Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу
Назва теми

Рівень вищої освіти *перший (бакалаврський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КРКІ 2302127.23.02.34 ПЗ

Виконав здобувач III курсу, група КІ2с-23-2 _____ Владислав ВАВРИНЧУК
Підпис Ініціали, прізвище

Керівник _____ Юрій ВОЙЧУР
Науковий ступінь, учене звання Підпис Ініціали, прізвище

Нормоконтролер _____ Сергій ЛИСЕНКО
Науковий ступінь, учене звання Підпис Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС _____ Ольга ПАВЛОВА
«01» червня 2026 р. підпис Ініціали, прізвище
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ПЕРШИЙ (БАКАЛАВРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІС
_____ Ольга ПАВЛОВА

" 10 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Вавринчуку Владислав Володимировичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу
Керівник проекту (роботи) Войчур Юрій Олексійович. д.ф
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 20.01.2026 р. № 7
2. Термін подання здобувачем роботи на кафедру 01.06.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу
Програмно-апаратна організація системи мереж та доступу до неї
Програмна реалізація захищеного доступу до мережі за допомогою протоколів VPN
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Топологія мережі проєкту
Конфігурації проєкту
Програмне забезпечення проєкту

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормконтроль			
Антиплагіат			

7. Дата видачі завдання «_10_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2026	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2026	виконано
4	Робота над розділом 2 – проектування середовища для реалізації внутрішньої корпоративної мережі із захищеним доступом.	01.04.2026	виконано
5	Робота над розділом 3 – налаштування внутрішньої корпоративної мережі із захищеним доступом на основі VPN	29.04.2026	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2026	виконано
7	Попередній захист ВКР	26.05.2026	виконано
8	Захист ВКР на засіданні ЕК	Червень 2026 року	

Здобувач_____ Владислав ВАВРИНЧУК
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи_____ Юрій ВОЙЧУР
Підпис Ім'я, ПРІЗВИЩЕ

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КРКІ 2302127.23.02.34 ПЗ	Пояснювальна записка	63		
			Графічні матеріали			
2		КРКІ 2302127.23.02.34 ПЗ	Топологія мережі проєкту	1		
3		КРКІ 2302127.23.02.34 ПЗ	Конфігурації проєкту	1		
4		КРКІ 2302127.23.02.34 ПЗ	Програмне забеспечення	1		
			проєкту			

Зм	Арк	№ докум	Підпис	Дата	КРКІ 2302127.23.02.34 ПЗ		
Розробив		Владислав		01.06	Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Войчур				У	1	1
						ХНУ, КІ2с-23-2		
Н. контр.		Лисенко						
Затв.		Павлова		01.06				

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу».

Автор роботи: Владислав ВАВРИНЧУК.

Керівник роботи: Юрій ВОЙЧУР.

Пояснювальна записка: 63 с., 36 рис., 5 табл., 3 дод., 41 джерел.

Графічна частина: 3 креслення.

АРХІТЕКТУРА, КОМП'ЮТЕРНА МЕРЕЖА, VPN, ОРГАНІЗАЦІЯ МЕРЕЖІ.

Кваліфікаційна робота бакалавра присвячена проєктуванню та реалізації внутрішньої корпоративної мережі компанії із захищеним віддаленим доступом. Актуальність теми зумовлена необхідністю безпечного об'єднання віддалених підрозділів підприємства, забезпечення стабільного обміну службовими даними, централізованого доступу до внутрішніх ресурсів та підтримки безперервної роботи корпоративної інформаційної інфраструктури.

Метою роботи є розробка, налаштування та перевірка працездатності захищеної мережевої інфраструктури, яка забезпечує взаємодію між окремими локальними сегментами організації. У межах роботи було розглянуто принципи побудови корпоративних мереж, організації захищеного зв'язку, маршрутизації між підмережами та підключення віддаленого підрозділу до єдиної доменної інфраструктури. У результаті було створено функціональну модель мережі, що забезпечує захищений обмін трафіком між підрозділами та може бути використана як основа для побудови корпоративної інфраструктури малого або середнього підприємства.

Підпис здобувача

30.05.2026

Дата

ЗМІСТ

ВСТУП

У сучасних умовах розвитку інформаційних технологій корпоративні мережі відіграють ключову роль у забезпеченні стабільної роботи підприємств, організацій та установ. Через локальні та глобальні мережі здійснюється обмін службовою інформацією, доступ до внутрішніх ресурсів, передавання файлів, робота з базами даних, використання серверних сервісів, систем відеоспостереження, телефонії, бухгалтерських програм та інших інформаційних систем. Саме тому правильна організація внутрішньої корпоративної мережі є важливою умовою для безперервної та безпечної роботи компанії.

Особливої актуальності набуває питання захищеного доступу до корпоративної мережі у випадках, коли підприємство має декілька територіально віддалених офісів або підрозділів. У такій ситуації виникає необхідність об’єднати декілька локальних мереж в єдину логічну інфраструктуру, щоб користувачі різних офісів могли безпечно обмінюватися даними та отримувати доступ до спільних ресурсів. При цьому використання відкритого Інтернету без додаткових засобів захисту створює значні ризики, пов’язані з перехопленням трафіку, несанкціонованим доступом, підміною даних або атакою на мережеве обладнання.

Одним із найбільш ефективних способів вирішення цієї проблеми є використання технології VPN. Віртуальна приватна мережа дозволяє створити захищений тунель між окремими мережевими вузлами або цілими локальними мережами поверх публічної мережі Інтернет. Завдяки цьому забезпечується конфіденційність переданих даних, контроль доступу, автентифікація учасників з’єднання та можливість безпечного об’єднання віддалених сегментів корпоративної інфраструктури.

Основна увага приділяється практичній реалізації мережі, яка складається з двох локальних сегментів, побудованих на базі маршрутизаторів MikroTik, та

віддаленого OpenVPN-сервера, що виконує роль центрального вузла для захищеного об’єднання цих мереж. Такий підхід дозволяє реалізувати модель site-to-site VPN, за якої не окремий користувач підключається до корпоративної мережі, а цілі локальні мережі з’єднуються між собою через захищений канал.

1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ВНУТРІШНЬОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАХИЩЕНИМ ДОСТУПОМ

1.1 Поняття про мережі

Комп’ютерна мережа – це сукупність взаємопов’язаних комп’ютерів, серверів, мережевого обладнання, периферійних пристроїв та програмних засобів, які забезпечують обмін даними між користувачами й інформаційними системами. Основним призначенням мережі є передавання інформації, спільне використання ресурсів, централізоване адміністрування, організація доступу до сервісів і забезпечення взаємодії між окремими пристроями в межах певної інфраструктури.

У сучасних умовах комп’ютерні мережі є основою роботи більшості підприємств, установ та організацій. Через мережу користувачі отримують доступ до внутрішніх баз даних, файлових серверів, систем електронного документообігу, бухгалтерських програм, корпоративної пошти, систем відеоспостереження, інтернет-ресурсів та інших служб. Без правильно організованої мережевої інфраструктури неможливо забезпечити стабільну роботу компанії, особливо якщо вона має декілька офісів або віддалених підрозділів.

Основними елементами комп’ютерної мережі є кінцеві пристрої, мережеве обладнання, середовище передавання даних і програмні служби. До кінцевих пристроїв належать персональні комп’ютери, ноутбуки, сервери, принтери, IP-телефони, камери відеоспостереження, мобільні пристрої та інше обладнання, яке створює або споживає мережевий трафік. Мережеве обладнання забезпечує передавання, фільтрацію та маршрутизацію даних. До нього належать комутатори, маршрутизатори, точки доступу, міжмережеві екрани, VPN-сервери та інші пристрої.

Для ідентифікації пристроїв у мережі використовується IP-адресація. IP-адреса дозволяє визначити, з якого пристрою надходить пакет і до якого

пристрою його потрібно доставити. У локальних мережах найчастіше застосовуються приватні адресні діапазони, наприклад 192.168.0.0/16, 172.16.0.0/12 або 10.0.0.0/8. Такі адреси не маршрутизуються безпосередньо в глобальній мережі Інтернет, але широко використовуються всередині домашніх, офісних і корпоративних мереж.

Важливим поняттям у комп'ютерних мережах є підмережа. Підмережа – це логічно виділена частина IP-мережі, у межах якої пристрої можуть взаємодіяти між собою напряму або через шлюз. Наприклад, одна локальна мережа може використовувати адресний простір 192.168.5.0/24, а інша – 192.168.6.0/24. Кожна з таких мереж має власний діапазон адрес, власний шлюз і власні клієнтські пристрої. Для передавання даних між різними підмережами необхідна маршрутизація.

Маршрутизація – це процес визначення шляху передавання пакетів між різними мережами. Якщо пристрій звертається до адреси, яка не належить до його локальної підмережі, пакет передається на шлюз за замовчуванням. Шлюз аналізує адресу призначення та пересилає пакет у потрібному напрямку відповідно до таблиці маршрутизації. У невеликих мережах часто застосовується статична маршрутизація, коли маршрути задаються адміністратором вручну. У великих інфраструктурах можуть використовуватися динамічні протоколи маршрутизації.

Для автоматичного налаштування клієнтських пристроїв у мережі використовується протокол DHCP. DHCP-сервер автоматично видає пристроям IP-адресу, маску підмережі, адресу шлюзу за замовчуванням, DNS-сервери та інші параметри. Це спрощує адміністрування, оскільки адміністратору не потрібно вручну задавати мережеві параметри на кожному комп'ютері. У корпоративних мережах DHCP є важливим сервісом, що забезпечує швидке підключення нових пристроїв і зменшує ризик конфліктів IP-адрес.

Комп'ютерні мережі можуть мати різний масштаб. Найпоширенішим типом є локальна мережа, або LAN, яка об'єднує пристрої в межах одного

приміщення, офісу, поверху або будівлі. Локальні мережі характеризуються високою швидкістю передавання даних, низькою затримкою та можливістю повного контролю з боку адміністратора. Саме локальні мережі є основою внутрішньої інфраструктури підприємства.

Глобальна мережа, або WAN, використовується для об'єднання локальних мереж на значних відстанях. Найвідомішим прикладом глобальної мережі є Інтернет. Для компаній WAN-з'єднання важливі тоді, коли потрібно об'єднати декілька офісів, віддалених підрозділів або надати доступ до корпоративних ресурсів працівникам, які перебувають поза межами основного офісу. Однак використання публічних мереж створює ризики для безпеки, тому в таких випадках застосовуються додаткові механізми захисту, зокрема VPN.

Внутрішня корпоративна мережа – це мережа, яка створюється для забезпечення інформаційних потреб конкретної організації. Вона може складатися з одного або кількох локальних сегментів, серверної частини, мережевого обладнання, служб адресації, систем безпеки та засобів віддаленого доступу. Основними вимогами до такої мережі є стабільність, керованість, масштабованість, захищеність і можливість контролю доступу до ресурсів.

Таким чином, комп'ютерна мережа є основою сучасної корпоративної інфраструктури. Вона забезпечує передавання даних, доступ до ресурсів, взаємодію між користувачами та централізоване адміністрування. Для правильної побудови мережі необхідно враховувати IP-адресацію, роботу DHCP, маршрутизацію, захист трафіку та організацію доступу між окремими підмережами.

1.2 Спосіб організації мереж

Спосіб організації мережі визначає її логічну та фізичну структуру, принципи взаємодії між пристроями, розподіл функцій між вузлами та порядок доступу до мережевих ресурсів. Від обраного способу організації залежить

стабільність роботи мережі, складність адміністрування, рівень безпеки, можливість масштабування та ефективність використання обладнання.

Мережі можуть організовуватися за різними принципами. Найчастіше їх класифікують за моделлю взаємодії пристроїв, топологією підключення, способом адміністрування та способом об’єднання окремих мережевих сегментів. Для корпоративних мереж найбільш важливими є клієнт-серверна модель, правильна організація маршрутизації, централізоване керування службами та захищене з’єднання між віддаленими мережами.

Одним із найпростіших способів організації є однорангова мережа. У такій мережі всі пристрої мають приблизно однаковий статус і можуть одночасно виконувати роль клієнта та сервера. Перевагою такої організації є простота налаштування та відсутність потреби в окремому сервері. Однак однорангова мережа має суттєві недоліки: складність контролю доступу, відсутність централізованого адміністрування, низький рівень безпеки та незручність масштабування. Приклад однорангової мережі зображений на рисунку 1.1.

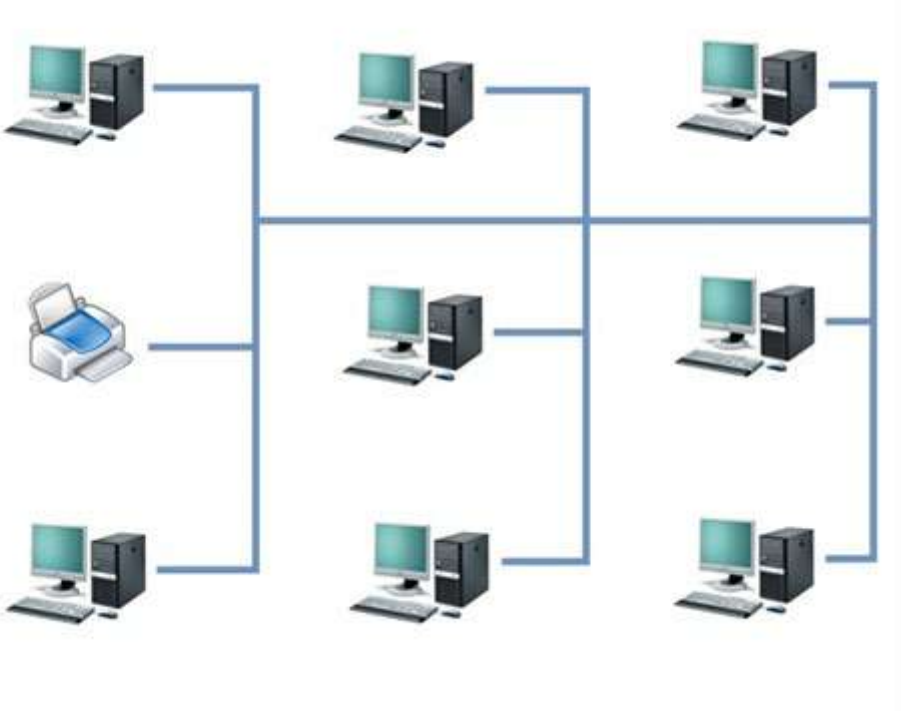


Рисунок 1.1 – Вигляд однорангової мережі [1]

Для корпоративного середовища більш доцільною є клієнт-серверна модель. У такій мережі окремі сервери або мережеві вузли надають послуги клієнтським пристроям. Сервер може виконувати функції зберігання файлів, керування користувачами, видачі IP-адрес, обробки запитів, маршрутизації або організації VPN-доступу. Клієнти звертаються до серверів для отримання відповідних сервісів. Така модель забезпечує кращий контроль, зручніше адміністрування та вищий рівень безпеки. На рисунку 1.2 зображений вигляд мережі «клієнт-сервер».

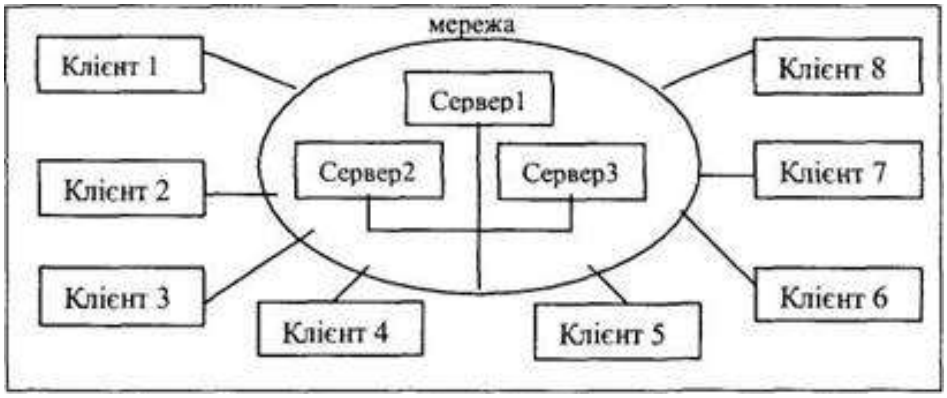


Рисунок 1.2 – Вигляд мережі «клієнт-сервер» [4]

За фізичною структурою мережі можуть будуватися за різними топологіями. Найбільш поширеними є топології «шина», «кільце», «зірка», «дерево», «коміркова» та змішана топологія. У сучасних локальних мережах найчастіше використовується топологія «зірка», за якої всі клієнтські пристрої підключаються до центрального вузла – комутатора або маршрутизатора. Така схема є простою, надійною та зручною для обслуговування.

Топологія «зірка» має низку переваг. Якщо один клієнтський пристрій або кабель виходить з ладу, інші пристрої продовжують працювати. Також у такій мережі легко додавати нові пристрої, контролювати підключення та виконувати діагностику несправностей. Саме тому ця топологія є типовою для офісних і корпоративних мереж невеликого та середнього масштабу.

Топологія «дерево» є розширенням топології «зірка» та використовується в більших мережах. Вона передбачає наявність декількох рівнів: центрального вузла, проміжних вузлів і кінцевих пристроїв. Такий підхід зручний для великих офісів, навчальних закладів або підприємств, де мережа охоплює кілька поверхів або корпусів. Проте для невеликої інфраструктури з двома окремими локальними мережами достатньо простішої схеми. Види топології мереж зображений на рисунку 1.3.

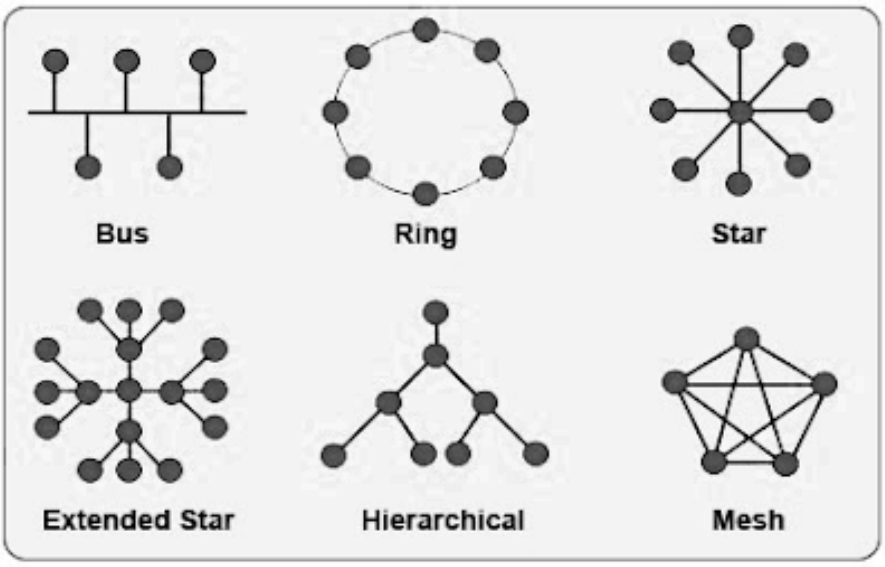


Рисунок 1.3 – Топологія мережі [2]

Особливістю даної реалізації є те, що розділення мереж виконується не за допомогою VLAN, а через використання окремих IP-підмереж. Кожна локальна мережа функціонує як самостійний сегмент із власними мережевими параметрами. Такий підхід спрощує схему, робить її зрозумілішою для адміністрування та є достатнім для поставленої задачі, оскільки основна мета роботи полягає не в сегментації однієї фізичної мережі, а в об'єднанні двох окремих мереж через VPN.

