

Отже, в даній роботі розроблено, налаштовано й експериментально перевірено модель VPN-інфраструктури малого офісу з різними рівнями доступу. Практичні результати засвідчили, що запропоноване рішення забезпечує керовану міжмережеву взаємодію, розмежування доступу до критичних ресурсів, перевірку політик безпеки та можливість подальшої модернізації шляхом впровадження повноцінних VPN-протоколів, зокрема IPsec, OpenVPN або WireGuard.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ACLs Configuration Guide - Access Control Lists. Cisco IOS XE 17 Configuration Guide. Cisco, 2025. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/security/acls/acls-configuration-guide/access-control-lists.html (дата звернення: 11.05.2026).
2. Chandramouli R. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments : NIST Special Publication 800-207A. Gaithersburg : National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800207A.pdf (дата звернення: 12.05.2026).
3. Choosing a VPN Solution. pfSense Documentation. Netgate, 2025. URL: https://docs.netgate.com/pfsense/en/latest/vpn/selection.html (дата звернення: 13.05.2026).
4. Cisco IOS XE 17 - Configuration Guides. Cisco Documentation. Cisco, 2024. URL: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html (дата звернення: 10.05.2026).
5. Cisco Packet Tracer. Cisco Networking Academy. Cisco, 2026. URL: https://www.netacad.com/cisco-packet-tracer (дата звернення: 16.05.2026).
6. Configure IP Access Lists. Cisco Support Documentation. Cisco, 2025. URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html (дата звернення: 16.05.2026).
7. Configure Route Based Site to Site VPN Tunnel on FTD Managed by FMC. Cisco Support Documentation. Cisco, 2024. URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/216276-configure-route-based-site-to-site-vpn-t.html (дата звернення: 11.05.2026).
8. Configuring Security for VPNs with IPsec. Cisco IOS XE 17 Documentation. Cisco, 2021. URL: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-

x/sec-vpn/b-security-vpn/m_sec-cfg-vpn-ipsec-0.html (дата звернення: 11.05.2026).

9. OpenVPN 2.6 Manual. OpenVPN Community Documentation. OpenVPN, 2023. URL: https://openvpn.net/community-docs/community-articles/openvpn-2-6-manual.html (дата звернення: 11.05.2026).
10. OpenVPN Connect User Guide. OpenVPN Documentation. OpenVPN, 2026. URL: https://openvpn.net/connect-docs/user-guide.html (дата звернення: 10.05.2026).
11. Security and VPN Configuration Guide, Cisco IOS XE 17.x. Cisco Documentation. Cisco, 2021. URL: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn.html (дата звернення: 11.05.2026).
12. Selecting and Hardening Remote Access VPN Solutions : Cybersecurity Information Sheet / NSA, CISA. 2021. URL: https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF (дата звернення: 12.05.2026).
13. WireGuard - RouterOS. MikroTik Documentation. MikroTik, 2026. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/69664792/WireGuard (дата звернення: 12.05.2026).
14. WireGuard. pfSense Documentation. Netgate, 2025. URL: https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/index.html (дата звернення: 13.05.2026).
15. Zohaib S. M. Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Modern Enterprises. Information. 2024. Vol. 15, No. 11. Article 734. URL: https://www.mdpi.com/2078-2489/15/11/734 (дата звернення: 12.05.2026).