За способом адміністрування мережі можуть бути централізованими, децентралізованими або комбінованими. У централізованій мережі основні функції керування зосереджені на одному або кількох центральних вузлах. Це

може бути сервер автентифікації, VPN-сервер, контролер домену, DHCP-сервер або центральний маршрутизатор. Централізований підхід забезпечує кращий контроль і зручніше адміністрування, однак створює залежність від працездатності центрального вузла.

Децентралізована мережа передбачає, що окремі вузли мають більшу автономність і не залежать від єдиного центру керування. Такий підхід може бути корисним у невеликих мережах або тимчасових інфраструктурах, але в корпоративному середовищі він менш зручний через складність контролю доступу, моніторингу та підтримки єдиної політики безпеки.

У практичній частині роботи доцільно використовувати комбіновану організацію. Кожна локальна мережа працює автономно та має власні служби адресації, але захищене з'єднання між мережами організовується через центральний VPN-сервер. У такій схемі локальні мережі можуть працювати самостійно, але при наявності VPN-з'єднання отримують можливість взаємодіяти між собою.

Загалом спосіб організації мережі в даній роботі можна визначити як об'єднання двох незалежних локальних мереж через центральний персональний VPN-сервер із використанням статичної маршрутизації. Такий підхід дозволяє забезпечити контрольований і захищений обмін даними між клієнтами різних мереж, не потребує складної сегментації та може бути застосований для малих і середніх корпоративних інфраструктур.

1.3 Види зв'язку мереж

Зв'язок між мережами – це спосіб організації передавання даних між окремими локальними або глобальними мережевими сегментами. Він необхідний у випадках, коли пристрої однієї мережі повинні отримувати доступ до ресурсів іншої мережі. У корпоративному середовищі такий зв'язок використовується для об'єднання офісів, підключення віддалених працівників,

доступу до серверів, взаємодії з хмарними сервісами та передавання службових даних між різними підрозділами.

Існує декілька основних способів зв’язку мереж: локальне з’єднання через комутаційне обладнання, маршрутизоване з’єднання між підмережами, з’єднання через провайдера, підключення через глобальну мережу Інтернет і захищене з’єднання за допомогою VPN. Кожен із цих способів має свої переваги, недоліки та сферу застосування.

Найпростішим видом зв’язку є з’єднання пристроїв у межах однієї локальної мережі. У такому випадку всі пристрої перебувають в одному адресному просторі та можуть обмінюватися даними без участі маршрутизатора. Передавання кадрів у межах локального сегмента забезпечується комутатором або іншим мережевим обладнанням канального рівня. Такий зв’язок є швидким і простим, але він підходить лише для мереж, розташованих в одному фізичному місці.

Якщо потрібно організувати взаємодію між різними IP-підмережами, використовується маршрутизоване з’єднання. У цьому випадку кожна мережа має власний адресний простір, а передавання даних між ними виконується через маршрутизатор або інший пристрій, здатний працювати на мережевому рівні. Маршрутизатор аналізує IP-адресу призначення та визначає, через який інтерфейс потрібно передати пакет. Саме такий принцип використовується при взаємодії між окремими локальними мережами.

Маршрутизоване з’єднання може бути реалізоване за допомогою статичних або динамічних маршрутів. Статичні маршрути задаються адміністратором вручну. Вони прості, передбачувані та зручні для невеликих інфраструктур. Динамічні маршрути формуються автоматично за допомогою спеціальних протоколів, таких як OSPF, RIP або BGP. Динамічна маршрутизація доцільна у великих мережах із великою кількістю вузлів і маршрутів.

Іншим видом зв’язку є підключення через мережу провайдера. У цьому випадку організація може орендувати канал зв’язку між офісами або

використовувати спеціалізовані послуги оператора. Такий підхід може забезпечувати високу стабільність, передбачувану якість каналу та технічну підтримку. Однак він часто потребує додаткових фінансових витрат і залежить від можливостей конкретного провайдера. Для невеликих компаній або навчальних проєктів такий варіант не завжди є доцільним.

Найбільш поширеним способом зв'язку між віддаленими мережами є використання Інтернету. Інтернет дозволяє з'єднувати мережі незалежно від їх фізичного розташування. Проте передавання службового або корпоративного трафіку через публічну мережу без додаткового захисту є небезпечним. Дані можуть проходити через проміжні вузли, які не контролюються організацією, що створює ризик перехоплення, аналізу або підміни трафіку.

Для усунення цих ризиків використовується захищений зв'язок на основі VPN. VPN дозволяє створити зашифрований тунель поверх публічної мережі. Через цей тунель передаються пакети між віддаленими мережами або окремими клієнтами. Завдяки шифруванню сторонні особи не можуть прочитати передані дані, навіть якщо мають доступ до каналу зв'язку. Крім того, VPN забезпечує автентифікацію учасників з'єднання, що дозволяє обмежити доступ лише для дозволених пристроїв.

За способом організації VPN-зв'язок можна поділити на два основні види: remote access VPN і site-to-site VPN. Remote access VPN використовується для підключення окремого користувача до корпоративної мережі. Наприклад, працівник може підключитися до VPN зі свого ноутбука та отримати доступ до внутрішніх ресурсів компанії. Такий варіант зручний для віддаленої роботи окремих співробітників.

Site-to-site VPN використовується для об'єднання цілих локальних мереж. У цьому випадку VPN-з'єднання встановлюється між шлюзами або маршрутизаторами, а кінцеві клієнти не потребують окремого VPN-клієнта. Вони працюють у своїй локальній мережі та передають трафік до віддаленої

мережі через свій шлюз. Саме цей вид зв’язку є основним для даної роботи, оскільки необхідно забезпечити взаємодію між двома локальними мережами.

Перевагою site-to-site VPN є прозорість для користувачів. Клієнтам не потрібно вручну запускати VPN-з’єднання або налаштовувати додаткове програмне забезпечення. Усі необхідні параметри задаються на рівні мережевого обладнання та VPN-сервера. Це спрощує адміністрування, підвищує стабільність і дозволяє централізовано контролювати захищений зв’язок між офісами.

Окрему увагу під час організації зв’язку між мережами потрібно приділяти правилам фільтрації та безпеки. Навіть якщо мережі об’єднані через VPN, це не означає, що всі пристрої повинні мати необмежений доступ один до одного. У корпоративному середовищі доцільно визначати, які саме підмережі, порти та сервіси мають бути доступними. Для цього можуть використовуватися правила firewall, списки доступу, обмеження маршрутів і політики безпеки.

Таким чином, існують різні види зв’язку мереж, починаючи від простого локального з’єднання і завершуючи захищеними тунелями через Інтернет. Для побудови корпоративної мережі з віддаленими сегментами найбільш доцільним є використання VPN-з’єднання типу site-to-site. Такий підхід дозволяє безпечно об’єднати окремі локальні мережі, забезпечити маршрутизацію між ними та зберегти контроль над передаванням корпоративного трафіку.

1.4. Поняття та види VPN-протоколів

VPN, або віртуальна приватна мережа, – це технологія, яка дозволяє створювати захищене з’єднання між пристроями або мережами поверх незахищеного середовища, найчастіше Інтернету. Основна ідея VPN полягає у створенні зашифрованого тунелю, через який передаються дані між учасниками з’єднання. Завдяки цьому інформація захищається від перехоплення, аналізу та підміни сторонніми особами.

VPN використовується як у персональних, так і в корпоративних сценаріях. У персональному використанні VPN часто застосовується для захисту трафіку в публічних Wi-Fi-мережах, приховування реальної IP-адреси або

доступу до віддалених ресурсів. У корпоративному середовищі VPN має більш прикладне значення: він дозволяє організовувати віддалений доступ працівників до внутрішньої мережі, об’єднувати філії компанії, підключати віддалені сервери та створювати захищену інфраструктуру між територіально розподіленими об’єктами.

Основними функціями VPN є шифрування трафіку, аунтифікація учасників з’єднання, інкапсуляція пакетів і забезпечення логічної присутності пристрою або мережі в іншому мережевому сегменті. Шифрування захищає дані від прочитання сторонніми особами. Автентифікація дозволяє перевірити, що до VPN підключаються лише дозволені користувачі або пристрої. Інкапсуляція дає змогу передавати пакети однієї мережі всередині пакетів іншої мережі.

VPN-протокол визначає спосіб встановлення захищеного з’єднання, методи шифрування, порядок автентифікації, принципи передавання пакетів і особливості роботи тунелю. Від вибору VPN-протоколу залежить рівень безпеки, швидкість роботи, стабільність з’єднання, складність налаштування та сумісність із різними операційними системами й мережевим обладнанням.

Одним із найвідоміших і найпоширеніших VPN-протоколів є OpenVPN.

OpenVPN має високий рівень безпеки завдяки використанню сертифікатів, ключів і сучасних алгоритмів шифрування. Він дозволяє налаштовувати автентифікацію клієнтів, шифрування трафіку, маршрутизацію, доступ до окремих підмереж і додаткові параметри захисту. Саме гнучкість є однією з головних переваг OpenVPN. Його можна використовувати як для підключення окремих користувачів, так і для організації site-to-site VPN між різними мережами.

До переваг OpenVPN належать надійність, відкритий вихідний код, широка підтримка операційних систем, сумісність із багатьма мережевими пристроями та можливість детального налаштування. Недоліками є відносно складна конфігурація, потреба в роботі з сертифікатами та більша кількість параметрів у порівнянні з деякими сучасними протоколами. Однак для

корпоративних задач OpenVPN залишається одним із найбільш універсальних і перевірених рішень.

Іншим сучасним VPN-протоколом є WireGuard. Це відносно новий протокол, який відрізняється простотою, високою продуктивністю та використанням сучасних криптографічних алгоритмів. WireGuard має значно менший обсяг коду порівняно з OpenVPN або IPSec, що спрощує аудит безпеки та знижує ймовірність помилок. Він працює поверх UDP і забезпечує низьку затримку, що робить його ефективним для мобільних пристроїв і швидких VPN-з'єднань.

WireGuard використовує пару ключів – приватний і публічний – для кожного учасника з'єднання. Кожен клієнт і сервер мають власні ключі, за допомогою яких виконується автентифікація та встановлення захищеного каналу. Такий підхід спрощує конфігурацію, але водночас вимагає уважного керування ключами. WireGuard добре підходить для сучасних легких VPN-рішень, однак у деяких корпоративних сценаріях OpenVPN може бути зручнішим через ширшу підтримку, гнучкість і звичність налаштування.

Ще одним поширеним протоколом є IPSec. IPSec – це набір протоколів для захисту IP-трафіку на мережевому рівні. Він може використовуватися для шифрування, автентифікації та забезпечення цілісності даних. IPSec часто застосовується в корпоративних мережах, особливо для site-to-site VPN між маршрутизаторами або міжмережевими екранами. Його перевагою є високий рівень безпеки та підтримка багатьма операційними системами й мережевими пристроями.

2 ПРОЄКТУВАННЯ СЕРЕДОВИЩА ДЛЯ РЕАЛІЗАЦІЇ ВНУТРІШНЬОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАХИЩЕНИМ ДОСТУПОМ

2.1 Топологія мережі

Топологія мережі є важливим етапом проєктування, оскільки вона дозволяє наочно відобразити логічну та фізичну структуру майбутньої інфраструктури. За допомогою карти мережі визначаються основні вузли, адресні простори, шлюзи, сервери, клієнтські пристрої та канали зв’язку між окремими сегментами. Такий підхід спрощує подальше налаштування обладнання, маршрутизації, DHCP-служб і VPN-з’єднання. Графічна карта та логічна топологія злбражена на рисунку 2.1, та таблиці 2.1.

У даному проєкті мережа складається з трьох основних частин:

1) головний підрозділ компанії;
2) додатковий підрозділ компанії;
3) віддалений VPN-сервер на базі OpenVPN.

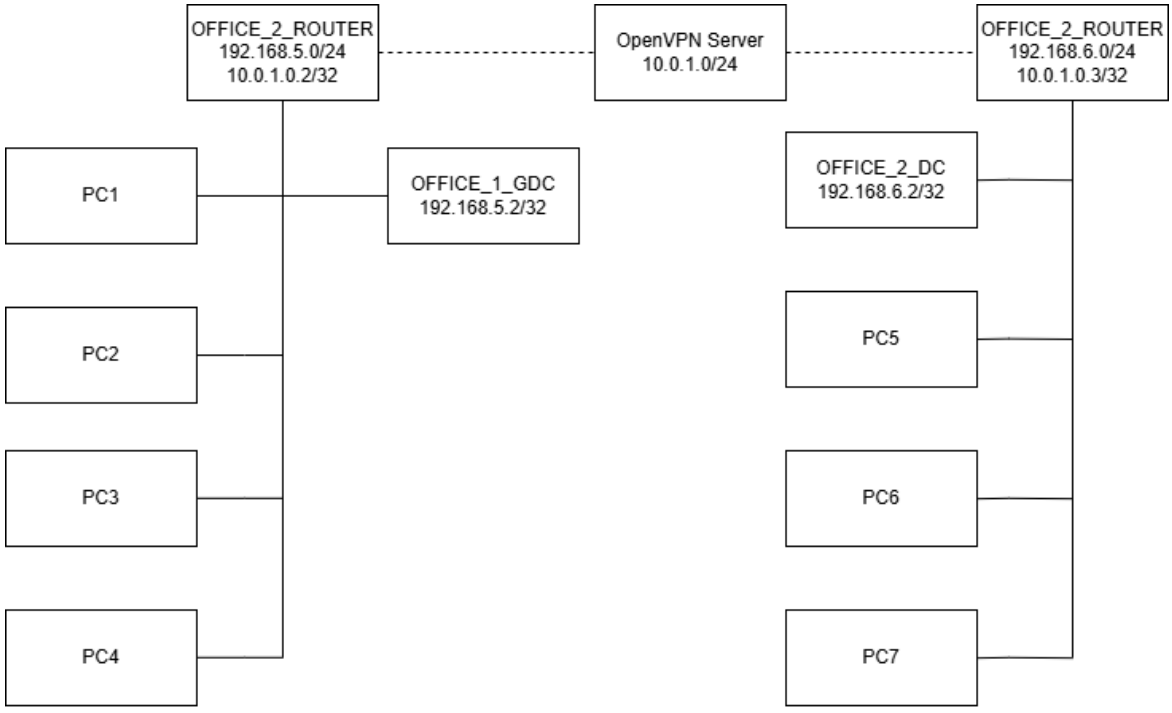


Рисунок 2.1 – Графічна карта мережі

Таблиця 2.1 – Логічна топологія мережі

Головний підрозділ(192.168.5.0/24)			
Назва пристрою	IP-адрес в мережі	Роль	VLAN
Office_1_Router	192.168.5.1 / 10.0.1.2	Роутер	-
Office1_gdc	192.168.5.2	Головний контролер домену, днс сервер	1
PC1	192.168.5.3	Комп'ютер адміністратора	1
PC2	dhcp	Комп'ютер співробітника	1
PC3	dhcp	Комп'ютер співробітника	1
PC4	dhcp	Комп'ютер співробітника	1
Додатковий підрозділ(192.168.6.0/24)			
Назва пристрою	IP-адрес в мережі	Роль	VLAN
Office_2_Router	192.168.6.1 / 10.0.1.3	Роутер	-
Office2_gdc	192.168.6.2	Контролер домену, днс сервер	1
PC5	dhcp	Комп'ютер співробітника	1
PC6	dhcp	Комп'ютер співробітника	1

Кінець таблиці 2.1

PC7	dhcp	Комп'ютер співробітника	1
Мережа OpenVPN			
Назва пристрою	IP-адрес в мережі	Роль	VLAN
Office_1_Router	10.0.1.2	Клієнт	-
Office_2_Router	10.0.1.3	Клієнт	-
Server	10.0.1.1	Сервер	-

Головний підрозділ використовує локальну мережу з адресним простором 192.168.5.0/24. Основним шлюзом цієї мережі є маршрутизатор з адресою 192.168.5.1. Також у головному офісі розміщений основний сервер Office1_gdc з адресою 192.168.5.2, який виконує роль головного контролера домену та DNS-сервера. Наявність контролера домену в головному офісі є важливою частиною корпоративної інфраструктури, оскільки саме він забезпечує централізовану автентифікацію користувачів, керування доменними обліковими записами та роботу служб імен.

У локальній мережі головного офісу також розміщені клієнтські комп’ютери працівників. Один із комп’ютерів має статичну IP-адресу 192.168.5.3, а інші клієнтські пристрої отримують мережеві параметри автоматично через DHCP. Використання DHCP дозволяє спростити адміністрування мережі, оскільки нові пристрої можуть автоматично отримувати IP-адресу, маску підмережі, шлюз і DNS-сервер без ручного налаштування.

Додатковий підрозділ використовує окрему локальну мережу з адресним простором 192.168.6.0/24. Його основним шлюзом є маршрутизатор з адресою 192.168.6.1. У цьому підрозділі передбачено сервер Office2_gdc з адресою 192.168.6.2, який у майбутньому може виконувати роль додаткового контролера

домену. Для коректної роботи такого сервера необхідно забезпечити стабільний зв’язок із головним контролером домену, розташованим у мережі головного офісу.

У головному офісі сервер Office1_gdc виконує роль головного контролера домену. Це означає, що він є ключовим елементом доменної інфраструктури. До його функцій може належати автентифікація користувачів, обробка DNS-запитів, зберігання інформації про домен, підтримка групових політик і взаємодія з іншими доменними службами. У додатковому підрозділі передбачається розміщення другого сервера Office2_gdc, який може бути налаштований як додатковий контролер домену.

Для того щоб додатковий контролер домену міг коректно працювати, він повинен мати стабільний мережевий зв’язок з основним контролером домену. Через цей зв’язок можуть передаватися DNS-запити, службовий трафік Active Directory, реплікація доменних даних і запити автентифікації. Оскільки підрозділи знаходяться в різних локальних мережах, передавання такого трафіку повинно виконуватися через захищений канал. У даній роботі таким каналом є OpenVPN-тунель.

Логічна топологія мережі передбачає, що кожен підрозділ має власний маршрутизатор, власну локальну мережу та власні клієнтські пристрої. Маршрутизатори підключаються до VPN-сервера як клієнти. Після встановлення VPN-з’єднання між ними налаштовується маршрутизація, яка дозволяє передавати трафік між мережами 192.168.5.0/24 і 192.168.6.0/24 через VPN-сегмент 10.0.1.0/24.

2.2 Вибір апаратних засобів для реалізації мережі

Для реалізації внутрішньої корпоративної мережі необхідно правильно обрати апаратні засоби, які забезпечуватимуть роботу локальних сегментів, маршрутизацію між підмережами, підключення клієнтських пристроїв, роботу

DHCP-служб і взаємодію з VPN-сервером. Від вибору мережевого обладнання залежить стабільність роботи інфраструктури, швидкість передавання даних, можливість подальшого масштабування та рівень захисту корпоративного трафіку.

Основними мережевими вузлами в даній роботі є два маршрутизатори, які виконують роль шлюзів для локальних мереж головного та додаткового підрозділів. Перший маршрутизатор обслуговує мережу головного офісу 192.168.5.0/24, а другий – мережу додаткового підрозділу 192.168.6.0/24. Кожен із них відповідає за передавання трафіку між локальними клієнтами, видачу мережевих параметрів через DHCP та підключення до VPN-сегмента.

У мережі головного офісу маршрутизатор має локальну адресу 192.168.5.1 і виконує функцію основного шлюзу для клієнтських пристроїв. Через нього робочі станції, сервер головного контролера домену та інші пристрої можуть отримувати доступ до інших мережевих сегментів. У VPN-мережі цей маршрутизатор отримує адресу 10.0.1.2, що дозволяє йому передавати трафік через захищений тунель до VPN-сервера.

Маршрутизатор додаткового підрозділу має локальну адресу 192.168.6.1 і є шлюзом для пристроїв мережі 192.168.6.0/24. До цієї мережі входить сервер Office2_gdc з адресою 192.168.6.2, який у майбутньому може виконувати роль додаткового контролера домену, а також клієнтські комп’ютери співробітників. У VPN-сегменті маршрутизатор додаткового підрозділу отримує адресу 10.0.1.3.

Для подібних задач можуть використовуватися маршрутизатори різних виробників. Основними вимогами до такого обладнання є підтримка IP-маршрутизації, DHCP, статичних маршрутів, firewall, NAT, VPN-клієнта або VPN-шлюзу, а також можливість гнучкого налаштування правил обробки трафіку. У невеликих корпоративних мережах важливими також є доступна вартість обладнання, простота обслуговування та достатня продуктивність для обробки трафіку між локальними мережами.

Під час вибору апаратних засобів для побудови корпоративної мережі можна розглядати різних виробників мережевого обладнання, зокрема Cisco, Juniper Networks, Ubiquiti, TP-Link Omada, Fortinet, Huawei, D-Link, Zyxel та MikroTik. Кожен із цих виробників має власну сферу застосування, рівень функціональності, модель адміністрування та ціновий сегмент.

Одним із найвідоміших виробників корпоративного мережевого обладнання є Cisco. Обладнання Cisco широко використовується у великих корпоративних, провайдерських і дата-центрових мережах. Його перевагами є висока надійність, підтримка великої кількості мережевих протоколів, розвинені можливості маршрутизації, якісна документація та професійна екосистема навчання. Водночас рішення Cisco часто мають високу вартість і потребують достатнього рівня підготовки адміністратора, тому для невеликої навчальної або лабораторної реалізації вони можуть бути надмірними.

Ubiquiti пропонує обладнання, яке активно використовується в малому та середньому бізнесі, офісних мережах, бездротових інфраструктурах і провайдерських рішеннях. Особливо популярною є лінійка UniFi, яка забезпечує централізоване керування мережевими пристроями через зручний інтерфейс. До переваг Ubiquiti можна віднести простоту адміністрування, сучасний веб-інтерфейс і хороше співвідношення вартості та функціональності. Недоліком є менша гнучкість низькорівневого налаштування у порівнянні з професійними маршрутизаторами.

TP-Link Omada є доступним рішенням для невеликих офісів, магазинів, навчальних закладів і малого бізнесу. Обладнання цієї серії підтримує централізоване керування, базову маршрутизацію, VLAN, VPN, firewall і бездротові мережі. Основною перевагою TP-Link Omada є невисока вартість і простота налаштування. Проте для складних сценаріїв маршрутизації або нестандартних VPN-конфігурацій такі рішення можуть мати обмеження.

Окремо варто розглянути MikroTik, оскільки обладнання цього виробника часто використовується в малому й середньому бізнесі, провайдерських мережах

і навчальних лабораторіях. Його основною перевагою є операційна система RouterOS, яка підтримує IP-маршрутизацію, DHCP, NAT, firewall, статичні та динамічні маршрути, VPN, тунелювання та інші мережеві функції. При цьому вартість таких пристроїв зазвичай нижча, ніж у багатьох професійних корпоративних рішень.

2.3 Вибір програми гіпервізора

Для реалізації симуляції мережевого середовища у даному проєкті використовується гіпервізор Hyper-V. Гіпервізор – це програмний або апаратно-програмний засіб, який дозволяє створювати та запускати віртуальні машини на одному фізичному комп’ютері. Кожна віртуальна машина працює як окремий комп’ютер із власною операційною системою, мережевими адаптерами, дисковим простором і виділеними апаратними ресурсами.

Hyper-V є вбудованою платформою віртуалізації від Microsoft, яка доступна у серверних і професійних редакціях Windows. Вона дозволяє створювати віртуальні машини, керувати їх ресурсами, налаштовувати віртуальні комутатори, організовувати ізольовані мережі та моделювати складні інфраструктури. Саме ці можливості роблять Hyper-V зручним інструментом для побудови тестового середовища корпоративної мережі.

Hyper-V також дозволяє гнучко розподіляти ресурси між віртуальними машинами. Для кожної машини можна визначити обсяг оперативної пам’яті, кількість віртуальних процесорів, розмір диска та кількість мережевих адаптерів. Це важливо для моделювання мережевого середовища, оскільки маршрутизатор, сервер VPN і контролер домену можуть мати різні вимоги до ресурсів.

Ще однією перевагою використання Hyper-V є можливість створення контрольних точок. Контрольна точка дозволяє зберегти стан віртуальної машини перед внесенням змін. Якщо після налаштування виникає помилка, систему можна швидко повернути до попереднього стану. Це особливо корисно

під час налаштування VPN, маршрутизації або серверних служб, оскільки дозволяє безпечно виконувати експерименти та тестування.

У порівнянні з іншими гіпервізорами, такими як VirtualBox або VMware Workstation, Hyper-V має тісну інтеграцію з Windows, стабільну роботу з віртуальними мережами та зручні засоби адміністрування. Це дозволяє використовувати його як основу для моделювання корпоративної інфраструктури з кількома серверами, маршрутизаторами та клієнтськими пристроями.

2.4 Вибір операційної системи для VPN-сервера

Для розгортання VPN-сервера у даному проєкті обрано операційну систему Ubuntu Server. Це серверна версія популярного дистрибутива Linux, яка широко використовується для побудови мережевих сервісів, веб-серверів, файлових серверів, VPN-серверів, систем моніторингу та інших інфраструктурних рішень. Ubuntu Server є стабільною, безкоштовною та добре документованою операційною системою, що робить її доцільним вибором для навчальних і практичних проєктів.

Ubuntu Server підтримує широкий набір мережевих інструментів. У ній можна налаштовувати IP-адресацію, маршрутизацію, firewall, NAT, VPN-служби, системні журнали та засоби моніторингу. Для розгортання OpenVPN доступні офіційні пакети, які встановлюються через стандартний менеджер пакетів. Це спрощує встановлення, оновлення та супровід VPN-сервера.

У межах даного проєкту Ubuntu Server виконує роль центрального вузла VPN-мережі. Саме на ньому розгортається OpenVPN-сервер, який приймає підключення від мережевих шлюзів двох локальних мереж. VPN-сервер має адресу 10.0.1.1 у VPN-сегменті 10.0.1.0/24. Після підключення клієнтів сервер забезпечує передачу трафіку між ними відповідно до налаштованих маршрутів.

Для правильної роботи OpenVPN-сервера на Ubuntu Server необхідно налаштувати кілька основних компонентів. По-перше, потрібно встановити пакет OpenVPN та інструменти для створення сертифікатів. По-друге, необхідно створити серверні та клієнтські сертифікати або ключі для автентифікації учасників VPN-з'єднання. По-третє, потрібно налаштувати конфігураційний файл сервера, у якому визначається VPN-підмережа, порт, протокол, параметри шифрування та маршрути. По-четверте, необхідно дозволити пересилання IP-пакетів між інтерфейсами системи.

Важливою функцією Ubuntu Server у даній схемі є підтримка маршрутизації. Оскільки VPN-сервер виступає центральним вузлом, через який проходить трафік між локальними мережами, він повинен знати маршрути до підмереж 192.168.5.0/24 і 192.168.6.0/24.

Окрему увагу потрібно приділити безпеці VPN-сервера. Оскільки сервер приймає зовнішні підключення, він повинен бути захищений від несанкціонованого доступу. Для цього слід використовувати надійні ключі та сертифікати, обмежити відкриті порти, налаштувати firewall, регулярно оновлювати систему та контролювати журнали підключень. Ubuntu Server надає всі необхідні засоби для виконання цих завдань.

До переваг Ubuntu Server для даного проєкту можна віднести:

4) стабільність роботи у серверному режимі;
5) безкоштовне використання;
6) підтримку OpenVPN;
7) зручне налаштування мережевих служб;
8) низькі вимоги до ресурсів;
9) можливість роботи у віртуальному середовищі Hyper-V;
10) наявність великої кількості документації та прикладів конфігурації.

2.5 Інсталювання RouterOS CHR у середовищі Hyper-V та підготовка віртуальних мережевих адаптерів

Для реалізації маршрутизаторів у межах даного проєкту використовується RouterOS CHR. CHR, або Cloud Hosted Router, – це віртуальна версія операційної системи RouterOS, призначена для запуску у середовищах віртуалізації. Такий підхід дозволяє змоделювати роботу маршрутизатора без використання фізичного обладнання, що є зручним для навчальної та лабораторної реалізації корпоративної мережі.

У межах проєкту RouterOS CHR використовується для створення віртуальних маршрутизаторів головного офісу та додаткового підрозділу. Кожен маршрутизатор виконує роль шлюзу для власної локальної мережі, забезпечує роботу DHCP, маршрутизацію та подальше підключення до віддаленого OpenVPN-сервера.

Першим етапом є завантаження образу RouterOS CHR з офіційного сайту MikroTik. Для цього необхідно перейти до розділу завантажень MikroTik, знайти версію Cloud Hosted Router та обрати образ, придатний для використання у середовищі віртуалізації. Для Hyper-V доцільно використовувати образ у форматі віртуального диска, який можна підключити до створеної віртуальної машини.

Після завантаження архів із образом необхідно розпакувати у підготовлений каталог на фізичному комп’ютері. У цьому каталозі буде зберігатися віртуальний диск RouterOS CHR, який надалі підключається до віртуальної машини Hyper-V як основний системний диск. Вигляд сторінки завантаження CHR знаходиться на рисунку 2.2.

На цьому етапі важливо обрати правильний тип образу, оскільки RouterOS CHR поширюється у кількох варіантах для різних платформ віртуалізації. Використання готового віртуального диска спрощує процес інсталяції, оскільки

немає потреби встановлювати операційну систему з ISO-образу. Достатньо створити віртуальну машину та підключити до неї завантажений диск.

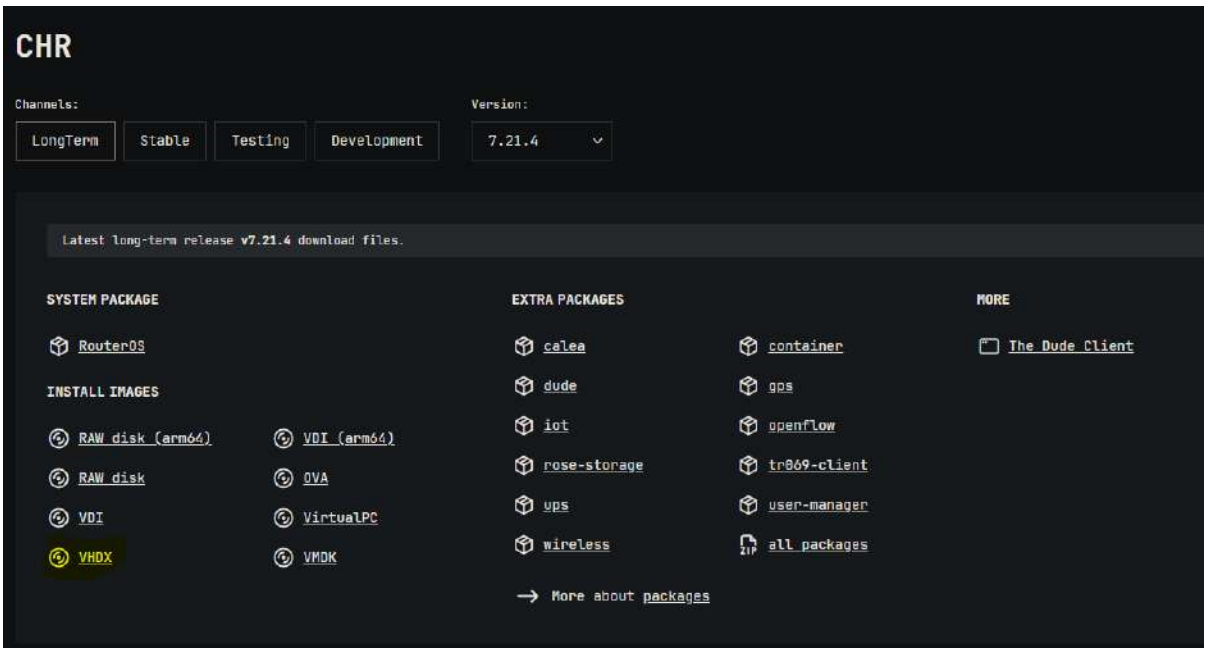


Рисунок 2.2 – Завантаження образу RouterOS CHR з офіційного сайту MikroTik

Після підготовки образу RouterOS CHR у Hyper-V створюється нова віртуальна машина. У даному проєкті перша віртуальна машина використовується як маршрутизатор головного офісу та має назву OFFICE_1_ROUTER. Друга віртуальна машина створюється аналогічно для додаткового підрозділу та може мати назву OFFICE_2_ROUTER.

Під час створення віртуальної машини необхідно вказати її назву, місце зберігання файлів, покоління віртуальної машини, обсяг оперативної пам’яті, параметри мережі та віртуальний жорсткий диск. Для RouterOS CHR достатньо мінімальних ресурсів, оскільки система не потребує значної кількості оперативної пам’яті або дискового простору. Приклад параметрів VM зображений на таблиці 2.2.

Під час створення машини важливо не створювати новий порожній диск, якщо вже використовується готовий образ RouterOS CHR. У такому випадку

потрібно обрати варіант підключення наявного віртуального диска. Це дозволяє одразу завантажити RouterOS після запуску віртуальної машини.

Таблиця 2.2 – Параметри віртуальних машин OFFICE_1/2_ROUTER

Параметр	Значення
Покоління віртуальної машини	Generation 2
Оперативна пам’ять	1024 МБ
Кількість процесорів	1–2 віртуальні процесори
Основний диск	Завантажений диск RouterOS CHR
Мережеві адаптери	Default Switch, OFFICE1_LAN1/ OFFICE1_LAN2

Після створення віртуальної машини необхідно перевірити її параметри. Особливу увагу потрібно приділити розділу Security, оскільки для деяких образів RouterOS CHR може знадобитися вимкнення Secure Boot. Якщо Secure Boot увімкнений і система не завантажується, його потрібно вимкнути в параметрах віртуальної машини. Список параметрів показаний на рисунку 2.3.

Після створення віртуальної машини необхідно підготувати віртуальні мережеві комутатори. У Hyper-V віртуальний комутатор виконує роль мережевого середовища, до якого підключаються віртуальні машини. За допомогою таких комутаторів можна моделювати окремі локальні мережі, ізольовані одна від одної.

Для створення віртуального комутатора необхідно відкрити Диспетчер віртуальних комутаторів Hyper-V. У цьому вікні доступні три типи комутаторів: зовнішній, внутрішній і приватний. Зовнішній комутатор використовується для доступу віртуальних машин до фізичної мережі. Внутрішній комутатор дозволяє

взаємодіяти віртуальним машинам із хостовою системою. Приватний комутатор забезпечує зв'язок лише між віртуальними машинами.

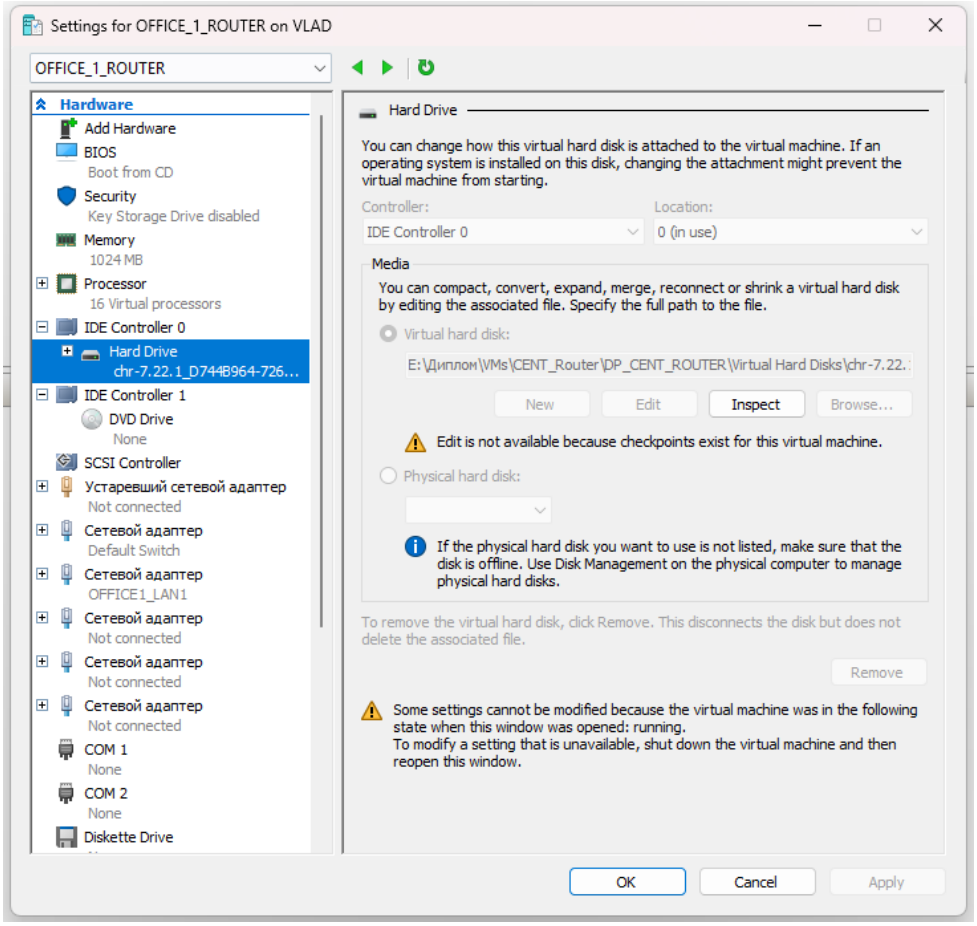


Рисунок 2.3 – Параметри віртуальної машини OFFICE_1_ROUTER

Після створення комутаторів у списку Hyper-V мають відображатися окремі мережеві сегменти: OFFICE1_LAN1, OFFICE2_LAN1 і стандартний Default Switch. Це означає, що середовище готове для підключення віртуальних машин до відповідних мереж.

Після створення віртуальних комутаторів необхідно перейти до налаштування мережевих адаптерів віртуального маршрутизатора OFFICE_1_ROUTER. Для роботи маршрутизатора потрібно щонайменше два мережеві інтерфейси. Перший інтерфейс використовується для підключення до

зовнішньої або службової мережі через Default Switch, а другий – для локальної мережі головного офісу через OFFICE1_LAN1 (рисунок 2.4).

У параметрах віртуальної машини відкривається розділ обладнання, де додаються мережеві адаптери. Перший адаптер прив'язується до Default Switch. Це підключення може використовуватися для доступу маршрутизатора до зовнішнього середовища або для подальшого встановлення VPN-з'єднання.

Другий мережевий адаптер прив'язується до комутатора OFFICE1_LAN1. Саме через цей інтерфейс маршрутизатор буде взаємодіяти з пристроями локальної мережі головного офісу. На цьому інтерфейсі надалі буде налаштована IP-адреса 192.168.5.1/24, яка виконуватиме роль шлюзу за замовчуванням для клієнтів головного офісу.

Таке підключення дозволяє маршрутизатору виконувати свою основну функцію – передавати трафік між локальною мережею головного офісу, глобальгої мережі та VPN-сегментом. Після запуску RouterOS CHR ці адаптери будуть відображені як окремі інтерфейси, наприклад ether1 і ether2.

Для другого маршрутизатора процес створення виконується аналогічно. Створюється віртуальна машина OFFICE_2_ROUTER, до якої підключаються два мережеві адаптери. Один адаптер використовується для підключення до зовнішнього або VPN-сегмента, а другий – для локальної мережі додаткового підрозділу.

Для локального інтерфейсу другого маршрутизатора використовується віртуальний комутатор OFFICE2_LAN1. На цьому інтерфейсі надалі буде налаштована IP-адреса 192.168.6.1/24, яка виконуватиме роль шлюзу для клієнтів додаткового підрозділу. Через цей шлюз клієнтські пристрої мережі 192.168.6.0/24 отримуватимуть доступ до головного офісу та VPN-сегмента.

Після завершення цього етапу в Hyper-V буде підготовлено два віртуальні маршрутизатори та два окремі локальні мережеві сегменти. Це створює основу для подальшого налаштування IP-адресації, DHCP.

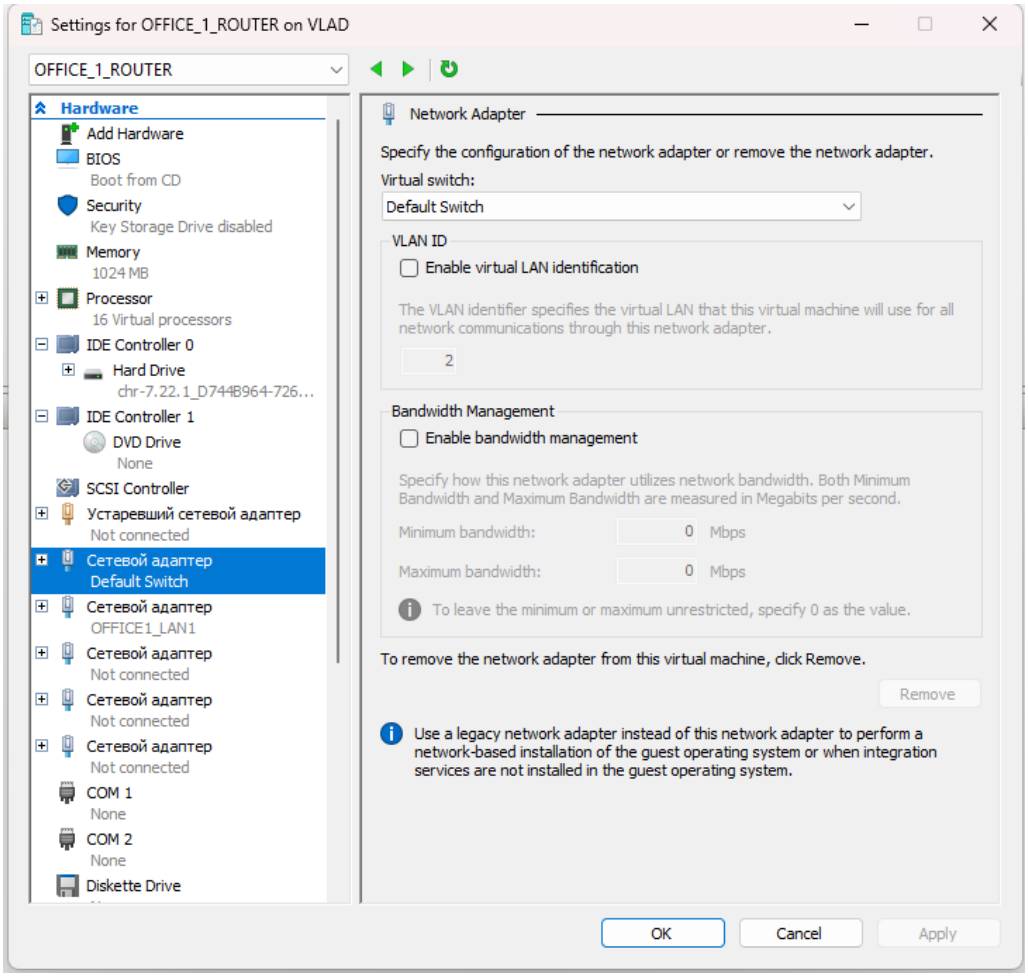


Рисунок 2.4 – Додавання мережевих адаптерів до віртуальної машини OFFICE_1_ROUTER

Згідно з рисунком 2.5, після створення віртуальних маршрутизаторів і окремих локальних мережевих сегментів необхідно підключити до них сервери, які виконують роль контролерів домену.

Сервер OFFICE_1_GDC підключається до локального мережевого сегмента головного офісу через віртуальний комутатор OFFICE1_LAN1. Саме цей сегмент відповідає мережі 192.168.5.0/24, у якій головний контролер домену має статичну IP-адресу 192.168.5.2.

Аналогічно виконується підключення сервера OFFICE_2_DC до локального сегмента додаткового підрозділу.

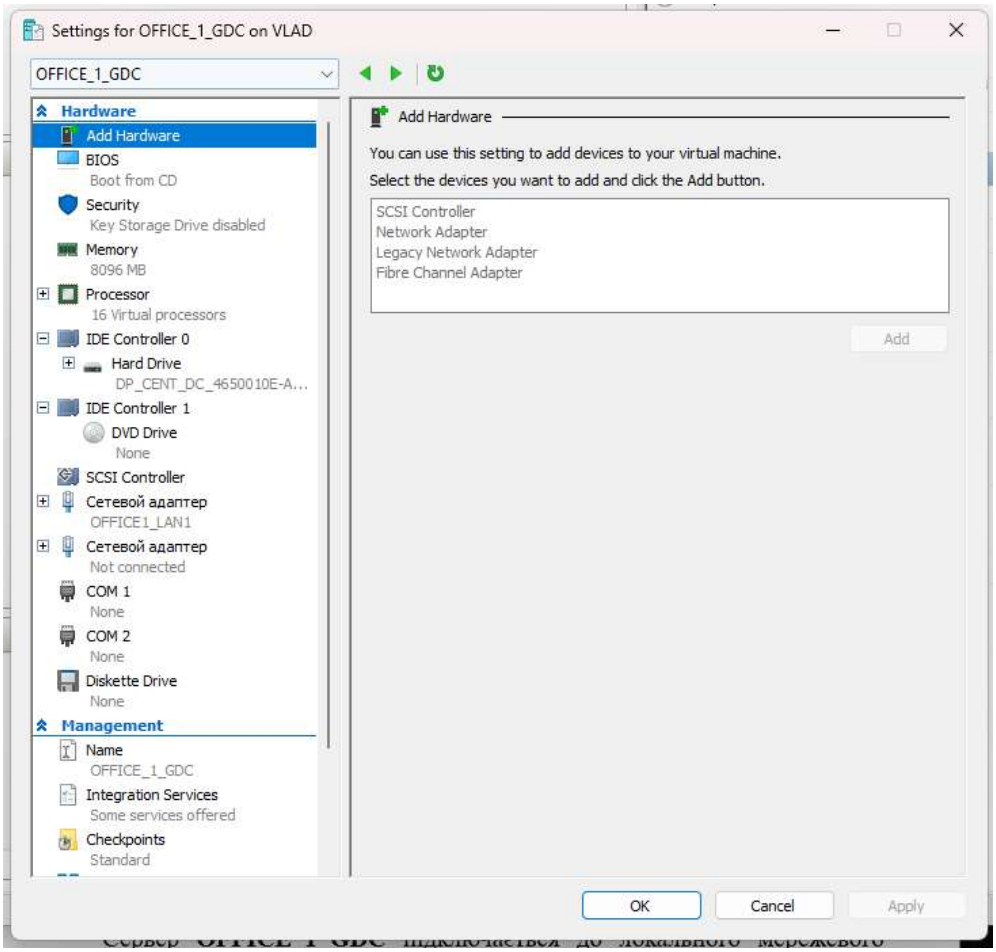


Рисунок 2.5 – Підключення сервера OFFICE_1_GDC до віртуального комутатора OFFICE1_LAN1

2.6 Підготовка VPN-сервера на базі Ubuntu Server

Після підготовки віртуальних маршрутизаторів і локальних мережевих сегментів наступним етапом є створення та налаштування віртуальної машини для VPN-сервера. У даному проєкті VPN-сервер виконує роль центрального вузла, до якого надалі будуть підключатися маршрутизатори головного офісу та додаткового підрозділу. Саме через цей сервер буде організовано захищений обмін трафіком між мережами 192.168.5.0/24 і 192.168.6.0/24.

Для реалізації VPN-сервера використовується операційна система Ubuntu Server, яка встановлюється у віртуальну машину Hyper-V. У межах даного етапу виконується завантаження ISO-образу Ubuntu Server, підключення образу до

заздалегідь створеної віртуальної машини, встановлення операційної системи, базове налаштування сервера та перевірка доступу до нього через SSH.

Першим етапом підготовки VPN-сервера є завантаження ISO-образу Ubuntu Server з офіційного сайту Ubuntu. Для цього необхідно перейти до розділу завантажень Ubuntu Server та обрати актуальну LTS-версію операційної системи. Використання LTS-версії є доцільним, оскільки вона має тривалий термін підтримки, отримує оновлення безпеки та підходить для серверного використання.

Після завантаження ISO-образ зберігається на фізичному комп'ютері, де встановлено Hyper-V. Надалі цей образ буде використано як інсталяційний носій для встановлення операційної системи у віртуальну машину. Сторінка завантаження образу зображена на рисунку 2.6.

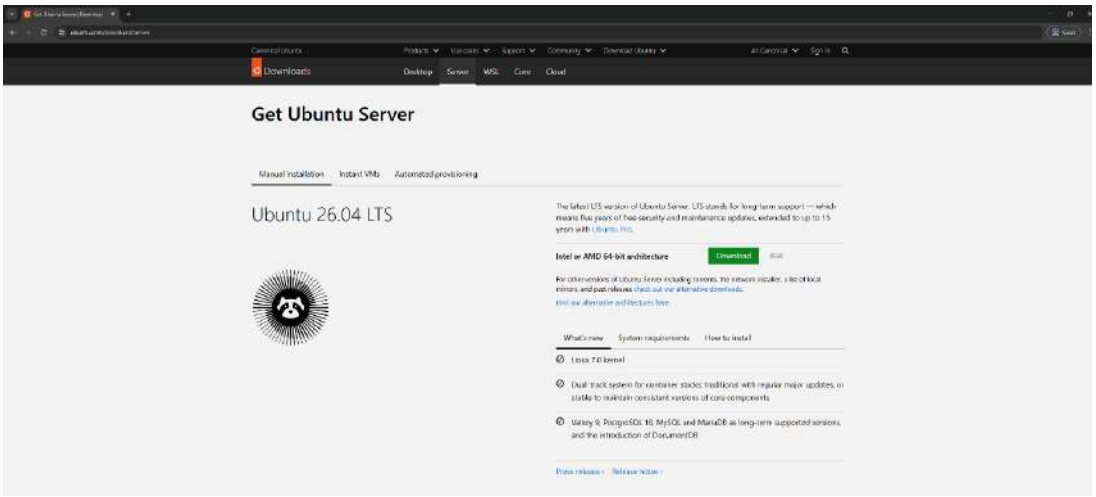


Рисунок 2.6 – Завантаження образу Ubuntu Server з офіційного сайту

Для встановлення Ubuntu Server у Hyper-V попередньо створюється віртуальна машина з назвою OpenVPN. Вона буде використовуватися як сервер для подальшого розгортання OpenVPN. Під час створення віртуальної машини задаються базові параметри: обсяг оперативної пам'яті, кількість віртуальних процесорів, розмір віртуального диска та мережевий адаптер. Параметри показані на таблиці 2.3.

Таблиця 2.3 – Список параметрів VM OpenVPN Server

Параметр	Значення
Назва віртуальної машини	OpenVPN
Операційна система	Ubuntu Server
Оперативна пам’ять	4096 МБ
Кількість процесорів	2–4 віртуальні процесори
Жорсткий диск	Віртуальний диск Hyper-V
Мережевий адаптер	Default Switch

У наданому прикладі віртуальна машина OpenVPN має виділену оперативну пам’ять 4096 МБ та підключений мережевий адаптер до Default Switch. Таке підключення дозволяє серверу отримати мережеву доступність у віртуальному середовищі та надалі використовуватися для встановлення OpenVPN, підключення клієнтів і налаштування маршрутизації.

На цьому етапі також перевіряється розділ Security. Якщо для встановлення або запуску Ubuntu Server виникають проблеми, можна вимкнути параметр Secure Boot.

Після створення віртуальної машини необхідно підключити завантажений ISO-образ Ubuntu Server як інсталяційний носій. Для цього у параметрах віртуальної машини відкривається розділ SCSI Controller або DVD Drive, після чого вибирається ISO-файл, завантажений з офіційного сайту Ubuntu.

Після запуску віртуальної машини з підключеним ISO-образом відкривається інсталятор Ubuntu Server рис. 2.7. На початку встановлення обирається мова інтерфейсу, розкладка клавіатури та базові параметри системи.

Далі налаштовується мережевий інтерфейс, диск для встановлення та обліковий запис адміністратора.

Під час встановлення важливо задати зрозуміле ім’я сервера, наприклад openvpn-server або OpenVPN. Це спрощує подальше адміністрування та дозволяє швидше ідентифікувати сервер у мережі.

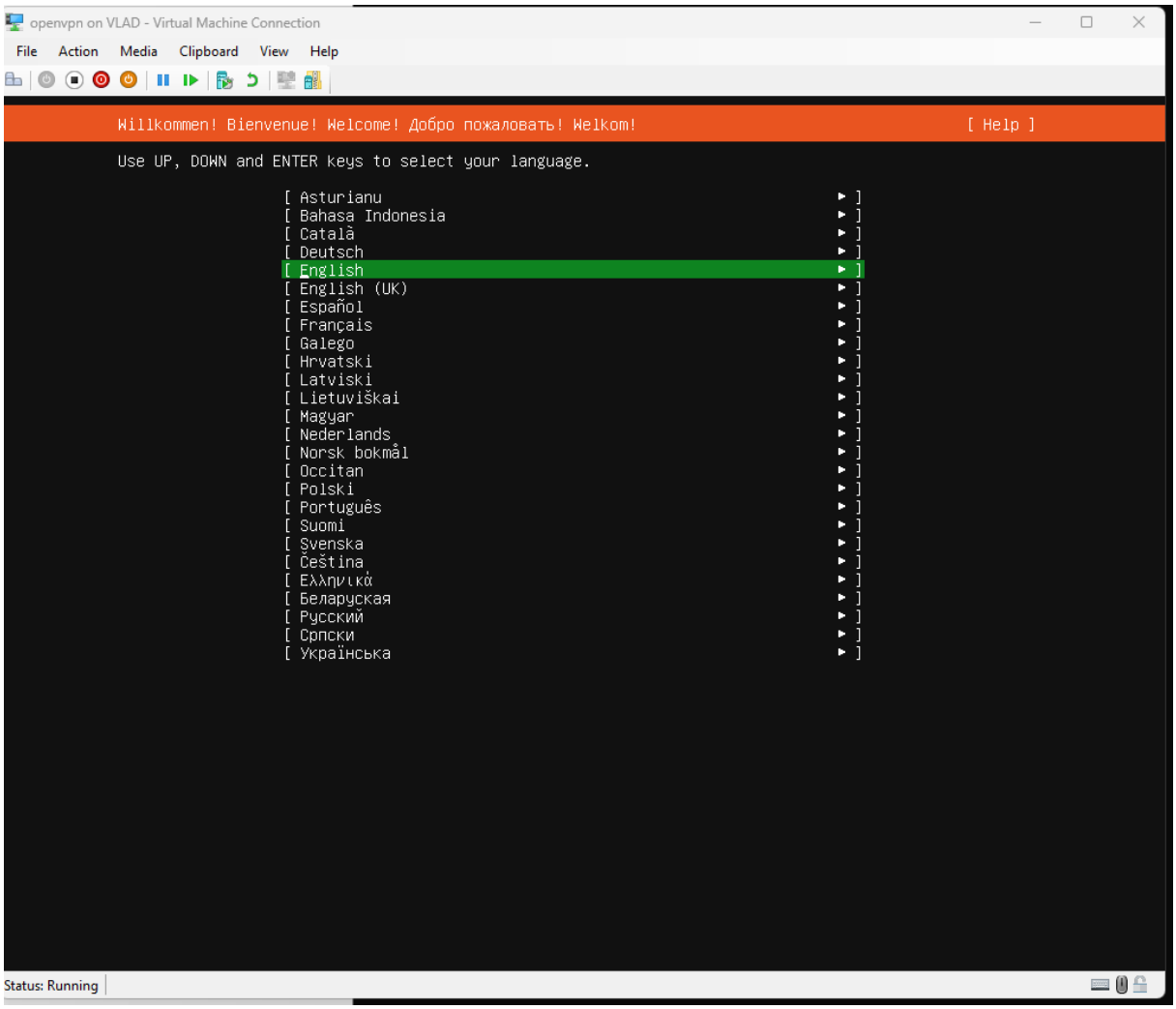


Рисунок 2.7 – Початок встановлення Ubuntu Server

На етапі налаштування диска можна обрати автоматичну розмітку, оскільки в межах даного проєкту сервер використовується переважно для роботи VPN-служби. Налаштування розмітки зображені на рис. 2.8.

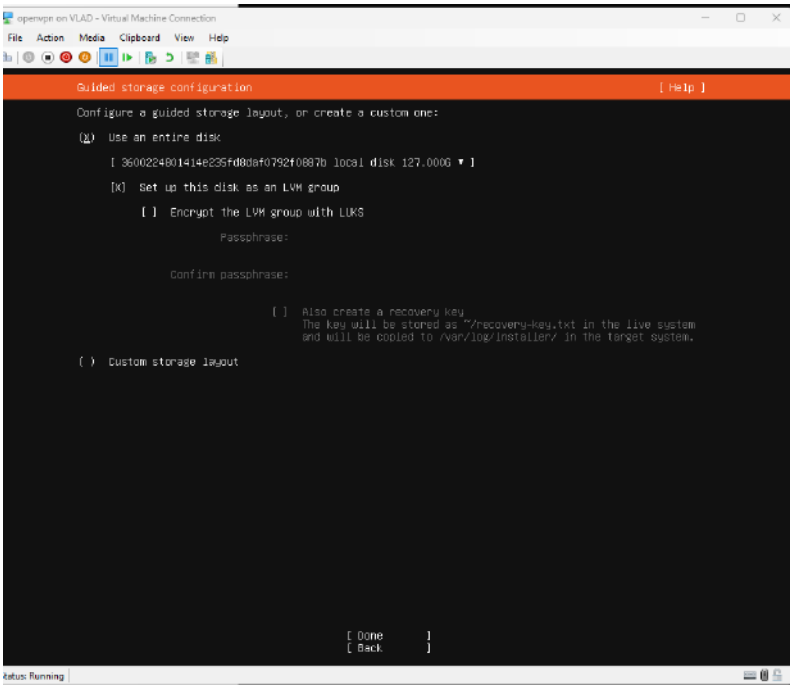


Рисунок 2.8 – Налаштування диска під час встановлення Ubuntu Server

Під час створення облікового запису адміністратора необхідно задати ім’я користувача та надійний пароль. Цей користувач надалі буде використовуватися для входу в систему, виконання команд з правами адміністратора через sudo, встановлення пакетів і налаштування VPN-сервера, предстaлено на рисунку 2.9.

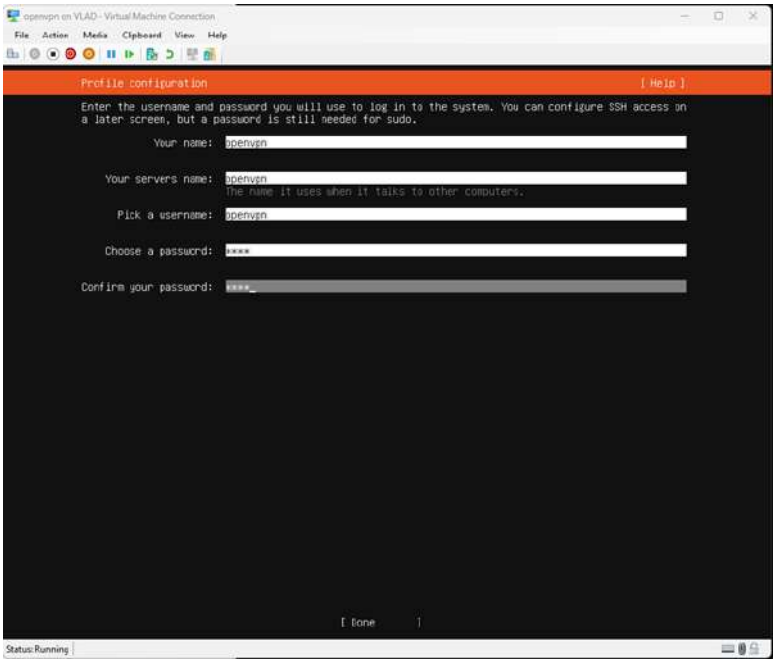


Рисунок 2.9 – Створення користувача адміністратора Ubuntu Server

Після завершення інсталяції система пропонує перезавантажити віртуальну машину. Перед перезавантаженням необхідно відключити ISO-образ від DVD-приводу, щоб сервер завантажився вже з установленої операційної системи, а не з інсталяційного носія.

Після перезавантаження віртуальної машини запускається встановлена операційна система Ubuntu Server. Користувач входить у систему за логіном і паролем, які були створені під час інсталяції. Після входу до системи можна виконати базову перевірку роботи сервера.

Перевірка ip-адресу сервера здійснюється за допомогою команди:

```
Ip a
```

Ця команда показує список мережевих інтерфейсів і призначені їм IP-адреси. Якщо сервер підключений до Default Switch, він може отримати адресу автоматично через DHCP(рисунок 2.10).

Рисунок 2.10 – Перевірка IP-адреси Ubuntu Server після встановлення

IP-адрес: 172.21.93.24

Після встановлення Ubuntu Server і перевірки мережевих параметрів виконується підключення до сервера через SSH. У даному проєкті для цього використовується Termux. Termux дозволяє працювати з Linux-подібним командним середовищем і виконувати SSH-підключення до серверів (рисунок 2.11).

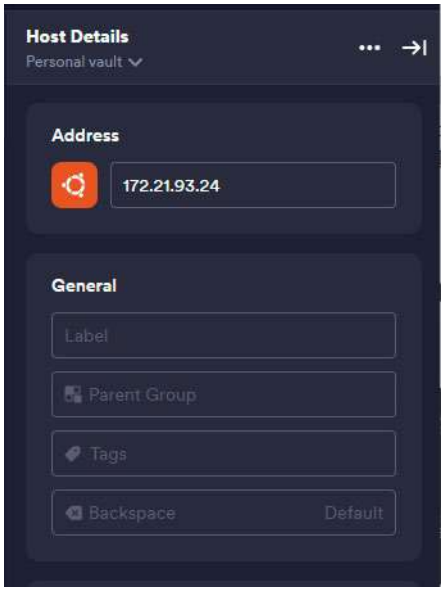


Рисунок 2.11 – Підключення до Ubuntu Server через SSH у Termux

Після першого підключення SSH може вивести повідомлення про додавання відбитка ключа сервера до списку відомих хостів. Необхідно підтвердити підключення, після чого ввести пароль користувача. Якщо дані введені правильно, відкривається командний рядок Ubuntu Server.

SSH-підключення є зручним способом адміністрування VPN-сервера, оскільки дозволяє виконувати всі подальші налаштування віддалено. Через SSH можна встановлювати пакети, редагувати конфігураційні файли, перевіряти журнали, налаштовувати OpenVPN, firewall і маршрутизацію.

2.7 Висновки до другого розділу

У другому розділі було розглянуто процес проєктування та підготовки середовища для реалізації внутрішньої корпоративної мережі компанії із захищеним доступом на основі персонального VPN-сервера. Основну увагу було приділено побудові базової карти мережі, вибору апаратних і програмних засобів, підготовці віртуального середовища Hyper-V, встановленню RouterOS CHR та підготовці VPN-сервера на базі Ubuntu Server.

На початковому етапі було сформовано топографічну карту мережі, яка відображає логічну структуру корпоративної інфраструктури. Мережа складається з головного офісу, додаткового підрозділу та віддаленого VPN-сервера. Для головного офісу використовується підмережа 192.168.5.0/24, для додаткового підрозділу – 192.168.6.0/24, а для VPN-сегмента – 10.0.1.0/24. Такий розподіл адресного простору дозволяє чітко відокремити локальні мережі та забезпечити подальшу маршрутизацію між ними через захищений VPN-канал.

Було визначено роль основних серверів у мережі. У головному офісі розміщено сервер OFFICE_1_GDC з адресою 192.168.5.2, який виконує роль головного контролера домену та DNS-сервера. У додатковому підрозділі підготовлено сервер OFFICE_2_DC з адресою 192.168.6.2, який надалі буде використовуватися як додатковий контролер домену. Для забезпечення коректної роботи доменної інфраструктури між цими серверами необхідно організувати стабільний обмін службовим трафіком через VPN-з’єднання.

Для побудови лабораторної інфраструктури було обрано гіпервізор Hyper-V. Його використання дозволило створити окремі віртуальні машини, змоделювати локальні мережеві сегменти, підключити віртуальні маршрутизатори та сервери до відповідних комутаторів. У середовищі Hyper-V було підготовлено віртуальні комутатори OFFICE1_LAN1 і OFFICE2_LAN1, які відповідають локальним мережам головного офісу та додаткового підрозділу.

Для моделювання маршрутизаторів було використано RouterOS CHR, що є віртуальною версією RouterOS. Було описано процес завантаження образу RouterOS CHR з офіційного сайту, створення віртуальних машин для маршрутизаторів, підключення віртуальних дисків і налаштування мережевих адаптерів. Для маршрутизатора головного офісу один адаптер було підключено до Default Switch, а другий – до OFFICE1_LAN1. Аналогічний підхід використовується для маршрутизатора додаткового підрозділу з підключенням до OFFICE2_LAN1.

Також було виконано підключення серверів контролерів домену до відповідних локальних мережевих сегментів. Сервер OFFICE_1_GDC було підключено до OFFICE1_LAN1, а сервер OFFICE_2_DC – до OFFICE2_LAN1. Це дозволило розмістити кожен сервер у відповідному мережевому сегменті та підготувати основу для подальшої взаємодії між ними через VPN.

3 НАЛАШТУВАННЯ ВНУТРІШНЬОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАХИЩЕНИМ ДОСТУПОМ

3.1 Налаштування мережі головного офісу Office_1

Першим етапом практичного налаштування є підготовка локальної мережі головного офісу Office_1. Цей сегмент є основним у проєкті, оскільки в ньому розміщено головний контролер домену OFFICE_1_GDC, який виконує роль DNS-сервера та центрального вузла доменної інфраструктури.

Мережа головного офісу використовує адресний простір 192.168.5.0/24. Основним шлюзом для клієнтських пристроїв є маршрутизатор Office_1_Router з адресою 192.168.5.1. Сервер головного контролера домену має адресу 192.168.5.2. Інші клієнтські пристрої отримують IP-адреси автоматично за допомогою DHCP. Параметри мережі відображені в таблиці 3.1.

Таблиця 3.1 – Основні параметри мережі Office_1

Параметр	Значення
Назва сегмента	Office_1
Адреса мережі	192.168.5.0/24
Шлюз за замовчуванням	192.168.5.1
Головний контролер домену	192.168.5.2
DNS-сервер	192.168.5.2
Домен	corp.diplom.com
Спосіб видачі адрес клієнтам	DHCP

На початковому етапі було перевірено список мережевих інтерфейсів маршрутизатора. У вікні Interfaces відображаються фізичні та логічні інтерфейси, зокрема Ethernet-інтерфейси, bridge-інтерфейс, WAN-інтерфейс і loopback-інтерфейс. Наявність цих інтерфейсів підтверджує, що віртуальна машина маршрутизатора коректно отримала мережеві адаптери від Hyper-V (рисунок 3.1).

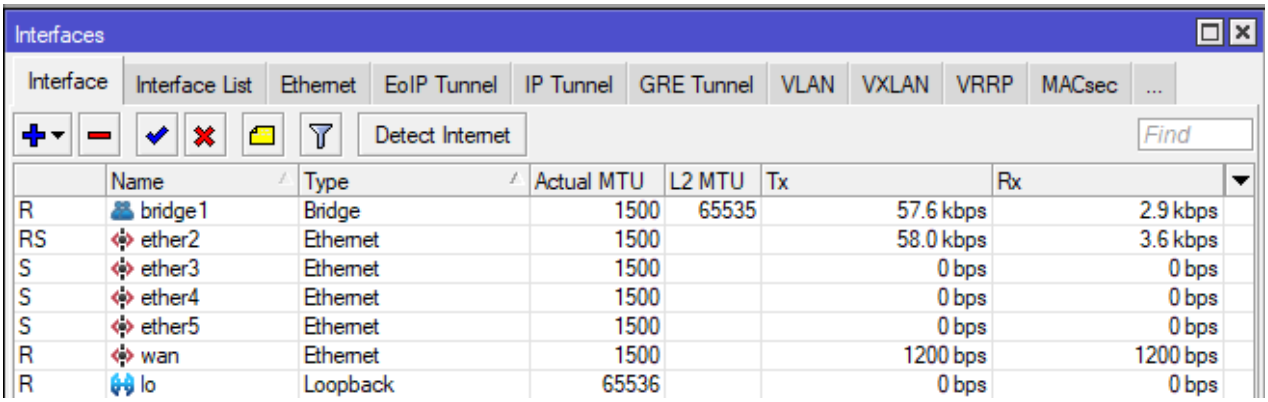


Рисунок 3.1 – Список інтерфейсів маршрутизатора Office_1

Для зручності адміністрування інтерфейси було розподілено за логічними списками. Локальний інтерфейс bridge1 належить до списку LAN, а зовнішній інтерфейс wan – до списку WAN (рисунок 3.2).

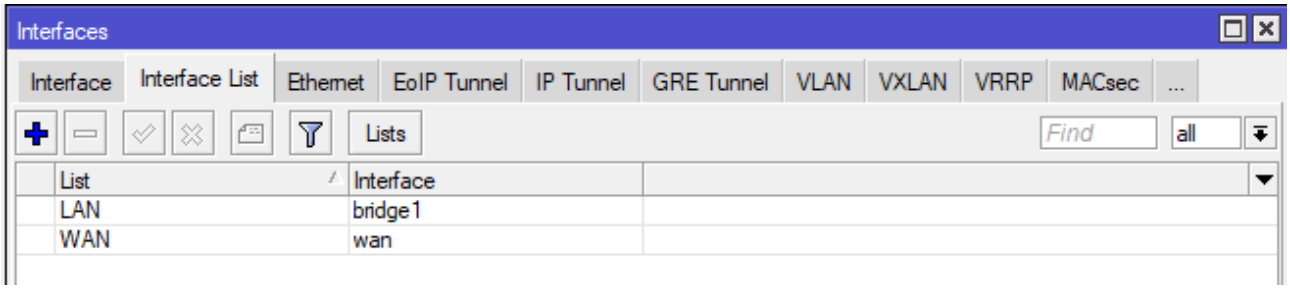


Рисунок 3.2 – Розподіл інтерфейсів за списками LAN і WAN

Після перевірки інтерфейсів було налаштовано IP-адреси. Для локальної мережі головного офісу на інтерфейсі bridge1 встановлено адресу 192.168.5.1/24

(рисунок 3.3). Саме ця адреса використовується клієнтськими пристроями як шлюз за замовчуванням.

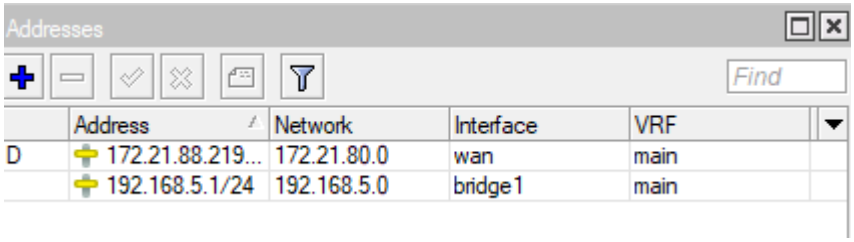


Рисунок 3.3 – Налаштування IP-адрес маршрутизатора Office_1

Наступним етапом було налаштування DHCP-сервера. DHCP використовується для автоматичної видачі IP-адрес, маски підмережі, шлюзу та DNS-сервера клієнтським пристроям. Це спрощує адміністрування мережі, оскільки немає необхідності вручну задавати параметри на кожному комп'ютері.

У RouterOS було створено DHCP-сервер dhcp1, який працює на інтерфейсі bridge1. Саме цей інтерфейс відповідає локальній мережі головного офісу. Для DHCP-сервера вказано відповідний пул адрес, з якого клієнтам видаються вільні IP-адреси. Час оренди адреси встановлено 30 хвилин (рисунок 3.4).

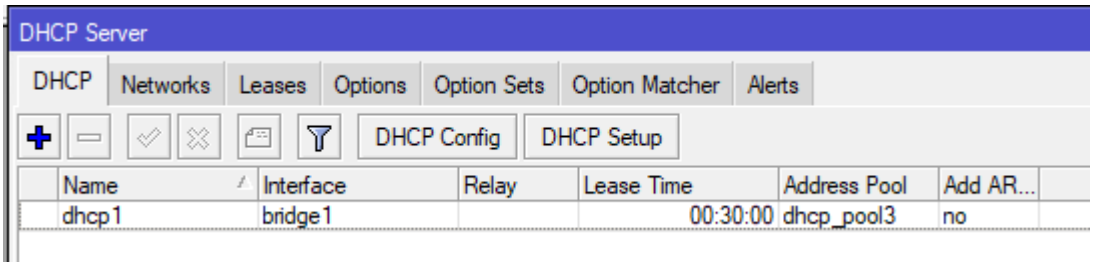


Рисунок 3.4 – DHCP-сервер dhcp1 для мережі Office_1

Окремо було налаштовано параметри DHCP-мережі. Для мережі 192.168.5.0/24 як шлюз вказано адресу 192.168.5.1, а як DNS-сервер – адресу 192.168.5.2. Також задано доменне ім'я corp.diplom.com. Це важливо для коректної роботи доменної інфраструктури, оскільки клієнти повинні звертатися саме до DNS-сервера контролера домену. Зображено на рисунку 3.5.

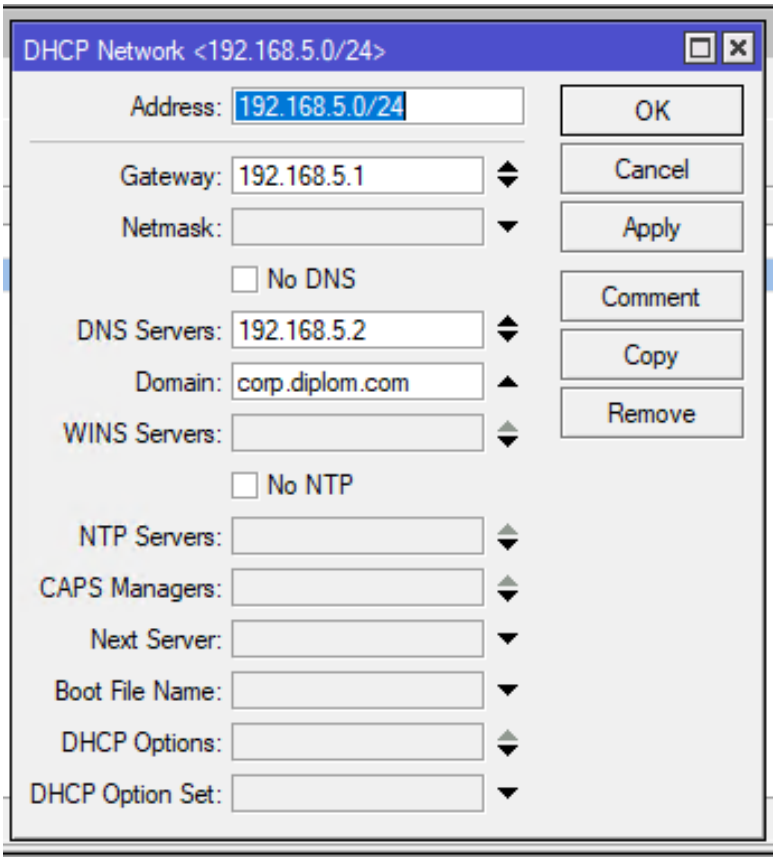


Рисунок 3.5 – Параметри DHCP-мережі 192.168.5.0/24

Після налаштування DHCP було перевірено список виданих адрес у вкладці Leases. У цьому списку відображаються пристрої, які отримали IP-адресу від DHCP-сервера. Наявність записів у цьому розділі підтверджує, що DHCP-сервер працює коректно та клієнтські пристрої можуть отримувати мережеві параметри автоматично.

Після налаштування локальної адресації та DHCP було створено правило NAT для виходу локальної мережі через WAN-інтерфейс. Для цього використовується правило типу masquerade у ланцюгу srcnat. Воно застосовується до трафіку, який виходить через інтерфейс зі списку WAN. Завдяки цьому клієнти локальної мережі можуть використовувати зовнішнє підключення маршрутизатора (рисунок 3.6).

Таким чином, локальна мережа головного офісу Office_1 була підготовлена до подальшої інтеграції з іншими сегментами корпоративної

інфраструктури. На цьому етапі вона ще не підключена до OpenVPN-сервера, однак має повністю налаштовану базову мережеву конфігурацію: власний адресний простір, шлюз, DHCP-сервер, DNS-напрямок на контролер домену та NAT для зовнішнього доступу. Це створює основу для наступних етапів, де буде виконано налаштування мережі додаткового підрозділу та подальше підключення обох мереж до захищеного VPN-сегмента.

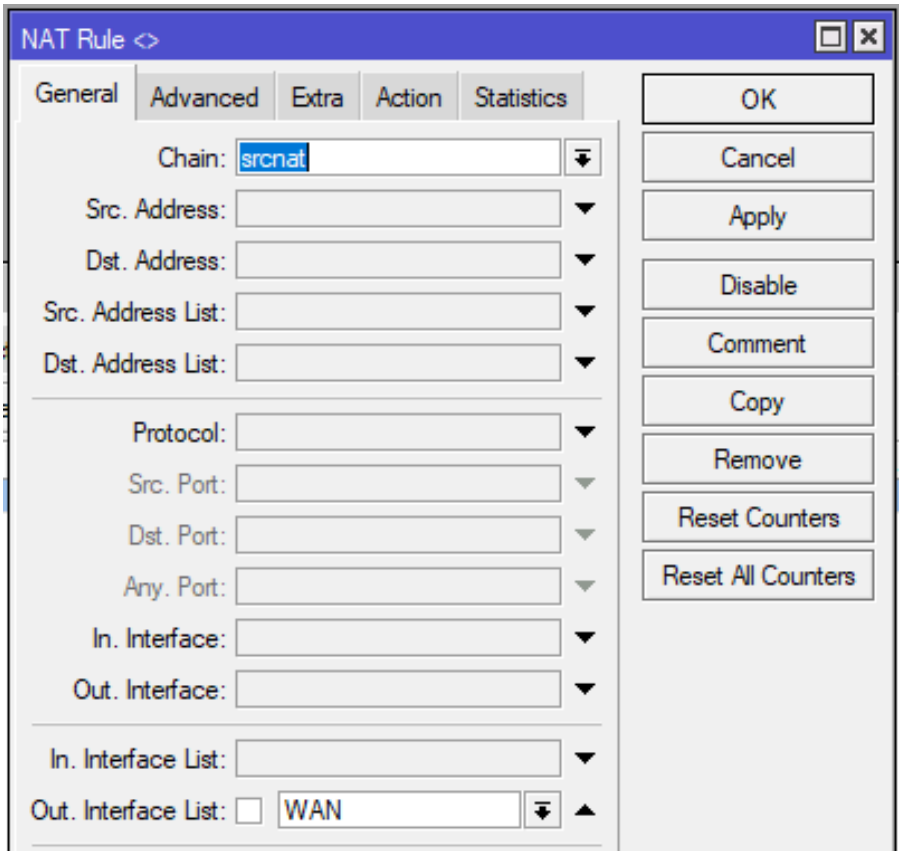


Рисунок 3.6 – NAT-правило masquerade для WAN-інтерфейсу

3.2 Налаштування мережі додаткового підрозділу Office_2.

Наступним етапом практичного налаштування є підготовка локальної мережі додаткового підрозділу Office_2. Цей сегмент є віддаленою частиною корпоративної інфраструктури, яка надалі буде об’єднана з головним офісом через захищене VPN-з’єднання. Параметри мережі відображені в таблиці 3.3.

Таблиця 3.3 – Основні параметри мережі Office_2

Параметр	Значення
Назва сегмента	Office_2
Адреса мережі	192.168.5.0/24
Шлюз за замовчуванням	192.168.6.1
Головний контролер домену	192.168.6.2
DNS-сервер	-
Спосіб видачі адрес клієнтам	DHCP

У вікні Interfaces відображаються Ethernet-інтерфейси, bridge-інтерфейс, WAN-інтерфейс та інші службові інтерфейси RouterOS. Це підтверджує, що віртуальний маршрутизатор Office_2_Router коректно отримав мережеві адаптери від середовища Hyper-V(рисунок 3.7).

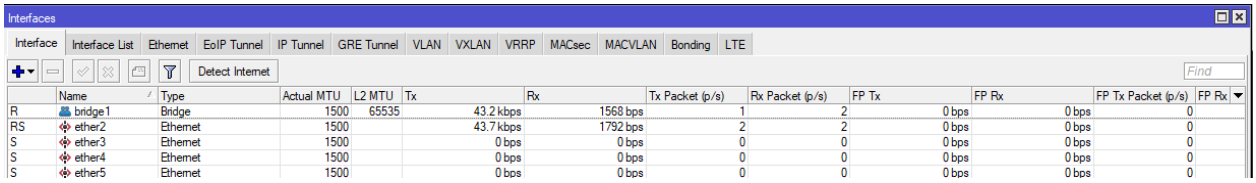


Рисунок 3.7 – Список інтерфейсів маршрутизатора Office_2

Як і в мережі головного офісу, для зручності адміністрування інтерфейси було розподілено за логічними списками. Локальний інтерфейс bridge1 належить до списку LAN, а зовнішній інтерфейс wan – до списку WAN. Такий поділ спрощує подальше налаштування правил NAT, firewall та інших параметрів обробки трафіку(рисунок 3.8).

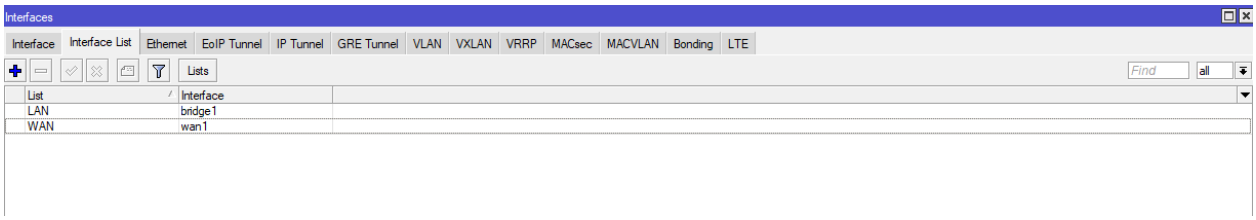


Рисунок 3.8 – Розподіл інтерфейсів Office_2 за списками LAN і WAN

Після перевірки інтерфейсів було налаштовано IP-адреси. Для локальної мережі додаткового підрозділу на інтерфейсі bridge1 встановлено адресу 192.168.6.1/24(рисунок 3.9).

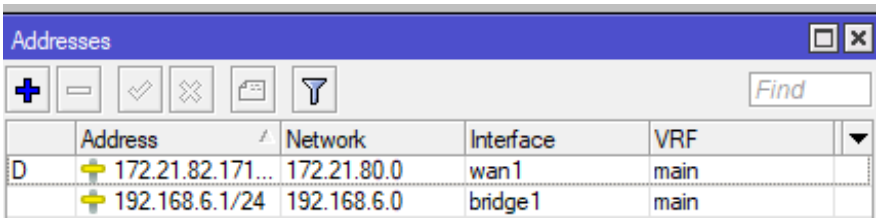


Рисунок 3.9 – Налаштування IP-адрес маршрутизатора Office_2

192.168.6.1 є основною адресою локального шлюзу для мережі Office_2. Через неї клієнти додаткового підрозділу передають трафік за межі власної підмережі. Сервер OFFICE_2_DC має адресу 192.168.6.2, тому на цьому етапі він може використовуватися як локальний DNS-сервер для клієнтів додаткового підрозділу. Після підключення цього сервера до домену та налаштування реплікації він виконуватиме роль додаткового контролера домену.

Наступним етапом було налаштування DHCP-сервера для мережі Office_2. DHCP потрібен для автоматичної видачі IP-адрес, маски підмережі, шлюзу та DNS-сервера клієнтським пристроям. Це дозволяє уникнути ручного налаштування кожної робочої станції та спрощує адміністрування мережі додаткового підрозділу.

У RouterOS було створено DHCP-сервер dhcp1, який працює на інтерфейсі bridge1. Цей інтерфейс відповідає локальному сегменту 192.168.6.0/24. Для

DHCP-сервера вказано пул адрес, з якого клієнтським пристроям видаються вільні IP-адреси. Час оренди адреси встановлено 30 хвилин, що є зручним для тестового середовища та дозволяє швидко перевіряти зміни в конфігурації. Зображено на рисунку 3.10.

Таким чином, локальна мережа додаткового і основного підрозділу Таким чином, локальні мережі головного офісу Office_1 та додаткового підрозділу Office_2 були повністю підготовлені до подальшої інтеграції в єдину корпоративну інфраструктуру. На цьому етапі обидва сегменти ще не підключені до OpenVPN-сервера, однак мають налаштовану базову мережеву конфігурацію: власні адресні простори, шлюзи, DHCP-сервери, DNS-параметри та NAT для зовнішнього доступу.

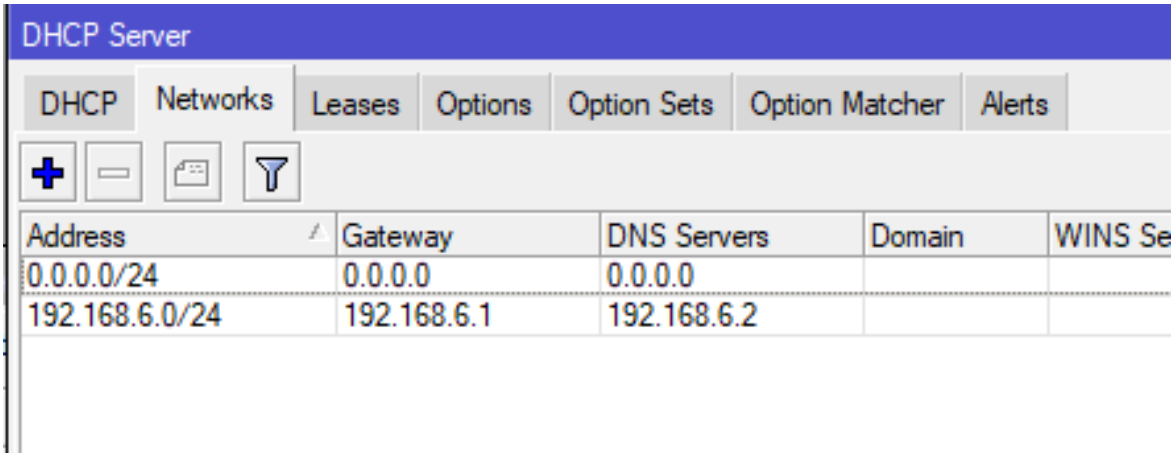


Рисунок 3.10 – DHCP-сервер dhcp1 для мережі Office_2

Мережа Office_1 використовує адресний простір 192.168.5.0/24, шлюз 192.168.5.1 та DNS-сервер 192.168.5.2, яким є головний контролер домену OFFICE_1_GDC. Мережа Office_2 використовує адресний простір 192.168.6.0/24, шлюз 192.168.6.1 та DNS-сервер 192.168.6.2, яким є сервер OFFICE_2_DC, підготовлений для подальшого використання як додатковий контролер домену.

Після завершення базового налаштування обидві локальні мережі готові до наступного етапу – підключення до VPN-сегмента та організації захищеного зв’язку між головним офісом і додатковим підрозділом.

3.3 Випуск сертифікатів і підготовка клієнтських конфігурацій OpenVPN

Після базового налаштування локальних мереж Office_1 та Office_2 необхідно підготувати криптографічні файли для роботи OpenVPN. Для встановлення захищеного VPN-з’єднання використовуються сертифікати, приватні ключі, сертифікат центру сертифікації, ключ Diffie-Hellman та TLS-auth ключ. У даному проєкті випуск сертифікатів виконується в середовищі Windows на головному контролері домену, де встановлено EasyRSA.

Сам VPN-сервер на Ubuntu Server не використовується для генерації сертифікатів. Він отримує вже готові файли ключів і сертифікатів через SSH. Такий підхід дозволяє розділити функції VPN-сервера та центру випуску сертифікатів. У разі компрометації VPN-сервера інфраструктура випуску сертифікатів не зберігається безпосередньо на ньому, що підвищує загальний рівень безпеки.

Перед випуском сертифікатів у EasyRSA виконується налаштування файлу vars (рисунок 3.11). У цьому файлі задаються основні параметри PKI-інфраструктури, зокрема строк дії кореневого сертифіката CA, серверних і клієнтських сертифікатів, а також списку відкликаних сертифікатів CRL.

```
set_var EASYRSA_CA_EXPIRE 3650     # строк дії кореневого сертифіката CA
set_var EASYRSA_CERT_EXPIRE 3650       # строк дії серверних і клієнтських сертифікатів
set_var EASYRSA_CRL_DAYS 3650        # строк дії списку відкликаних сертифікатів CRL
set_var EASYRSA_OPENSSL      "/easy-rsa/openvpn/bin/openssl.exe"
```

Після налаштування файлу vars виконується ініціалізація PKI-інфраструктури. Для цього запускається EasyRSA та виконується команда:

```
./easyrsa init-pki
```

```
#set_var EASYRSA_ALGO       rsa

# Define the named curve, used in ec & ed modes:
#
#set_var EASYRSA_CURVE      secp384r1

# In how many days should the root CA key expire?
#
set_var EASYRSA_CA_EXPIRE   3650

# In how many days should certificates expire?
#
set_var EASYRSA_CERT_EXPIRE 3650

# How many days until the next CRL publish date?  Note that the CRL can still
# be parsed after this timeframe passes. It is only used for an expected next
# publication date.
#
set_var EASYRSA_CRL_DAYS    3650
```

Рисунок 3.11 – Налаштування строку дії сертифікатів у файлі vars

У результаті створюється структура каталогів PKI, де надалі зберігаються запити, приватні ключі, сертифікати та службові файли EasyRSA. У використаному порядку налаштування після виконання init-pki створюється каталог pki, який використовується для подальшої роботи з сертифікатами.

Далі створюється кореневий центр сертифікації:

```
./easyrsa build-ca
```

Після виконання цієї команди формується сертифікат центру сертифікації ca.crt та відповідний приватний ключ. Сертифікат ca.crt надалі використовується як на OpenVPN-сервері, так і на клієнтах для перевірки довіри до виданих сертифікатів. Приклад налаштувань поданий на рисунку 3.12.

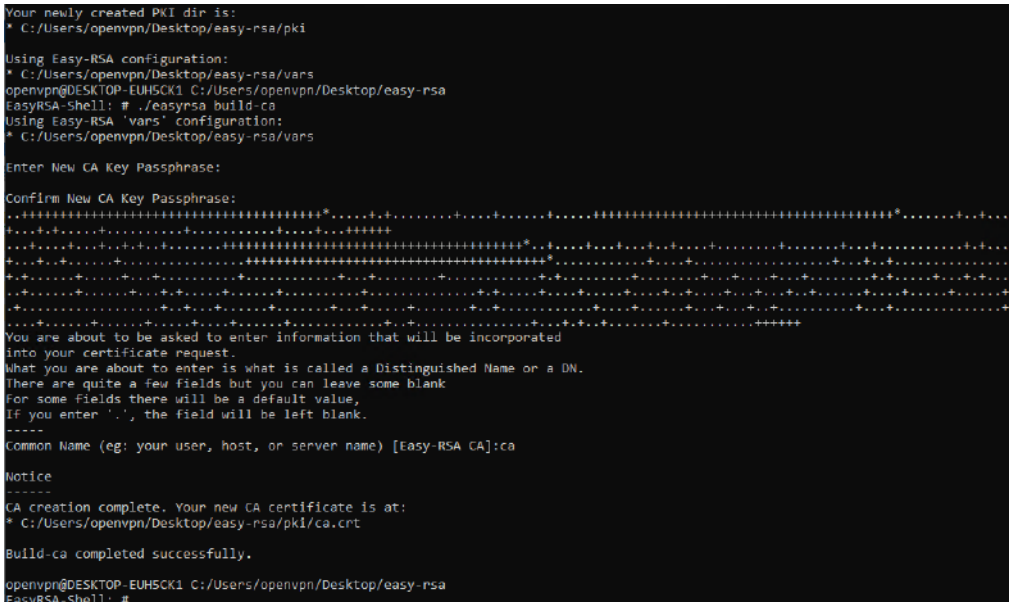


Рисунок 3.12 – Ініціалізація PKI та створення кореневого CA

Після створення кореневого CA генерується запит і приватний ключ для OpenVPN-сервера:

```
./easyrsa gen-req server nopass
```

Параметр nopass означає, що приватний ключ сервера створюється без пароля.

Після створення запиту сертифікат сервера підписується центром сертифікації:

```
./easyrsa sign-req server server
```

У результаті створюється серверний сертифікат server.crt, який використовується OpenVPN Server для підтвердження своєї автентичності перед клієнтами.

Окремо генеруються параметри Diffie-Hellman:

```
./easyrsa gen-dh
```

Також створюється TLS-auth ключ:

```
openvpn --genkey secret ta.key
```

Ключ ta.key використовується як додатковий механізм захисту TLS-з’єднання.

Місце розташування файлів:

```
.key – \easy-rsa\pki\private
.crt – \easy-rsa\pki\issued
ca.crt – \easy-rsa\pki
```

Випуск клієнтських сертифікатів

Для кожного VPN-клієнта створюється окремий сертифікат. У межах даної роботи клієнтами виступають маршрутизатори головного офісу та додаткового підрозділу, тому створюються окремі клієнтські сертифікати office_1 та office_2.

Для створення запиту сертифіката клієнта office_1 виконується команда:

```
./easyrsa gen-req office_1 nopass
```

Після цього запит підписується як клієнтський:

```
./easyrsa sign-req client office_1
```

Аналогічно створюється сертифікат для office_2.

У результаті для кожного клієнта формується окремий сертифікат і приватний ключ. Це дозволяє ідентифікувати кожний маршрутизатор окремо та надалі задавати для нього індивідуальні параметри, зокрема статичну VPN-адресу.

Серверні файли передаються на VPN-сервер через SSH до відповідного каталогу OpenVPN. Клієнтські сертифікати та ключі використовуються для створення конфігураційних файлів, які надалі імпортуються на маршрутизатори.

Після випуску сертифікатів створюються клієнтські конфігураційні файли для маршрутизаторів Office_1_Router та Office_2_Router. Кожен маршрутизатор отримує власний файл формату .ovpn, який містить параметри підключення до VPN-сервера.

Основна структура клієнтського конфігураційного файлу представлена в додатку Б. Аналогічно має бути оформлений файл office_2.ovpn.

3.4 Налаштування OpenVPN Server

Після завершення базового налаштування локальних мереж Office_1 та Office_2 наступним етапом є підготовка центрального OpenVPN Server. У

даному проєкті він використовується як проміжний захищений вузол, через який надалі буде організовано обмін трафіком між головним офісом, додатковим підрозділом і VPN-сегментом. OpenVPN Server розгортається на Ubuntu Server, а для VPN-з'єднань використовується окрема підмережа 10.0.1.0/24.

Першим етапом є встановлення програмних пакетів, необхідних для роботи OpenVPN Server. Для цього на Ubuntu Server виконується оновлення списку пакетів і встановлення OpenVPN та iptables-persistent:

```
sudo apt update
sudo apt install openvpn iptables-persistent -y
```

Пакет openvpn забезпечує створення VPN-тунелю, приймання клієнтських підключень, шифрування трафіку та роботу віртуального мережевого інтерфейсу tun. Пакет iptables-persistent використовується для збереження правил firewall і NAT після перезавантаження сервера.

Для зберігання конфігураційних файлів, сертифікатів і журналів OpenVPN створюється окрема структура каталогів. У даній роботі використовується каталог /etc/openvpn/openvpn_conf, у якому розміщуються серверні ключі та файли журналів:

```
sudo mkdir -p /etc/openvpn/openvpn_conf/server
sudo mkdir -p /etc/openvpn/openvpn_conf/log
sudo mkdir -p /etc/openvpn/ccd
```

Каталог /etc/openvpn/openvpn_conf/server призначений для файлів сертифікатів і ключів OpenVPN Server. Каталог /etc/openvpn/openvpn_conf/log використовується для журналів роботи сервера. Каталог /etc/openvpn/ccd потрібен для індивідуальних клієнтських параметрів, зокрема для закріплення статичних VPN-адрес за маршрутизаторами.

Оскільки сертифікати вже були випущені, на VPN-сервер передаються готові файли:

1. ca.crt;
2. server.crt;
3. server.key;

4. dh.pem;
5. ta.key.

Передавання виконується через захищене SSH-з’єднання. У результаті VPN-сервер отримує лише ті файли, які потрібні для роботи OpenVPN, а компоненти випуску сертифікатів залишаються на контролері домену. Такий підхід зменшує ризик компрометації центру сертифікації у випадку несанкціонованого доступу до VPN-сервера.

Для роботи OpenVPN Server у режимі маршрутизації необхідно дозволити пересилання IP-пакетів між інтерфейсами та налаштувати правила firewall. У даному проєкті ці параметри винесені в окремий скрипт /etc/nat, який автоматично запускається під час старту OpenVPN.

sudo nano /etc/nat

Далі у скрипті вмикається IP forwarding:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Цей рядок дозволяє серверу пересилати трафік між VPN-інтерфейсом і мережевим інтерфейсом сервера.

Після цього очищуються попередні правила firewall та NAT:

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
```

Далі дозволяються основні підключення: уже встановлені з’єднання, SSH-доступ, OpenVPN-порт 1194/UDP та трафік через VPN-інтерфейс tun0:

```
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --dport 1194 -j ACCEPT
iptables -A INPUT -i tun0 -j ACCEPT
```

Для проходження транзитного трафіку між зовнішнім інтерфейсом і VPN-тунелем додаються правила:

```
iptables -A FORWARD -i eth0 -o tun0 -j ACCEPT
iptables -A FORWARD -i tun0 -o eth0 -j ACCEPT
```

Після створення файлу йому надаються права на виконання:

```
chmod 755 /etc/nat
```

Кінцевий вигляд файлу можна переглянути на рисунку 3.13.

Після налаштування файлу /etc/nat виконується створення основного конфігураційного файлу OpenVPN Server – server.conf. У ньому задаються параметри роботи VPN-сервера, шляхи до сертифікатів, VPN-підмережа, правила передавання DNS-параметрів і маршрути до локальних мереж головного офісу та додаткового підрозділу.

Файл відкривається командою:

```
sudo nano /etc/openvpn/server.conf
```

У файл вноситься конфігурація server.conf згідно додатку Б.

```
#!/bin/sh

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X

iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --dport 1194 -j ACCEPT

iptables -A INPUT -i tun0 -j ACCEPT

iptables -A FORWARD -i eth0 -o tun0 -j ACCEPT
iptables -A FORWARD -i tun0 -o eth0 -j ACCEPT
```

Рисунок 3.13 – Налаштування файлу /etc/nat

У цій конфігурації OpenVPN Server працює на UDP-порту 1194 та створює VPN-підмережу 10.0.1.0/24. Сервер використовує сертифікати й ключі, які були попередньо випущені за допомогою EasyRSA на головному контролері домену та передані на VPN-сервер. У файлі також задано маршрути до локальних мереж

192.168.5.0/24 і 192.168.6.0/24, а клієнтам передаються DNS-сервери 192.168.5.2 та 192.168.6.2 для коректної роботи доменної інфраструктури.

Підготовка CCD-файлів для статичних VPN-адрес та маршрутів:

Для клієнта office_1 створюється файл:

```
sudo nano /etc/openvpn/ccd/office_1
```

У нього додається:

```
ifconfig-push 10.0.1.2 255.255.255.0
iroute 192.168.5.0 255.255.255.0
```

Для клієнта office_2:

```
sudo nano /etc/openvpn/ccd/office_2
ifconfig-push 10.0.1.3 255.255.255.0
iroute 192.168.6.0 255.255.255.0
```

3.5 Встановлення клієнтських файлів на маршрутизатори через WinBox

Після підготовки клієнтських конфігураційних файлів office_1.ovpn та office_2.ovpn необхідно перенести їх на відповідні маршрутизатори та імпортувати в RouterOS. Для виконання цього етапу використовується програма WinBox, яка дозволяє керувати маршрутизаторами через графічний інтерфейс.

Кожен маршрутизатор отримує власний файл конфігурації. Для маршрутизатора головного офісу використовується файл office_1.ovpn, а для маршрутизатора додаткового підрозділу – office_2.ovpn. У цих файлах уже містяться параметри підключення до OpenVPN-сервера, сертифікат центру сертифікації, клієнтський сертифікат, приватний ключ і TLS-auth ключ.

Спочатку виконується підключення до маршрутизатора через WinBox. Після входу в систему відкривається розділ Files, який використовується для зберігання файлів у RouterOS. У це вікно завантажується відповідний .ovpn файл за допомогою кнопки Upload або перетягуванням файлу у вікно. Після успішного завантаження файл з’являється у списку файлів маршрутизатора (рисунок 3.14).

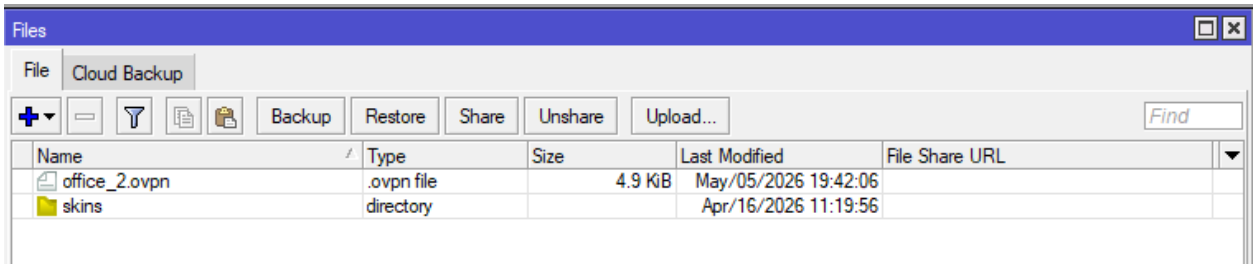


Рисунок 3.14 – Завантаження файлу office_2.ovpn у розділ Files

Після завантаження конфігураційного файлу виконується його імпорт. Для цього відкривається розділ PPP, де доступна кнопка Import .ovpn. Після вибору потрібного файлу RouterOS зчитує параметри підключення та створює новий клієнтський OpenVPN-інтерфейс.

Для головного офісу імпортується файл: office_1.ovpn

Для додаткового підрозділу імпортується файл: office_2.ovpn

Після імпорту в розділі PPP з'являється новий запис типу OVPN Client. Це означає, що конфігурація була успішно оброблена маршрутизатором.

3.6 Налаштування маршрутизації між маршрутизаторами

Після імпорту OpenVPN-конфігурацій на маршрутизатори необхідно дозволити проходження трафіку між локальними мережами Office_1 і Office_2, а також між кожною локальною мережею та VPN-сегментом 10.0.1.0/24.

Для забезпечення взаємодії між цими мережами на обох маршрутизаторах були створені правила firewall у ланцюгу forward. Цей ланцюг відповідає за транзитний трафік, тобто за пакети, які проходять через маршрутизатор з однієї мережі в іншу. Зображено на рисунку 2.15.

На маршрутизаторі Office_1_Router були дозволені такі напрямки:

1. з 192.168.5.0/24 до 192.168.6.0/24;
2. з 192.168.5.0/24 до 10.0.1.0/24;
3. з 10.0.1.0/24 до 192.168.5.0/24.

#		Action	Chain	Src. Address	Dst. Address
0		accept	forward	192.168.5.0/24	192.168.6.0/24
1		accept	forward	192.168.6.0/24	192.168.5.0/24
;;; LAN1 -> VPN					
2		accept	forward	192.168.5.0/24	10.0.1.0/24
;;; VPN -> LAN1					
3		accept	forward	10.0.1.0/24	192.168.5.0/24

Рисунок 3.15 – Firewall-правила маршрутизатора Office_1_Router

На маршрутизаторі Office_2_Router були дозволені такі напрямки (рисунок 3.16):

1. з 192.168.6.0/24 до 192.168.5.0/24;
2. з 192.168.6.0/24 до 10.0.1.0/24;
3. з 10.0.1.0/24 до 192.168.6.0/24.

#		Action	Chain	Src. Address	Dst. Address
0		accept	forward	192.168.6.0/24	192.168.5.0/24
1		accept	forward	192.168.5.0/24	192.168.6.0/24
;;; LAN2 -> VPN					
2		accept	forward	192.168.6.0/24	10.0.1.0/24
;;; VPN -> LAN2					
3		accept	forward	10.0.1.0/24	192.168.6.0/24

Рисунок 3.16 – Firewall-правила маршрутизатора Office_2_Router

Після додавання цих правил маршрутизатори не блокують трафік між локальними підмережами та VPN-сегментом. Це дозволяє клієнтам мережі Office_1 звертатися до пристроїв у мережі Office_2, а клієнтам Office_2 – до ресурсів головного офісу.

3.7 Проведення основних тестів підключення та під’єднання додаткового сервера до домену

Після налаштування VPN-з’єднання, імпорту клієнтських конфігурацій на маршрутизатори та створення правил firewall необхідно перевірити працездатність усієї мережевої схеми.

Спочатку виконується перевірка доступності VPN-сегмента між маршрутизаторами. Маршрутизатор головного офісу має VPN-адресу 10.0.1.2, а маршрутизатор додаткового підрозділу – 10.0.1.3. За допомогою команди ping (рисунок 3.17).

```
[admin@MikroTik] > ping 10.0.1.3
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 10.0.1.3                                   56  64 684us
    1 10.0.1.3                                   56  64 750us
    2 10.0.1.3                                   56  64 675us

[admin@MikroTik] > ping 10.0.1.2
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 10.0.1.2                                   56  64 650us
    1 10.0.1.2                                   56  64 762us
    2 10.0.1.2                                   56  64 724us
    3 10.0.1.2                                   56  64 829us
    4 10.0.1.2                                   56  64 807us
    5 10.0.1.2                                   56  64 711us
    sent=6 received=6 packet-loss=0% min-rtt=650us avg-rtt=747us max-rtt=829us
```

Рисунок 3.17 – Перевірка доступності VPN-адрес між маршрутизаторами

Після цього перевіряється доступність локальних мереж (рисунок 3.18.) З мережі Office_1 виконується перевірка доступності сервера OFFICE_2_DC з адресою 192.168.6.2, а з мережі Office_2 – доступність головного контролера домену OFFICE_1_GDC з адресою 192.168.5.2.

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin> ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\admin>
```

Рисунок 3.18 – Перевірка доступності серверів між Office_1 та Office_2

Наступним етапом є підключення сервера OFFICE_2_DC до домену. Перед цим на самому сервері необхідно вручну задати статичні мережеві параметри. Особливо важливо вказати DNS-сервером головний контролер домену OFFICE_1_GDC (рисунок 3.19), тобто адресу 192.168.5.2. Це потрібно для того, щоб сервер OFFICE_2_DC міг знайти домен corp.diplom.com і отримати необхідні DNS-записи Active Directory.

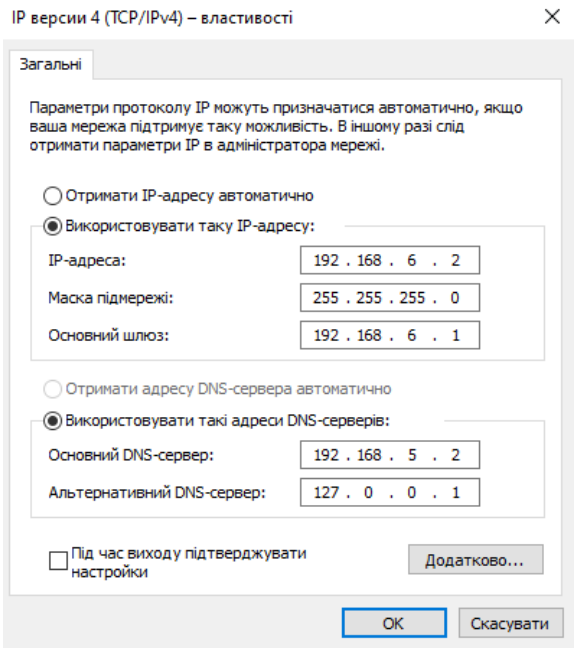


Рисунок 3.19 – Мережеві параметри Office_2.

Після внесення цих параметрів перевіряється доступність головного контролера домену (рисунок 3.20).

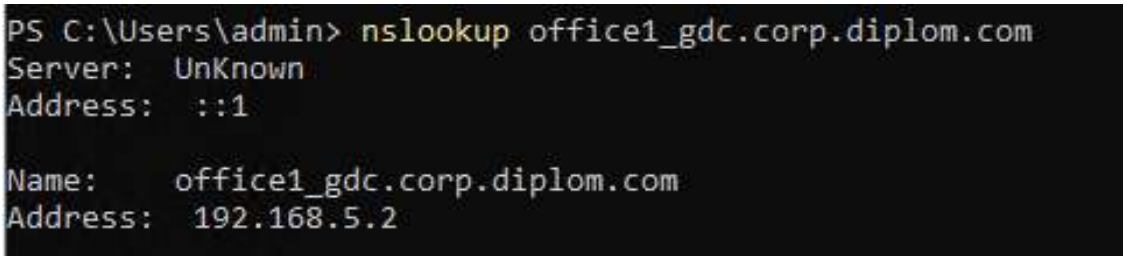


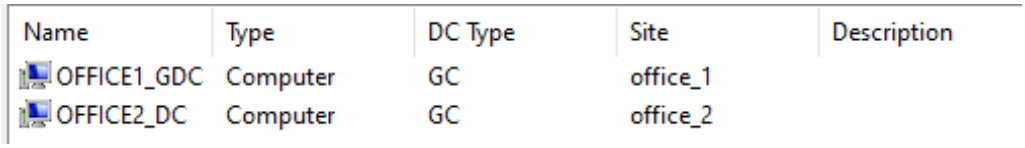
Рисунок 3.20 – Перевірка доступності домену.

Якщо сервер отримує відповідь від DNS-сервера та коректно визначає домен, можна переходити до підключення OFFICE_2_DC до домену. Для цього

у властивостях системи Windows Server відкриваються параметри імені комп'ютера, після чого замість робочої групи вказується домен.

Під час підключення до домену система запитує облікові дані доменного адміністратора. Після успішної перевірки облікових даних сервер приєднується до домену та потребує перезавантаження.

Після перезавантаження сервера виконується встановлення ролі Active Directory Domain Services. У майстрі налаштування сервер додається не як новий окремий домен, а як додатковий контролер до вже існуючого домену corp.diplom.com. Після завершення налаштування сервер OFFICE_2_DC стає додатковим контролером домену та DNS-сервером для мережі додаткового підрозділу. Зображено на рисунку 3.21.

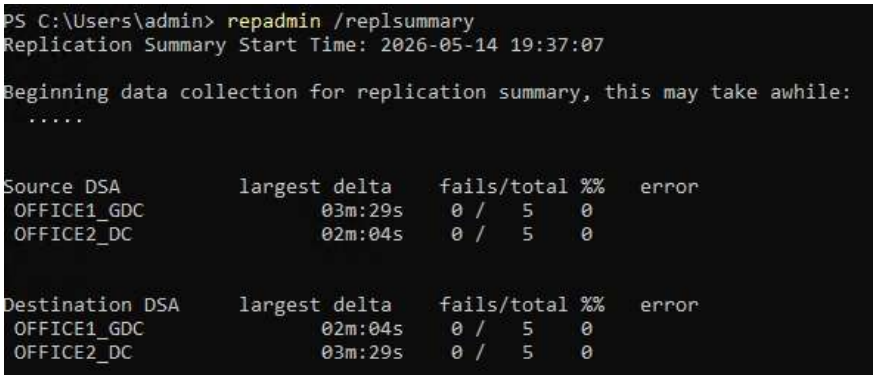


Name	Type	DC Type	Site	Description
OFFICE1_GDC	Computer	GC	office_1	
OFFICE2_DC	Computer	GC	office_2	

Рисунок 3.21 – Список контролерів домену.

Після підняття ролі додаткового контролера домену необхідно перевірити реплікацію Active Directory (рисунок 3.22). Для цього можна використати стандартні команди Windows Server:

```
repadmin /replsummary
repadmin /showrepl
```



```
PS C:\Users\admin> repadmin /replsummary
Replication Summary Start Time: 2026-05-14 19:37:07

Beginning data collection for replication summary, this may take awhile:
  .....


Source DSA          largest delta    fails/total %%   error
 OFFICE1_GDC               03m:29s    0 /   5    0
 OFFICE2_DC                02m:04s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 OFFICE1_GDC               02m:04s    0 /   5    0
 OFFICE2_DC                03m:29s    0 /   5    0
```

Рисунок 3.22 – Перевірка реплікації між OFFICE_1_GDC та OFFICE_2_DC

3.8 Висноки до третього розділу

У третьому розділі було виконано практичне налаштування внутрішньої корпоративної мережі із захищеним доступом на основі OpenVPN. На початковому етапі було налаштовано локальні мережі головного офісу Office_1 та додаткового підрозділу Office_2. Для кожної мережі було задано окремий адресний простір, налаштовано шлюзи, DHCP-служби, DNS-параметри та базові правила доступу.

Далі було підготовлено сертифікати та ключі для OpenVPN-з'єднання. Випуск сертифікатів виконувався на головному контролері домену за допомогою EasyRSA, після чого були створені клієнтські конфігураційні файли для маршрутизаторів обох підрозділів. Це дозволило забезпечити автентифікацію VPN-клієнтів і підготувати основу для захищеного з'єднання між мережами.

Після цього було налаштовано OpenVPN-сервер, визначено VPN-підмережу 10.0.1.0/24, підготовлено параметри маршрутизації, firewall і NAT. Клієнтські конфігурації були імпортовані на маршрутизатори через WinBox, після чого маршрутизатори головного офісу та додаткового підрозділу отримали можливість підключатися до VPN-сервера.

Окремо було налаштовано правила firewall на маршрутизаторах для дозволу транзитного трафіку між мережами 192.168.5.0/24, 192.168.6.0/24 та VPN-сегментом 10.0.1.0/24. Завдяки цьому клієнти обох локальних мереж отримали можливість взаємодіяти між собою через захищений VPN-канал.

На завершальному етапі було проведено тестування доступності між мережами та підключено сервер OFFICE_2_DC до домену як додатковий контролер домену. Перед підключенням на сервері було налаштовано DNS головного контролера домену, а після успішного введення сервера в домен були змінені DNS-параметри на маршрутизаторі додаткового підрозділу.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень було розроблено і реалізовано модель внутрішньої корпоративної мережі компанії із захищеним доступом на основі персонального VPN-сервера. У процесі виконання роботи було вирішено задачу об’єднання двох окремих локальних мереж у єдину захищену інфраструктуру з можливістю взаємного доступу клієнтів до ресурсів обох підрозділів. Запропоноване рішення дозволяє організувати захищений обмін службовим трафіком між головним офісом і додатковим підрозділом, а також забезпечити роботу доменної інфраструктури через VPN-з’єднання.

У першому розділі проведено аналіз теоретичних основ побудови комп’ютерних і корпоративних мереж. Було розглянуто поняття мережі, способи її організації, види мережевого зв’язку, принципи маршрутизації та особливості застосування VPN-технологій. Окрему увагу приділено видам VPN-протоколів, їхнім перевагам, недолікам і доцільності використання у корпоративному середовищі. Також було виконано порівняння персонального VPN-сервера з хмарними рішеннями захищеного доступу, на основі чого обґрунтовано доцільність використання персонального VPN-рішення для даного проєкту.

У другому розділі проведено проєктування середовища для реалізації корпоративної мережі. Було розроблено базову карту мережі, визначено логічну та фізичну структуру інфраструктури, обрано адресні простори для головного офісу, додаткового підрозділу та VPN-сегмента. Також було обґрунтовано вибір апаратних і програмних засобів, підготовлено віртуальне середовище, створено віртуальні маршрутизатори та окремі локальні мережеві сегменти. Додатково було підготовлено серверну платформу для подальшого розгортання VPN-сервера та забезпечено базові умови для подальшого налаштування мережевої взаємодії.

У третьому розділі виконано практичне налаштування розробленої інфраструктури. Було налаштовано локальні мережі головного офісу та додаткового підрозділу, DHCP-служби, DNS-параметри, firewall-правила, клієнтські VPN-конфігурації та маршрутизацію між мережами. Також було випущено сертифікати для сервера і клієнтів, налаштовано OpenVPN-сервер, імпортовано клієнтські файли на маршрутизатори та перевірено проходження трафіку між підмережами. На завершальному етапі сервер додаткового підрозділу було підключено до доменної інфраструктури як додатковий контролер домену, після чого перевірено роботу DNS, реплікації та службових ресурсів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Децентралізована мережа URL: https://studfile.net/html/2706/1176/html_Bh5Rguqnvg.UBnc/img-aUcCBq.jpg (дата звернення: 20.02.2026).
2. Sadiku M. N. O., Akujuobi C. M. Network models. Fundamentals of computer networks. Cham, 2022. P. 19–36. (дата звернення: 22.02.2026).
3. Базові Технології Локальних Мереж. URL: https://studfile.net/preview/5199186/ (дата звернення: 22.02.2026).
4. Основи технології клієнт/сервер. URL: https://buklib.net/books/24515/ (дата звернення: 22.02.2026).
5. Основи маршрутизації в мережах: Покроковий посібник. URL: https://proxys-rating.com/osnovy-marshrutyzacziyi-v-merezhah-pokrokovyj-posibnyk/ (дата звернення: 20.02.2026).
6. What Is a VPN? URL: https://www.cloudflare.com/learning/network-layer/what-is-a-vpn/ (дата звернення (дата звернення: 25.04.2026).
7. What Is a DNS? URL: https://www.cloudflare.com/learning/dns/what-is-dns/ (дата звернення: 20.02.2026).
8. Що таке віртуальна машина та як вона працює. URL: https://gigacloud.ua/articles/shho-take-virtualna-mashyna-ta-yak-vona-praczyuye/ (дата звернення: 22.02.2026).
9. Hyper-V documentation. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/ (дата звернення: 25.04.2026).
10. Kristianto P. E., Putra A. T. Comparative analysis of ipv4 and ipv6 openvpn protocol performance based on qos parameters. Journal of advances in information systems and technology. 2021. Vol. 3, no. 1. P. 53–60. (дата звернення: 22.02.2026).

11. Plan for Hyper-V networking in Windows Server. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-networking-in-windows-server (дата звернення: 25.04.2026)..

12. How does VPN work?. URL: http://bit.ly/42Lkfr7 (дата звернення: 20.02.2026).

13. OpenVPN 2.4 Manual. URL: https://openvpn.net/community-docs/community-articles/openvpn-2-4-manual.html (дата звернення: 20.02.2026).

14. Cloud Hosted Router, CHR. Documentation. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/18350234/Cloud+Hosted+Router+CHR (дата звернення: 21.03.2026).

15. IPv4 and IPv6 Fundamentals. Documentation. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/119144661/IPv4+and+IPv6+Fundamentals (дата звернення: 22.03.2026).

16. Virtual Routing and Forwarding – VRF URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328206/Virtual+Routing+and+Forwarding+-+VRF (дата звернення: 22.03.2026).

17. OpenVPN server.conf and client.conf URL: https://gist.github.com/deargle/ce70b597645dc7c7c9eaec40875faaf5 (дата звернення: 24.04.2026).

18. iptables(8) – Linux manual page URL: https://man7.org/linux/man-pages/man8/iptables.8.html (дата звернення: 20.03.2026).

19. Documentation directory Server URL: https://ubuntu.com/server/docs/ (дата звернення: 20.02.2026).

20. OpenVPN client Documentation. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/2031655/OpenVPN#OpenVPN-OVPNClient (дата звернення: 23.04.2026).

21. Tutorial: Configure External PKI with Easy-RSA. URL: https://openvpn.net/as-docs/tutorials/tutorial--epki-with-easy-rsa.html#tutorial--configure-external-pki-with-easy-rsa (дата звернення: 20.04.2026).

22. Active Directory Domain Services overview URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення 12.05.2026).

23. Install Active Directory Domain Services URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100- (дата звернення 12.05.2026).

24. OpenVPN GitHub URL: https://github.com/OpenVPN (дата звернення 23.04.2026).

25. What is OSI Model? URL: https://aws.amazon.com/what-is/osi-model/ (дата звернення 23.02.2026).

26. What is UDP? URL: https://www.cloudflare.com/ru-ru/learning/ddos/glossary/user-datagram-protocol-udp/ (дата звернення 23.02.2026).

27. What happens in a TLS handshake? URL: https://www.cloudflare.com/ru-ru/learning/ddos/glossary/user-datagram-protocol-udp/ (дата звернення 26.03.2026).

28. EasyRSA URL: https://github.com/OpenVPN/easy-rsa (дата звернення 26.04.2026).

29. WireGuard vs OpenVPN URL: https://www.rtings.com/vpn/learn/wireguard-vs-openvpn (дата звернення 26.04.2026).

30. Знайомство з операційною системою Linux¶ URL: https://docs.rockylinux.org/10/uk/books/admin_guide/01-presentation/ (дата звернення 26.04.2026).

31. В чому переваги Linux та як почати працювати з цією ОС. URL: https://dou.ua/forums/topic/41333/ (дата звернення 22.02.2026).

32. Getting and Upgrading the License CHR URL: https://help.mikrotik.com/docs/spaces/ROS/pages/18350234/Cloud+Hosted+Router+CHR#CloudHostedRouter%2CCHR-GettingandUpgradingtheLicense (дата звернення 26.04.2026).

33. What is DHCP? and Why is it important? URL: https://efficientip.com/glossary/what-is-dhcp-and-why-is-it-important/ (дата звернення 26.04.2026).

34. What’s the Difference Between IPv4 and IPv6? URL: https://aws.amazon.com/compare/the-difference-between-ipv4-and-ipv6/ (дата звернення 26.04.2026).

35. IPv4 URL: https://uk.wikipedia.org/wiki/IPv4 (дата звернення 26.04.2026).

36. Bridging and Switching - RouterOS - MikroTik Documentation. MikroTik Support Service. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching (дата звернення: 26.05.2026).

37. Fast Forward URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching#BridgingandSwitching-FastForward (дата звернення 26.04.2026).

38. What’s the Difference Between LAN and WAN? URL: https://aws.amazon.com/compare/the-difference-between-lan-and-wan/ (дата звернення 26.04.2026).

39. Install and configure DNS Server on Windows Server URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server?tabs=powershell (дата звернення 26.04.2026).

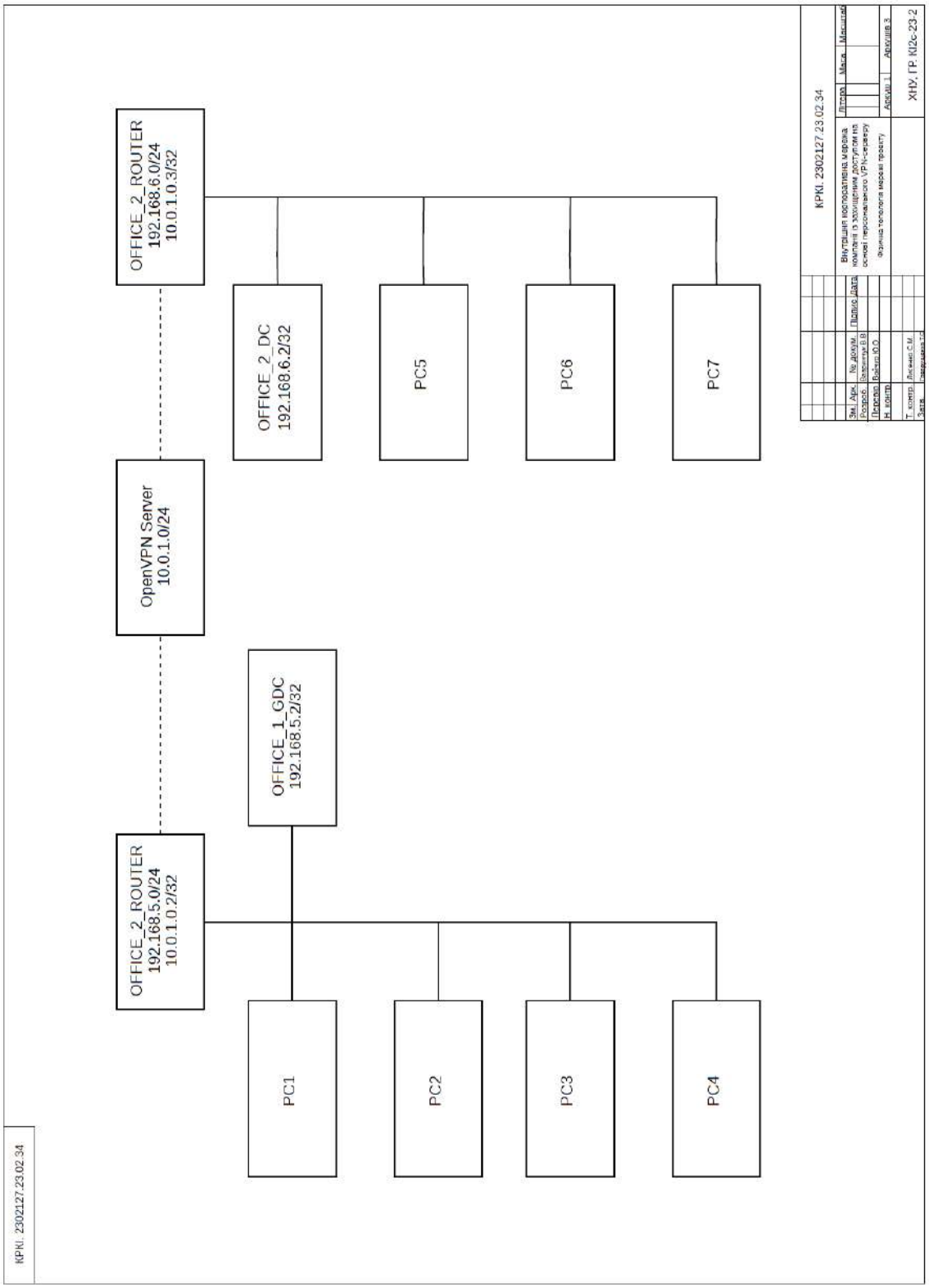
40. What is Domain Name System (DNS)? URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-overview (дата звернення 26.04.2026).

41. Secure VPN solutions for business & remote access openvpn. OpenVPN. URL: https://openvpn.net (дата звернення: 26.05.2026).

ДОДАТОК А

(обов’язковий)

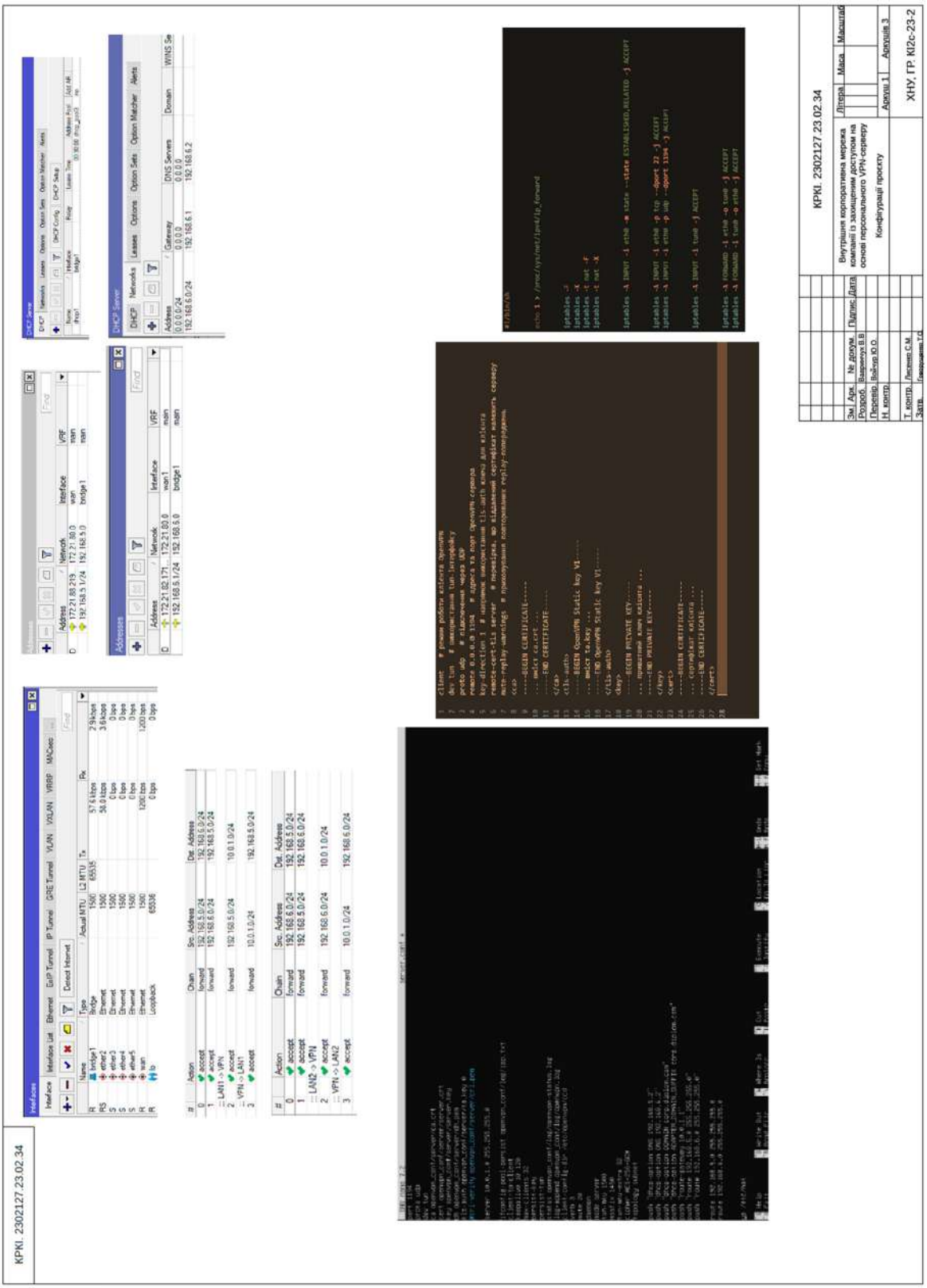
Копія креслення «Фізична топологія мережі проекту»



ДОДАТОК Б

(обов’язковий)

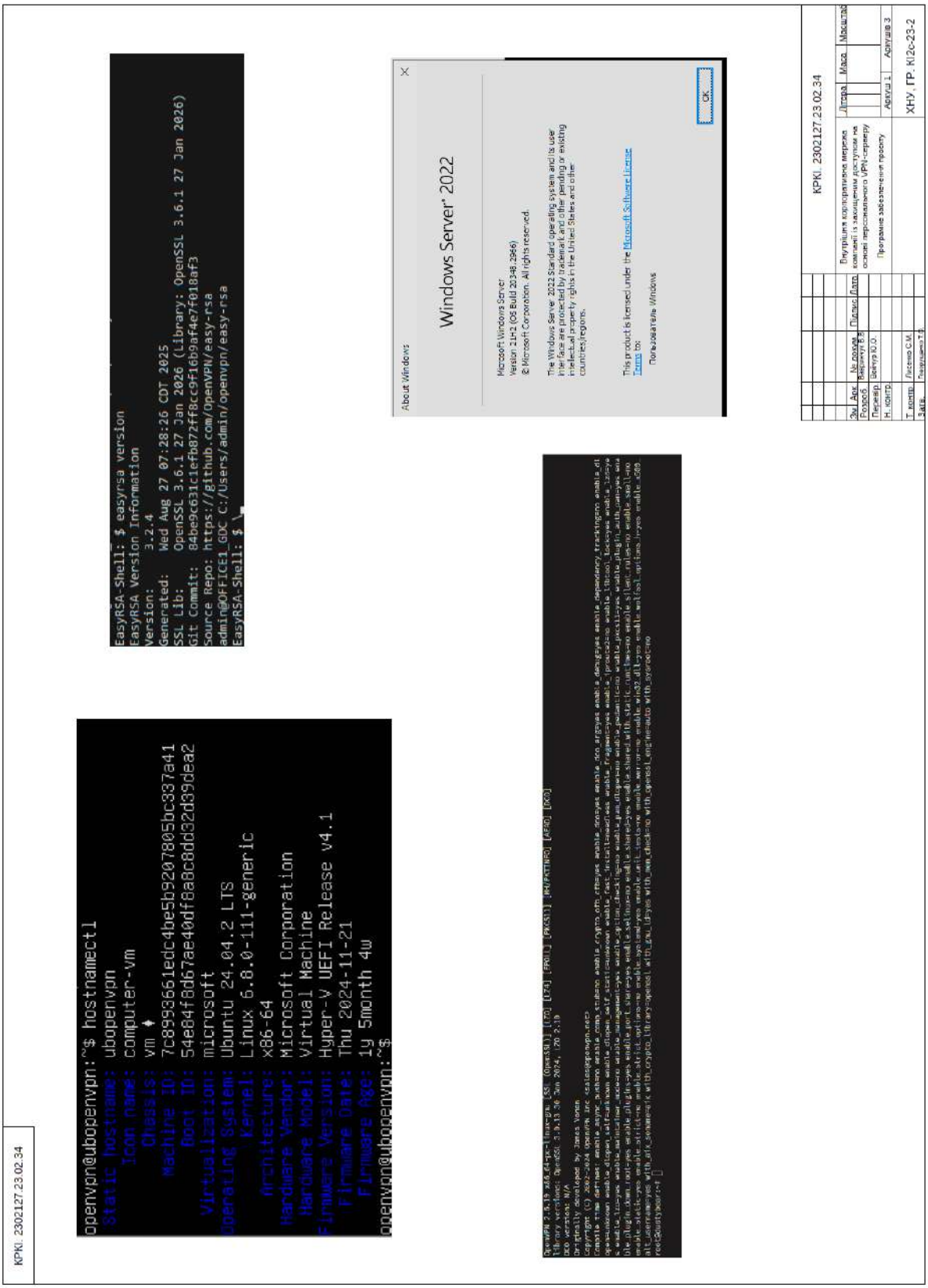
Копія креслення «Конфігурації проєкту»



ДОДАТОК В

(обов’язковий)

Копія креслення «Програмне забезпечення проєкту»



РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу
Автор Владислав ВАВРИНЧУК
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: Юрій ВОЙЧУР д.ф

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 1,96%; та системою Anti-Plagiarism складає 2%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.06.2026

Завідувач кафедри _____ Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

Гарант освітньої програми _____ Підпис — Андрій НІЧЕПОРУК (Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи _____ Підпис — Юрій ВОЙЧУР (Ім'я, ПРІЗВИЩЕ)

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Владислав ВАВРИНЧУК

Співавтор:

Назва: Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу

Експерт: Юрій ВОЙЧУР

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:1.96%

Коефіцієнт подібності 2:0.31%

Мікропробіли: 0

Заміна букв: 1

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2026-05-27 21:06:13.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-05-28 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Вавринчук Владислав Володимирович

Тема: Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3___ Кількість сторінок записки ___63___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проєктування, налаштування та тестування внутрішньої корпоративної мережі компанії із захищеним доступом на основі персонального VPN-сервера для об'єднання локальних мереж головного офісу й додаткового підрозділу в єдину захищену інфраструктуру.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі кваліфікаційної роботи проведено аналіз теоретичних основ побудови комп'ютерних і корпоративних мереж, а саме: розглянуто поняття комп'ютерної мережі, способи організації мережевої інфраструктури, види зв'язку між мережами, принципи маршрутизації, особливості використання VPN-технологій, основні види VPN-протоколів, їх переваги й недоліки; у другому розділі кваліфікаційної роботи проведено проєктування середовища для реалізації корпоративної мережі, а саме: розроблено топологічну карту мережі, визначено логічну та фізичну структуру інфраструктури, обрано адресні простори для головного офісу, додаткового підрозділу та VPN-сегмента, обґрунтовано вибір апаратних і програмних засобів, підготовлено віртуальне середовище, створено віртуальні маршрутизатори, окремі локальні мережеві сегменти та серверну платформу для подальшого розгортання VPN-сервера; у третьому розділі кваліфікаційної роботи виконано практичну

реалізацію розробленої мережевої інфраструктури, а саме: налаштовано локальні мережі головного офісу та додаткового підрозділу, DHCP-служби, DNS-параметри, firewall-правила, сертифікати для OpenVPN, клієнтські конфігураційні файли та маршрутизацію між підмережами, виконано налаштування VPN-сервера, імпорт клієнтських файлів на маршрутизатори, перевірку доступності між мережами та підключення сервера додаткового підрозділу до домену як додаткового контролера домену.

4. Позитивні сторони роботи: позитивною стороною роботи є практична реалізація працездатної захищеної корпоративної мережі з об'єднанням віддалених підрозділів та перевіркою її роботи в умовах, наближених до реальної інфраструктури.

5. Негативні сторони роботи: недоліки в роботі відсутні.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на високому технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: відмінно (A/93)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Пеньовський Сергій Степанович, доцент кафедри КН, к.п.н.,
Хмельницький національний університет

"1" 06 2026 р. _____(підпис)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Владислав ВАВРИНЧУК

ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-23-2

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

27 травня 2026 року

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 2.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 15%**

ID: 272550 Назва: БКР Внутрішня корпоративна мережа компанії із захищеним доступом на основі персонального VPN-серверу Додано в БД: 2026-05-28 Автора: Владислав ВАВРИНЧУК Керівники: Юрій ВОЙЧУР Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	82378	759	1863 (2%)	27 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми