

Міністерство освіти і науки України
Луцький національний технічний університет

(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій

(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем

(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА
«ОРИОН» З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN ДЛЯ ЗАХИЩЕНОЇ
ВЗАЄМОДІЇ МІЖ ФІЛІЯМИ

DESIGNING THE CORPORATE NETWORK OF THE «ORION»
ENTERPRISE USING VPN TECHNOLOGY FOR SECURE INTERACTION
BETWEEN BRANCHES

спеціальність 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія

(назва освітньої програми)

Виконав: здобувач вищої освіти
групи KI-41
Нікітчук Марія Олександрівна

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія Володимирівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« » 2026 р.

Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних та інформаційних технологій

Кафедра комп'ютерної інженерії та безпеки

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

доц. Т. Терлецький

« 23 » 12 2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Нікітчук Марії Олександрівні

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Проектування корпоративної мережі підприємства «Оріон» з використанням технології VPN для захищеної взаємодії між філіями

Керівник роботи к.т.н., доцент Багнюк Наталія Володимирівна

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026 р.

3. Вихідні дані до роботи: джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

Вступ

Теоретичні основи побудови корпоративних мереж і VPN-технологій

Аналіз підприємства «Оріон» та вимог до корпоративної мережі

Практична реалізація побудови мережі

Висновки

5. Перелік графічного (ілюстративного) матеріалу:

Класифікація VPN-технологій

Загальна характеристика підприємства «Оріон»

Логічна структура корпоративної мережі

Налаштування VPN-тунелів між філіями

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
<i>Теоретичні основи побудови корпоративних мереж і VPN-технологій</i>	<i>Багнюк Н. В., доцент</i>		
<i>Аналіз підприємства «Оріон» та вимог до корпоративної мережі</i>	<i>Багнюк Н. В., доцент</i>		
<i>Практична реалізація побудови мережі</i>	<i>Багнюк Н. В., доцент</i>		
<i>Нормоконтроль</i>	<i>Багнюк Н. В., доцент</i>		
<i>Гарант ОП</i>	<i>Лавренчук С. В., доцент</i>		
<i>Показник запозичень тексту</i>		%	
<i>Академічна доброчесність</i>	<i>Міскевич О. І., ст. викладач</i>		

7. Дата видачі завдання 23.12.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	<i>Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень</i>	до 10.02.2026 р.	
2.	<i>Теоретичні основи побудови корпоративних мереж і VPN-технологій</i>	до 02.03.2026 р.	
3.	<i>Аналіз підприємства «Оріон» та вимог до корпоративної мережі</i>	до 02.04.2026 р.	
4.	<i>Практична реалізація побудови мережі</i>	до 10.04.2026 р.	
5.	<i>Представлення остаточного варіанту кваліфікаційної роботи керівникові</i>	до 01.05.2026 р.	
6.	<i>Нормоконтроль</i>	до 23.05.2026 р.	
7.	<i>Інструментальна перевірка на академічний плагіат</i>	до 26.05.2026 р.	
8.	<i>Здача кваліфікаційної роботи та всіх супровідних документів на кафедру</i>	до 28.05.2026 р.	

Здобувач вищої освіти

(підпис)

Марія НІКІТЧУК

(прізвище, ініціали)

Керівник кваліфікаційної роботи

(підпис)

Наталія БАГНЮК

(прізвище, ініціали)

АНОТАЦІЯ

Нікітчук М. О. Проектування корпоративної мережі підприємства «Оріон» з використанням технології VPN для захищеної взаємодії між філіями. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

У першому розділі проаналізовано теоретичні основи побудови корпоративних мереж і VPN-технологій: розглянуто поняття та структуру корпоративних комп'ютерних мереж, основні принципи побудови розподілених мереж підприємств, технології VPN та їх класифікацію, а також протоколи і методи забезпечення захищеного каналу зв'язку.

У другому розділі виконано аналіз підприємства та вимог до корпоративної мережі, надано загальну характеристику підприємства та його організаційної структури, описано філіальну мережу й інформаційні потоки, розроблено логічну структуру мережі та сформульовано вимоги до захисту даних і мережевої безпеки.

Третій розділ містить практичну реалізацію побудови мережі: налаштування VLAN на комутаторах та DHCP-сервера, конфігурацію протоколу HSRP для забезпечення відмовостійкості, налаштування списків контролю доступу (ACL), маршрутизацію на основі протоколу OSPF, а також налаштування VPN-тунелів між філіями підприємства.

Ключові слова: корпоративна мережа, VPN, IPsec, OSPF, VLAN, HSRP, ACL, мережева безпека, захищений канал зв'язку, розподілена мережа, філія.

ANNOTATION

Nikitchuk M. Designing the corporate network of the «Orion» enterprise using VPN technology for secure interaction between branches. Manuscript.

Qualifying work of a bachelor of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

Qualification work consists of an introduction, three sections, conclusions, a references, and an appendix.

In the first chapter, the theoretical foundations of building corporate networks and VPN technologies are analyzed: the concepts and structure of corporate computer networks, the main principles of designing distributed enterprise networks, VPN technologies and their classification, as well as protocols and methods for ensuring secure communication channels are considered.

The second chapter provides an analysis of the enterprise and the requirements for the corporate network, including a general description of the enterprise and its organizational structure, a description of the branch network and information flows, the development of the logical network structure, and the formulation of requirements for data protection and network security.

The third chapter contains the practical implementation of the network design: VLAN configuration on switches and DHCP server setup, HSRP protocol configuration to ensure fault tolerance, Access Control List (ACL) configuration, OSPF-based routing, as well as the configuration of VPN tunnels between enterprise branches.

Keywords: corporate network, VPN, IPsec, OSPF, VLAN, HSRP, ACL, network security, secure communication channel, distributed network, branch office.

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ І VPN-ТЕХНОЛОГІЙ.....	9
1.1 Поняття та структура корпоративних комп'ютерних мереж	9
1.2 Основні принципи побудови розподілених мереж підприємств	11
1.3 Технології віртуальних приватних мереж (VPN), їх види та призначення	14
1.4 Протоколи та методи забезпечення захищеного каналу зв'язку	16
РОЗДІЛ 2 АНАЛІЗ ПІДПРИЄМСТВА «ОРІОН» ТА ВИМОГ ДО КОРПОРАТИВНОЇ МЕРЕЖІ	19
2.1 Загальна характеристика підприємства та його організаційної структури	19
2.2 Опис філіальної мережі та інформаційних потоків.....	20
2.3 Логічна структура мережі	21
2.4 Вимоги до захисту даних та мережевої безпеки.....	23
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ПОБУДОВИ МЕРЕЖІ	26
3.1 Створення та налаштування vlan на комутаторах та налаштування DHCP-сервера.....	26
3.2 Налаштування протоколу HSRP.....	30
3.3 Налаштування списків контролю доступу	31
3.4 Налаштування маршрутизації з використання протоколу OSPF	32
3.5 Налаштування VPN.....	37
ВИСНОВКИ.....	40
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	42

ВСТУП

Зростання обсягів корпоративного трафіку, підвищення вимог до конфіденційності комерційних даних, а також поширення дистанційної роботи зумовлюють необхідність впровадження сучасних рішень для організації захищених каналів зв'язку. Побудова надійної та захищеної корпоративної мережі набуває першочергового значення для підприємств із розгалуженою структурою філій. Підприємство «Оріон», як і більшість організацій із географічно розподіленою інфраструктурою, стикається з необхідністю забезпечити безперебійний, швидкий і захищений обмін даними між центральним офісом та відокремленим підрозділом.

Технологія VPN (Virtual Private Network) є одним із найефективніших інструментів побудови таких каналів, оскільки дозволяє організувати шифрований тунель між вузлами мережі поверх публічної інфраструктури Інтернету без витрат на прокладання виділених ліній зв'язку.

Незважаючи на широке практичне застосування VPN-рішень, їх проектування для конкретного підприємства потребує врахування особливостей топології мережі, кількості вузлів, вимог до пропускної здатності, обраних протоколів шифрування та механізмів автентифікації. Тому розробка проєкту корпоративної мережі підприємства «Оріон» із використанням технології VPN є актуальним науково-практичним завданням, що має пряме прикладне значення.

Метою кваліфікаційної роботи є розробка проєкту корпоративної мережі підприємства із застосуванням технології VPN для забезпечення захищеної взаємодії між філіями підприємства.

Об'єкт дослідження – процеси проектування та організації захищеної взаємодії між філіями розподіленого підприємства засобами корпоративної мережі.

Предмет дослідження – методи та засоби побудови корпоративної мережевої інфраструктури підприємства з використанням технології VPN для забезпечення конфіденційності, цілісності та доступності корпоративних даних.

Для досягнення поставленої мети визначено такі завдання дослідження:

- проаналізувати сучасний стан та тенденції розвитку технологій побудови корпоративних мереж і технології VPN;
- дослідити основні протоколи та стандарти VPN та обґрунтувати вибір оптимального протоколу для корпоративного середовища підприємства;
- розробити топологію корпоративної мережі підприємства з урахуванням розташування центрального офісу та філій;
- спроектувати адресний простір мережі, налаштувати маршрутизацію та визначити вимоги до мережевого обладнання;
- розробити та налаштувати VPN-тунелі між філіями підприємства для забезпечення захищеної передачі корпоративних даних;
- сформулювати рекомендації щодо політики інформаційної безпеки та адміністрування спроектованої мережної інфраструктури.

Розроблений проєкт корпоративної мережі підприємства може бути безпосередньо використаний у практичній діяльності підприємства для розгортання мережевої інфраструктури, а запропоновані рішення щодо архітектури VPN-з'єднань та налаштування засобів безпеки є універсальними і можуть бути адаптовані для аналогічних підприємств із розгалуженою структурою філій.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ І VPN-ТЕХНОЛОГІЙ

1.1 Поняття та структура корпоративних комп'ютерних мереж

Корпоративні комп'ютерні мережі (рис. 1.1) є складними інформаційно-комунікаційними системами, які забезпечують взаємодію між обчислювальними ресурсами, користувачами та сервісами в межах одного підприємства або групи взаємопов'язаних організацій. Їх основне призначення полягає у забезпеченні надійного, безпечного та ефективного обміну даними, централізованого управління інформаційними ресурсами, а також підтримці бізнес-процесів підприємства незалежно від його географічної розподіленості [1].

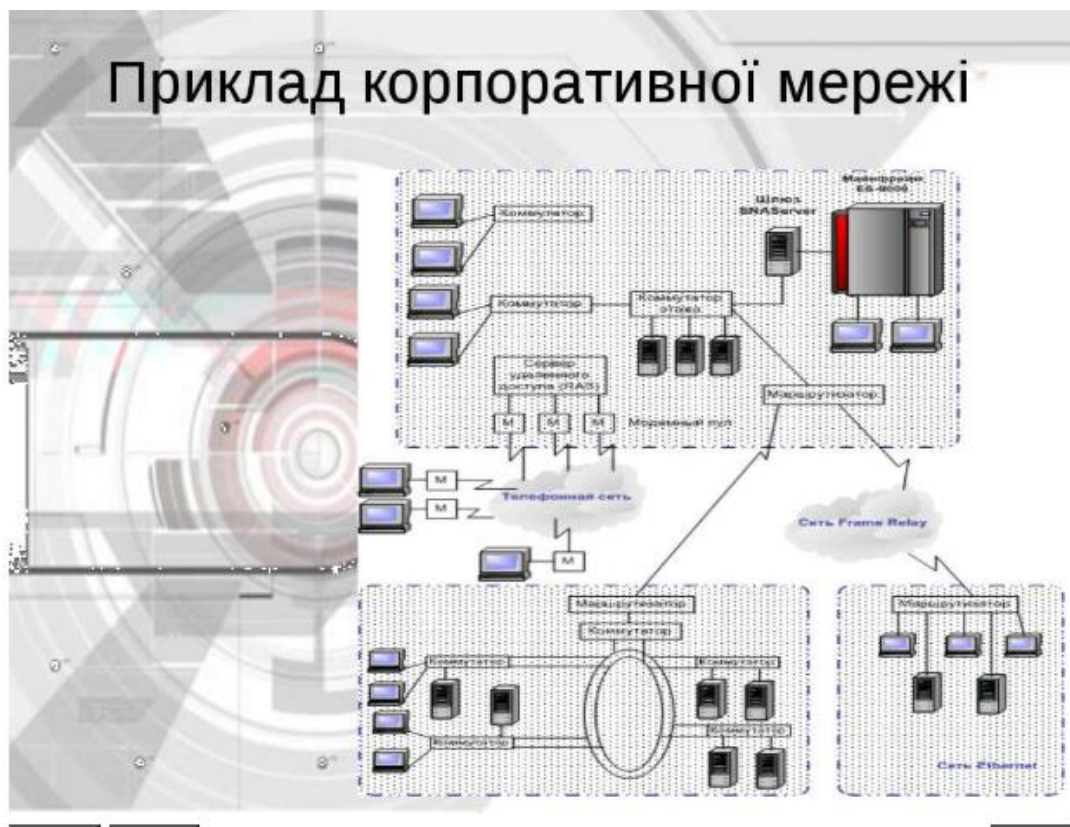


Рисунок 1.1 – Приклад корпоративної мережі [2]

З точки зору інфраструктурної організації корпоративна мережа являє собою багаторівневу систему, яка включає сукупність апаратних, програмних та

комунікаційних компонентів. До апаратної складової належать сервери, робочі станції, мережеве обладнання, таке як маршрутизатори, комутатори, міжмережеві екрани та пристрої забезпечення бездротового доступу. Програмна складова охоплює операційні системи, мережеві служби, системи керування базами даних, засоби моніторингу та захисту інформації, а також прикладне програмне забезпечення, яке використовується для реалізації бізнес-функцій підприємства. Комунікаційна складова базується на сукупності мережевих протоколів і технологій передачі даних, що забезпечують взаємодію між вузлами мережі як у локальному, так і в глобальному середовищі.

Структура корпоративної мережі, як правило, має ієрархічний характер і може бути представлена у вигляді багаторівневої архітектури, що включає рівень доступу, рівень розподілу та рівень ядра. Рівень доступу забезпечує підключення кінцевих пристроїв користувачів до мережі та реалізує базові функції комутації трафіку. Рівень розподілу виконує функції маршрутизації, агрегації трафіку, застосування політик безпеки та управління потоками даних між підмережами. Рівень ядра, у свою чергу, відповідає за високошвидкісну передачу даних між різними сегментами мережі та забезпечує її загальну продуктивність і надійність.

Важливою особливістю сучасних корпоративних мереж є їхня розподіленість, що обумовлена наявністю територіально віддалених філій, віддалених користувачів та хмарних сервісів. У таких умовах корпоративна мережа виходить за межі локальної інфраструктури та інтегрується з глобальними мережами передачі даних, що потребує впровадження механізмів захисту інформації, зокрема використання VPN-технологій [3], систем аутентифікації та шифрування трафіку.

Таким чином, корпоративна комп'ютерна мережа розглядається як інтегроване середовище, що поєднує апаратні та програмні ресурси підприємства в єдину систему, здатну забезпечити безперервність бізнес-процесів, високий рівень інформаційної безпеки та ефективну взаємодію між структурними підрозділами організації.

1.2 Основні принципи побудови розподілених мереж підприємств

Розподілені мережі підприємств є сучасною формою організації телекомунікаційної інфраструктури, що забезпечує інтеграцію територіально віддалених підрозділів у єдиний інформаційний простір. Основні принципи їх побудови базуються на необхідності забезпечення високого рівня доступності ресурсів, масштабованості, відмовостійкості та інформаційної безпеки, що в сукупності визначає ефективність функціонування всієї корпоративної системи.

Одним із ключових принципів побудови розподілених мереж є принцип ієрархічної організації. Він передбачає структурування мережевої інфраструктури на логічні та функціональні рівні, що дозволяє спростити керування мережею, оптимізувати маршрутизацію трафіку та підвищити її керованість. Ієрархічний підхід забезпечує можливість локалізації змін у межах окремих сегментів мережі без впливу на всю систему, що є особливо важливим для великих підприємств із розгалуженою структурою.

Не менш важливим є принцип масштабованості, який визначає здатність мережі адаптуватися до зростання кількості користувачів, пристроїв та сервісів без суттєвого погіршення продуктивності. Реалізація цього принципу передбачає використання гнучкої адресації, модульної архітектури мережевого обладнання та можливості інтеграції нових сегментів без кардинальної перебудови існуючої інфраструктури. Завдяки цьому підприємство може поступово розширювати свою мережу відповідно до потреб бізнесу.

Принцип відмовостійкості є ще одним базовим елементом побудови розподілених мереж. Він полягає у забезпеченні безперервності роботи мережевих сервісів навіть у разі виходу з ладу окремих компонентів інфраструктури. Досягнення відмовостійкості забезпечується шляхом резервування каналів зв'язку, дублювання критичних вузлів, використання протоколів динамічної маршрутизації та механізмів автоматичного переключення трафіку. Такий підхід мінімізує ризики простою системи та підвищує загальну надійність мережі.

Окреме місце займає принцип безпеки, який у розподілених мережах набуває особливої значущості через наявність зовнішніх каналів зв'язку та потенційних

загроз несанкціонованого доступу. Реалізація цього принципу передбачає використання комплексних засобів захисту інформації, включаючи криптографічні методи (рис. 1.2), механізми автентифікації користувачів, сегментацію мережі, а також впровадження віртуальних приватних мереж для захищеної передачі даних між віддаленими підрозділами (рис. 1.3).



Симетричні криптосистеми.

У симетричних криптосистемах і для шифрування, і для дешифрування використовується один і той самий ключ. (Шифрування – перетворювальний процес. Оригінальний текст, який носить також назву відкритого тексту, замінюється шифрованим текстом, дешифрування – зворотний шифруванню процес. На основі ключа шифрований текст перетворюється у початковий);



Криптосистеми з відкритим ключем.

У системах з відкритим ключем використовуються два ключі – відкритий і закритий, які математично пов'язані один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний всім бажаним, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення.



Електронний підпис.

Системою електронного підпису називається його криптографічне перетворення, що приєднуються до тексту і дозволяє при отриманні його іншим користувачем перевірити авторство і достовірність повідомлення.



Управління ключами.

Це процес системи обробки інформації, який полягає в складанні та розподілі ключів між користувачами.

Основні напрямки використання криптографічних методів – передача конфіденційної інформації по каналах зв'язку (наприклад, електронна пошта), встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді.

Рисунок 1.2 – Криптографічні методи захисту [4]

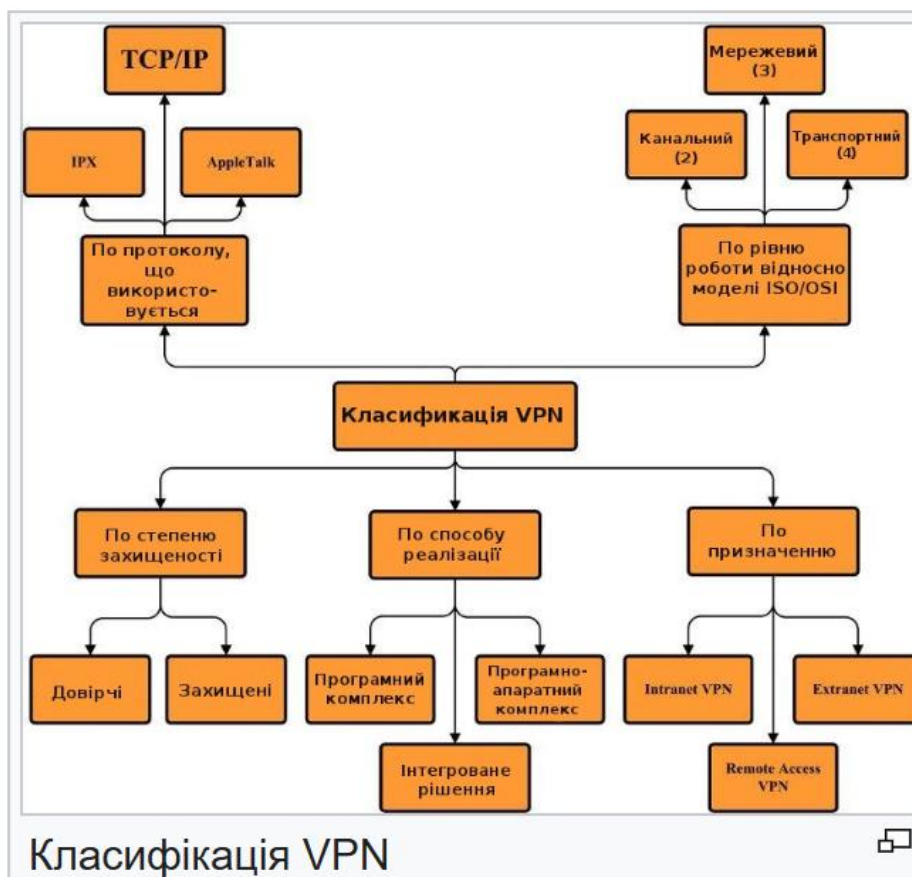


Рисунок 1.3 – Криптографічні методи захисту [5]

Важливим також є принцип ефективного управління трафіком, який спрямований на оптимізацію використання мережевих ресурсів та забезпечення стабільної якості обслуговування. Він реалізується шляхом пріоритезації трафіку, балансування навантаження та використання механізмів контролю пропускної здатності каналів зв'язку. Це дозволяє забезпечити належний рівень продуктивності навіть за умов високого навантаження на мережу.

Таким чином, побудова розподілених мереж підприємств ґрунтується на комплексі взаємопов'язаних принципів, які забезпечують їхню ефективність, надійність та безпеку. Дотримання цих принципів є необхідною умовою створення сучасної корпоративної інфраструктури, здатної підтримувати стабільне функціонування інформаційних систем у динамічних умовах розвитку інформаційних технологій.

1.3 Технології віртуальних приватних мереж (VPN), їх види та призначення

Технології віртуальних приватних мереж (Virtual Private Network, VPN) є одним із ключових інструментів забезпечення безпечної передачі даних у сучасних корпоративних інформаційних системах. Їх поява та розвиток були зумовлені необхідністю захищеної взаємодії між віддаленими сегментами мережі через потенційно небезпечні публічні канали зв'язку, зокрема Інтернет. VPN-технології дозволяють створювати логічно ізольовані канали комунікації, які функціонують поверх загальнодоступної інфраструктури, забезпечуючи при цьому конфіденційність, цілісність та автентичність переданих даних.

З технічної точки зору VPN являє собою сукупність методів і протоколів, що забезпечують формування захищеного тунелю між вузлами мережі. Основою такої взаємодії є процес інкапсуляції, під час якого пакети внутрішнього корпоративного трафіку поміщаються в інші пакети, придатні для передачі через зовнішню мережу. Додатково застосовуються криптографічні механізми, які гарантують шифрування інформації та захист від несанкціонованого доступу або модифікації даних під час їх передавання. Завдяки цьому VPN забезпечує рівень безпеки, наближений до захищених приватних каналів зв'язку, навіть при використанні відкритих мережесередовищ.

Призначення VPN-технологій у корпоративних мережах полягає насамперед у забезпеченні безпечної взаємодії між територіально розподіленими підрозділами підприємства. Це дозволяє організовувати єдиний інформаційний простір, у межах якого користувачі можуть отримувати доступ до спільних ресурсів незалежно від їх фізичного розташування. Крім того, VPN широко застосовується для організації віддаленого доступу співробітників до внутрішніх сервісів організації, що є особливо актуальним у контексті розвитку віддаленої роботи та мобільних робочих середовищ. Таким чином, VPN виступає як технологічна основа для побудови гнучких та масштабованих корпоративних інфраструктур.

Існує кілька основних типів VPN, які класифікуються залежно від архітектури підключення та способу організації захищеного каналу. Одним із

найпоширеніших є віддалений доступ VPN, який забезпечує індивідуальне підключення користувача до корпоративної мережі через захищений тунель (рис. 1.4). Такий підхід дозволяє працівникам отримувати доступ до внутрішніх ресурсів організації з будь-якої точки мережі Інтернет, зберігаючи при цьому високий рівень безпеки.



Рисунок 1.4 – Криптографічні методи захисту [6]

Іншим важливим типом є site-to-site VPN, який використовується для об'єднання двох або більше локальних мереж у єдину корпоративну інфраструктуру (рис. 1.5).

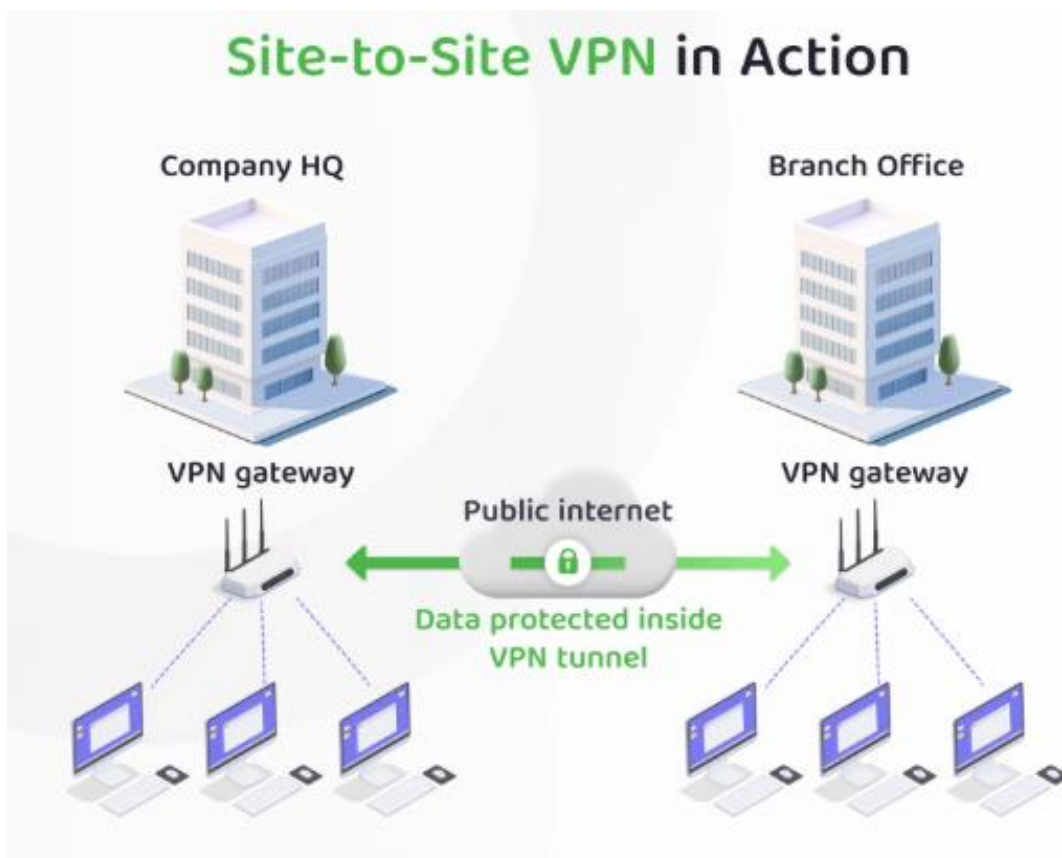


Рисунок 1.5 – Криптографічні методи захисту [7]

У цьому випадку VPN-з'єднання встановлюється між мережевими шлюзами або маршрутизаторами різних підрозділів організації, що дозволяє здійснювати прозору взаємодію між сегментами мережі без необхідності індивідуального підключення кожного користувача. Така модель є особливо ефективною для підприємств із розгалуженою філіальною структурою.

Окремо слід відзначити внутрішньомережеві VPN, які використовуються для сегментації корпоративної мережі та ізоляції окремих її частин з метою підвищення рівня безпеки та керованості. Вони дозволяють створювати логічні підмережі всередині єдиної інфраструктури, забезпечуючи контроль доступу та захист критичних ресурсів від несанкціонованого використання.

Таким чином, VPN-технології відіграють ключову роль у забезпеченні безпечної та ефективної взаємодії в сучасних корпоративних мережах. Вони поєднують у собі механізми тунелювання, шифрування та автентифікації, що дозволяє створювати захищені канали зв'язку поверх відкритих мережесередовищ. Завдяки своїй гнучкості та масштабованості VPN є невід'ємним елементом сучасних розподілених інформаційних систем підприємств.

1.4 Протоколи та методи забезпечення захищеного каналу зв'язку

Забезпечення захищеного каналу зв'язку в сучасних комп'ютерних мережах є одним із ключових завдань інформаційної безпеки, оскільки саме під час передачі даних через мережеві середовища виникає найбільша кількість потенційних загроз, пов'язаних із перехопленням, модифікацією або підміною інформації. У цьому контексті протоколи та методи захисту мережесередовищ формують комплексну систему механізмів, спрямованих на забезпечення конфіденційності, цілісності та автентичності даних, що передаються між вузлами мережі.

Однією з фундаментальних технологій, що застосовуються для захисту каналів зв'язку, є криптографічні протоколи транспортного рівня, серед яких особливе місце займає TLS (Transport Layer Security) [8]. Даний протокол забезпечує шифрування даних між клієнтом і сервером, використовуючи симетричні та асиметричні криптографічні алгоритми, а також механізми

цифрових сертифікатів для автентифікації сторін. У процесі встановлення захищеного з'єднання відбувається так званий TLS-handshake, під час якого узгоджуються параметри шифрування, здійснюється перевірка сертифікатів та формується спільний секретний ключ для подальшого обміну даними. Це дозволяє запобігти несанкціонованому доступу до інформації навіть у випадку перехоплення мережевого трафіку.

На мережевому рівні широкого застосування набув протокол IPsec (Internet Protocol Security) [9], який забезпечує захист безпосередньо IP-пакетів незалежно від прикладних сервісів. Його особливістю є можливість функціонування у двох основних режимах: транспортному та тунельному. У транспортному режимі захищається лише корисне навантаження пакета, тоді як у тунельному режимі весь IP-пакет інкапсулюється в новий пакет, що дозволяє створювати захищені VPN-з'єднання між мережевими вузлами або цілими мережами. IPsec використовує протоколи АН (Authentication Header) [10] та ESP (Encapsulating Security Payload) [11], які забезпечують автентифікацію, цілісність і шифрування даних, що передаються.

Важливу роль у забезпеченні захищеного каналу зв'язку відіграють також механізми автентифікації та керування ключами. До таких належать протоколи обміну ключами, зокрема Diffie–Hellman, який дозволяє сторонам сформувати спільний секретний ключ через відкритий канал без його безпосередньої передачі. Це значно підвищує рівень безпеки, оскільки навіть у разі перехоплення обміну злоумисник не має можливості відновити ключ шифрування. У сучасних реалізаціях цей механізм часто використовується у поєднанні з цифровими сертифікатами та інфраструктурою відкритих ключів (PKI), що забезпечує довіру до учасників мережевої взаємодії.

Окрім криптографічних протоколів, важливе значення мають методи багаторівневого захисту каналів зв'язку, які передбачають поєднання різних механізмів безпеки на різних рівнях мережевої моделі. Такий підхід включає використання міжмережевих екранів, систем виявлення та запобігання вторгненням, а також механізмів сегментації мережі. Завдяки цьому створюється

багатошарова система захисту, в якій навіть у разі компрометації одного з рівнів інші продовжують забезпечувати безпеку передавання даних.

Таким чином, протоколи та методи забезпечення захищеного каналу зв'язку формують комплексну інфраструктуру інформаційної безпеки, яка базується на поєднанні криптографічних алгоритмів, механізмів автентифікації та мережових засобів контролю. Їх використання є критично важливим для функціонування сучасних корпоративних мереж, особливо в умовах розподіленої архітектури та активного використання відкритих телекомунікаційних середовищ.

РОЗДІЛ 2

АНАЛІЗ ПІДПРИЄМСТВА «ОРІОН» ТА ВИМОГ ДО КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Загальна характеристика підприємства та його організаційної структури

Діяльність компанії орієнтована на створення конкурентоспроможних ІТ-рішень, підвищення ефективності роботи клієнтів та впровадження сучасних цифрових технологій у різні сфери діяльності (рис. 2.1). Це зумовлює необхідність побудови надійної, масштабованої та захищеної комп'ютерної мережі, яка забезпечує безперервний доступ до корпоративних ресурсів і стабільне функціонування всіх сервісів підприємства та віддаленого офісу. Компанія здійснює діяльність у сфері розробки сучасних програмних рішень для широкого кола замовників, включаючи підприємства малого бізнесу, великі корпорації, а також організації приватного і державного секторів. Фірма складається з відділів: продажі, розробки, адміністрація та віддалені працівники.



Рисунок 2.1 – Структурна схема підприємства

Відділ продажів спілкується з клієнтами, команда досліджень та розробок працює над проектами, адміністративний відділ обробляє конфіденційні дані співробітників, фінансові записи та комунікації в масштабах всієї компанії, віддалені працівники працюють з різних місць по всьому світу та потребують безпечних та ефективних рішень для віддаленого доступу.

Кожен відділ має унікальні потреби в безпеці та мережі, що відображають їхні різні ролі в організації. При проектуванні топології мережі створено логічний план усієї мережі, визначено розгляньте розміщення маршрутизаторів, комутаторів, брандмауерів та інших відповідних пристроїв, задокументовано за допомогою чіткої схеми IP-адресація та конфігурація VLAN, для кожного пристрою та сегмента визначено IP-адреси, впроваджено віртуальні локальні мережі (VLAN) для кожного відділу, задокументовано конфігурацію мережі.

Також при виконанні даного проєкту визначено шляхи маршрутизації для ефективного потоку даних, впроваджено списки контролю доступу (ACL) для кожного відділу. Для віддалених працівників налаштовано VPN.

2.2 Опис філіальної мережі та інформаційних потоків

Мережа підприємства побудована з метою забезпечення ефективної взаємодії між головним офісом та віддаленими підрозділами компанії. До складу мережевої інфраструктури входять центральний офіс у Луцьк, а також філія у Києві. Усі підрозділи об'єднані в єдину корпоративну мережу із використанням захищених каналів зв'язку та сучасних технологій маршрутизації й комутації.

Головний офіс виконує функції центрального вузла мережі, де розміщені основні серверні ресурси, системи зберігання даних, служби автентифікації користувачів, файлові сервіси та засоби моніторингу мережевої інфраструктури. Віддалені філії забезпечують доступ працівників до корпоративних ресурсів через захищені VPN-з'єднання, що дозволяє організувати безпечний обмін інформацією між підрозділами компанії.

Інформаційні потоки в мережі включають передачу службового трафіку, електронної пошти, даних корпоративних інформаційних систем, IP-телефонії,

відеоконференцій та доступу до хмарних сервісів. Для підвищення ефективності роботи мережі використовується сегментація трафіку за допомогою VLAN, що дозволяє розділити користувачів та сервіси відповідно до їх функціонального призначення.

Передача даних між філіями здійснюється через маршрутизатори та міжмережеві екрани із застосуванням механізмів шифрування й контролю доступу. Для забезпечення безперервності роботи мережі реалізовано резервування каналів зв'язку, автоматичне перенаправлення трафіку у випадку відмови окремих вузлів та системи резервного копіювання критично важливих даних.

Створена мережа забезпечує централізоване управління ресурсами підприємства, підвищує рівень інформаційної безпеки та дозволяє організувати стабільну взаємодію між усіма структурними підрозділами компанії.

2.3 Логічна структура мережі

Логічна структура корпоративної мережі підприємства побудована за ієрархічним принципом та включає рівень доступу, рівень розподілу і рівень ядра мережі. Такий підхід забезпечує ефективне управління трафіком, масштабованість мережевої інфраструктури та підвищення її надійності [12].

На рівні доступу розташовані комутатори, до яких підключаються робочі станції користувачів, принтери та інші мережеві пристрої. Для розмежування трафіку та підвищення безпеки мережі використовується технологія VLAN, що дозволяє логічно поділити мережу на окремі сегменти відповідно до функціонального призначення підрозділів підприємства. Зокрема, окремі VLAN виділені для адміністрації, відділу розробки, адміністративного відділу, демілітаризованої зони, в якій розміщені сервери.

Рівень розподілу виконує функції маршрутизації між VLAN, фільтрації трафіку та реалізації політик безпеки. На цьому рівні використовуються комутатори третього рівня та маршрутизатори, які забезпечують міжмережеву взаємодію, контроль доступу та оптимізацію передавання даних між сегментами мережі. Для динамічної маршрутизації застосовується протокол OSPF, який

дозволяє автоматично визначати оптимальні маршрути передачі пакетів між підрозділами підприємства та віддаленими філіями.

Рівень ядра мережі забезпечує високошвидкісну передачу даних між основними мережевими вузлами та серверною інфраструктурою. У центральному сегменті мережі розміщені сервери корпоративних сервісів, файлові сервери, а також системи моніторингу й резервного копіювання даних. Для захисту внутрішнього периметра мережі використовуються міжмереві екрани та системи контролю доступу.

Взаємодія між головним офісом у Луцьк та філією у Київ реалізована через захищені VPN-з'єднання. Це забезпечує безпечний обмін даними між підрозділами компанії та централізований доступ до корпоративних ресурсів.

Розроблена логічна структура мережі дозволяє забезпечити стабільну роботу інформаційної системи підприємства, ефективне управління мережевими ресурсами, високий рівень інформаційної безпеки та можливість подальшого масштабування мережевої інфраструктури.

В таблиці 2.1 подано IP-адресації відділів та нумерацію vlan.

Таблиця 2.1 – Таблиця IP-адресації відділів

Відділи	VLAN	IPv6 мережа	Маска мережі	Шлюз
Відділ продажів	2	172.16.1.0	255.255.255.0 (/24)	172.16.1.1
Відділ розробок	3	172.17.1.0	255.255.255.0 (/24)	172.17.1.1
Адміністративний відділ	4	172.18.1.0	255.255.255.0 (/24)	172.18.1.1
DMZ		172.22.1.0	255.255.255.0 (/24)	172.22.1.1
Віддалений офіс		172.19.1.0	255.255.255.0 (/24)	172.19.1.1

У наведеній таблиці 2.2 представлено IP-адресацію міжмаршрутизаторних з'єднань корпоративної мережі підприємства. Для організації WAN-з'єднань використано підмережі з маскою /30, що дозволяє ефективно використовувати адресний простір та забезпечує наявність двох робочих IP-адрес для кожного каналу зв'язку.

Така адресація є стандартною практикою для точкових з'єднань між маршрутизаторами, оскільки мінімізує витрати адресного простору, виділяючи лише необхідну кількість адрес для кожного каналу. Завдяки використанню масок /30 мережевий адміністратор може чітко ідентифікувати кожен

міжмаршрутизаторний канал як окрему підмережу, що спрощує діагностику та усунення несправностей у корпоративній мережі.

Таблиця 2.2 – Таблиця IP-адресації між маршрутизаторами

Мережа між проміжним мережевим обладнанням	IPv6 мережа	Маска мережі
ASA0_Nikitchuk–ISP1	75.12.1.0	255.255.255.252 (/30)
ISP1– Internet	76.12.1.0	255.255.255.252 (/30)
Internet –ISP2	77.12.1.0	255.255.255. 252 (/30)
ISP2–ASA1_Nikitchuk	78.12.1.0	255.255.255. 252 (/30)
ASA0_Nikitchuk–Multilayer2_Nikitchuk2	172.21.1.0	255.255.255.0 (/24)
ASA0_Nikitchuk– Multilayer1_Nikitchuk1	172.20.1.0	255.255.255.0 (/24)

У таблиці 2.3 наведено таблицю IP-адресації на портах для мережі з урахуванням міжмережових з'єднань.

Таблиця 2.3 – Таблиця IP-адресації на портах

Назва обладнання	Порт	IP адреса	
ASA0_Nikitchuk	Gig1/1	172.22.1.1	255.255.255.0 (/24)
	Gig1/2	75.12.1.1	255.255.255.252 (/30)
	Gig1/3	172.21.1.1	255.255.255.0 (/24)
	Gig1/4	172.20.1.1	255.255.255.0 (/24)
ISP1	Fa0/0	75.12.1.1	255.255.255.252 (/30)
	Fa0/1	76.12.1.1	255.255.255.0 (/24)
Internet	Fa0/0	76.12.1.2	255.255.255.0 (/24)
	Fa0/1	77.12.1.1	255.255.255.252 (/30)
ISP2	Fa0/0	77.12.1.2	255.255.255.252 (/30)
	Fa0/1	78.12.1.2	255.255.255.252 (/30)
ASA1_Nikitchuk	Gig1/1	78.12.1.1	255.255.255.252 (/30)
	Gig1/2	172.19.1.1	255.255.255.0 (/24)

2.4 Вимоги до захисту даних та мережевої безпеки

Вимоги до захисту даних та мережевої безпеки в корпоративній інформаційній системі визначають комплекс організаційних і технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів підприємства (рис. 2.2).

Першочерговою вимогою є забезпечення розмежування доступу до інформаційних ресурсів відповідно до ролей користувачів. Реалізується політика найменших привілеїв, яка передбачає надання користувачам лише тих прав доступу, що необхідні для виконання їх службових обов'язків. Для цього

застосовуються механізми централізованої автентифікації та авторизації, зокрема служби каталогів і контроль доступу на рівні мережевих пристроїв.

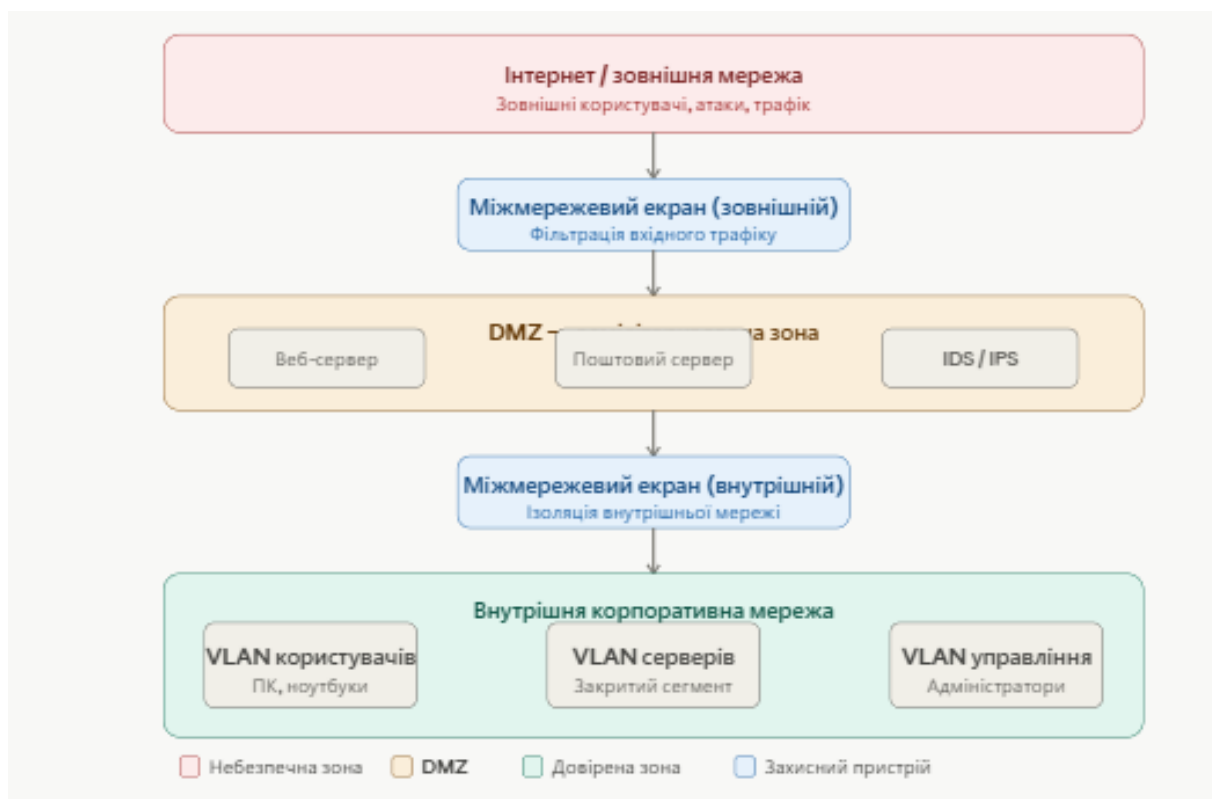


Рисунок 2.2 – Захисту даних та мережева безпека

Важливим елементом є захист мережевого периметра підприємства. Для цього використовуються міжмережеві екрани, системи виявлення та запобігання вторгненням, а також фільтрація трафіку на маршрутизаторах і комутаторах. Усі міжофісні з'єднання між підрозділами у Луцьк та Києві повинні бути захищені за допомогою VPN із використанням сучасних криптографічних протоколів.

Обов'язковою вимогою є сегментація мережі за допомогою VLAN, що дозволяє ізолювати критичні сервіси від користувацького трафіку та зменшити ризик поширення потенційних атак. Серверні ресурси повинні бути розміщені в окремому захищеному сегменті з обмеженим доступом.

Для захисту даних під час передачі застосовується шифрування трафіку, а також використання захищених протоколів (HTTPS, SSH, IPsec). Дані, що зберігаються на серверах, підлягають регулярному резервному копіюванню з можливістю швидкого відновлення у разі інцидентів або збоїв [13].

Додатково впроваджуються системи моніторингу (рис. 2.3) та журналювання подій, які дозволяють відстежувати підозрілу активність і своєчасно реагувати на інциденти безпеки. Усі мережеві пристрої повинні бути захищені від несанкціонованого доступу шляхом використання складних паролів, багатофакторної автентифікації та регулярного оновлення програмного забезпечення.

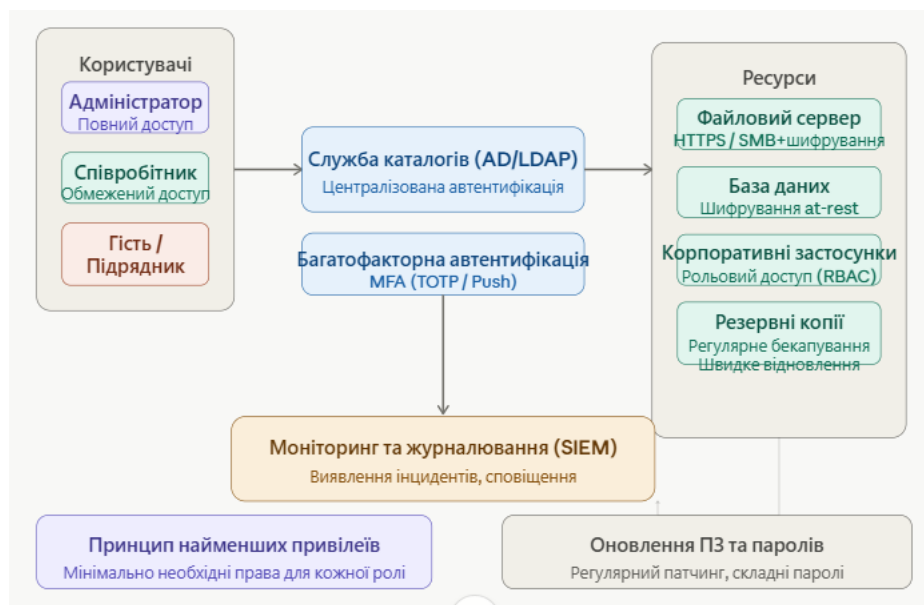


Рисунок 2.3 – Управління доступом

Таким чином, комплекс реалізованих вимог забезпечує високий рівень захищеності корпоративної мережі, мінімізує ризики витоку або втрати даних та гарантує стабільне функціонування інформаційної інфраструктури підприємства.

РОЗДІЛ 3

ПРАКТИЧНА РЕАЛІЗАЦІЯ ПОБУДОВИ МЕРЕЖІ

3.1 Створення та налаштування vlan на комутаторах та налаштування DHCP-сервера

У процесі проектування корпоративної мережі важливим етапом є логічна сегментація мережевої інфраструктури та автоматизація процесу адресації вузлів. Для реалізації використано технологію VLAN та протокол DHCP. Використання VLAN дозволяє розділити єдину фізичну мережу на декілька логічних сегментів, що забезпечує підвищення рівня безпеки, зменшення широкомовного трафіку та спрощення адміністрування мережі. DHCP-сервер, у свою чергу, забезпечує автоматичне призначення IP-адрес, масок підмережі, шлюзів та DNS-серверів для клієнтських пристроїв [14, 15].

У межах роботи реалізовано декілька VLAN для різних структурних підрозділів підприємства. На комутаторах Cisco створено відповідні віртуальні мережі та призначено порти доступу для підключення кінцевих пристроїв. Кожен порт комутатора прив'язаний до конкретної VLAN, що дозволило ізолювати трафік між підрозділами та забезпечити контроль доступу до ресурсів мережі (рис. 3.1-3.3).

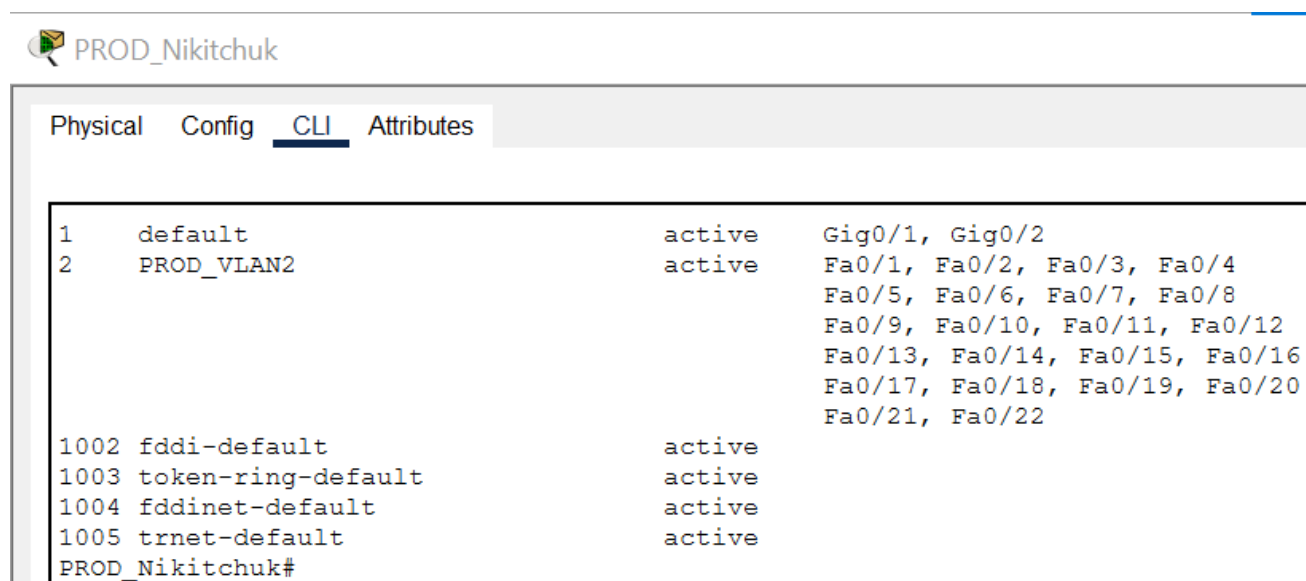


Рисунок 3.1 – Налаштування vlan на комутаторі PROD_Nikitchuk

ROZR_Nikitchuk

Physical Config CLI Attributes

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
3	ROZR_VLAN3	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

ROZR_Nikitchuk#
ROZR_Nikitchuk#

Рисунок 3.2 – Налаштування vlan на комутаторі ROZR_Nikitchuk

ADMIN_Nikitchuk

Physical Config CLI Attributes

VLAN	Name	Status	Ports
1	default	active	Fa0/23, Gig0/1, Gig0/2
4	ADMIN_VLAN4	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

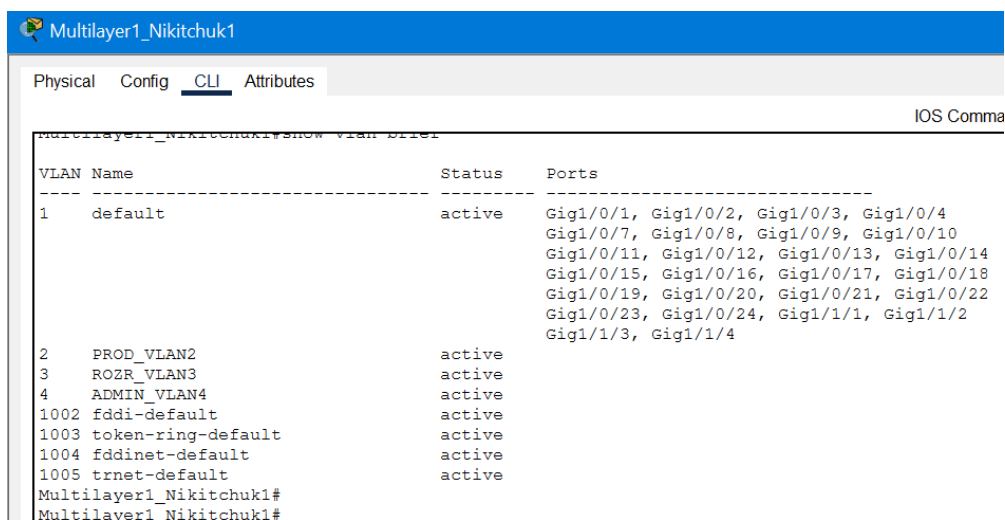
ADMIN_Nikitchuk#

Рисунок 3.3 – Налаштування vlan на комутаторі ADMIN_Nikitchuk

У сучасних корпоративних мережах комутатори третього рівня (Layer 3 Switches) поєднують функції комутації та маршрутизації, що дозволяє забезпечити ефективне керування мережевим трафіком між різними VLAN без використання окремого маршрутизатора. Використання L3-комутаторів підвищує продуктивність мережі, зменшує затримки передачі даних та спрощує структуру мережевої інфраструктури.

У процесі виконання роботи реалізовано налаштування VLAN на комутаторі третього рівня. Для логічного поділу мережі створено декілька VLAN, які відповідали структурним підрозділам підприємства. Після створення VLAN на комутаторі кожному порту призначено відповідний режим access та визначено належність до конкретної віртуальної мережі.

Для забезпечення маршрутизації між VLAN на L3-комутаторі створені віртуальні інтерфейси SVI (Switch Virtual Interface). Кожен SVI виконує роль шлюзу за замовчуванням для пристроїв певної VLAN та має власну IP-адресу. Завдяки цьому забезпечується передавання пакетів між різними сегментами мережі без використання зовнішнього маршрутизатора (рис. 3.4-3.5).



Multilayer1_Nikitchuk1

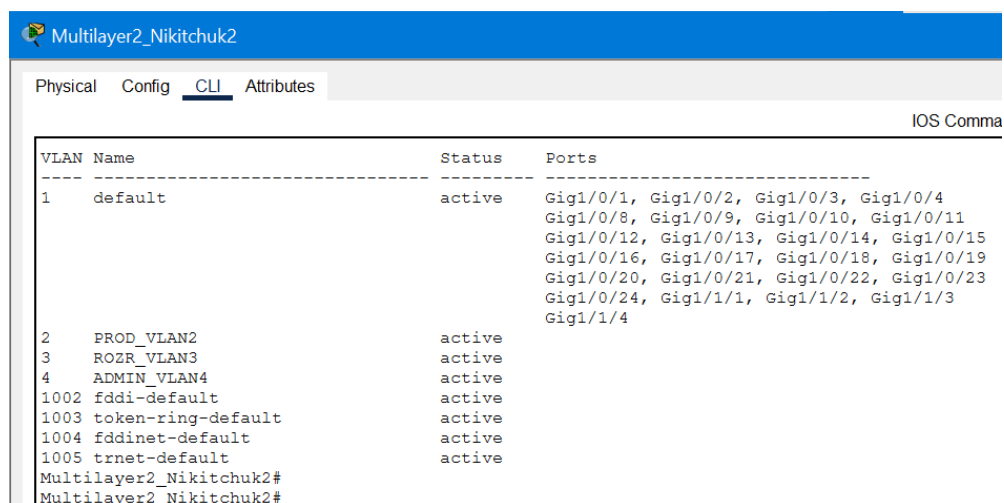
Physical Config **CLI** Attributes

Multilayer1_Nikitchuk1#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Gig1/0/1, Gig1/0/2, Gig1/0/3, Gig1/0/4 Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10 Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14 Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18 Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22 Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2 Gig1/1/3, Gig1/1/4
2	PROD_VLAN2	active	
3	ROZR_VLAN3	active	
4	ADMIN_VLAN4	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Multilayer1_Nikitchuk1#
Multilayer1_Nikitchuk1#

Рисунок 3.4 – Налаштування vlan на комутаторі Multilayer1_Nikitchuk1



Multilayer2_Nikitchuk2

Physical Config **CLI** Attributes

Multilayer2_Nikitchuk2#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Gig1/0/1, Gig1/0/2, Gig1/0/3, Gig1/0/4 Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11 Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15 Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19 Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23 Gig1/0/24, Gig1/1/1, Gig1/1/2, Gig1/1/3 Gig1/1/4
2	PROD_VLAN2	active	
3	ROZR_VLAN3	active	
4	ADMIN_VLAN4	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Multilayer2_Nikitchuk2#
Multilayer2_Nikitchuk2#

Рисунок 3.5 – Налаштування vlan на комутаторі Multilayer2_Nikitchuk2

Для забезпечення взаємодії між комутаторами налаштовано trunk-з'єднання. Trunk-порти використовують технологію IEEE 802.1Q для передачі трафіку декількох VLAN через один фізичний канал зв'язку. Це дозволяє зменшити кількість необхідних кабельних з'єднань та забезпечує централізовану передачу мережевого трафіку між мережевими пристроями.

Для автоматичного призначення мережевих параметрів налаштовано DHCP-сервер (рис. 3.6). Для кожної VLAN створювався окремий DHCP-пул, у якому визначались параметри мережі, зокрема IP-адресний простір, маска підмережі, адреса шлюзу та DNS-сервера. Після підключення клієнтських пристроїв до мережі вони автоматично отримують необхідні параметри конфігурації без потреби ручного налаштування.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
VLAN4_ADMIN_N...	172.18.1.1	172.22.1.2	172.18.1.0	255.255.25...	256	0.0.0.0	0.0.0.0
VLAN3_ROZR_Ni...	172.17.1.1	172.22.1.2	172.17.1.0	255.255.25...	256	0.0.0.0	0.0.0.0
VLAN2_PROD_Ni...	172.16.1.1	172.22.1.2	172.16.1.0	255.255.25...	256	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.22.1.0	255.255.25...	512	0.0.0.0	0.0.0.0

Рисунок 3.6 – Налаштування DHCP-сервера

Таким чином, реалізація VLAN та DHCP у корпоративній мережі дозволила підвищити рівень керованості мережі, забезпечити логічне розмежування користувачів та автоматизувати процес конфігурації мережевих пристроїв.

3.2 Налаштування протоколу HSRP

HSRP (Hot Standby Router Protocol) – це протокол резервування шлюзу за замовчуванням, розроблений компанією Cisco Systems для забезпечення відмовостійкості комп'ютерних мереж. Даний протокол використовується в мережесхемних інфраструктурах з метою підвищення надійності маршрутизації та мінімізації часу простою у випадку відмови основного маршрутизатора [16].

Принцип роботи HSRP базується на створенні віртуального маршрутизатора, який має спільну IP-адресу та MAC-адресу. У межах групи HSRP один із маршрутизаторів виконує роль активного (Active Router) та здійснює обробку мережевого трафіку, тоді як інший маршрутизатор перебуває у резервному стані (Standby Router). У разі виходу з ладу активного маршрутизатора резервний пристрій автоматично перебирає на себе його функції, що забезпечує безперервність мережевого з'єднання для кінцевих користувачів.

Використання HSRP дозволяє реалізувати механізми високої доступності мережі, знизити ризик втрати зв'язку та забезпечити стабільність роботи корпоративних інформаційних систем. Протокол підтримує автоматичне визначення стану маршрутизаторів шляхом обміну службовими повідомленнями між пристроями групи. Для вибору активного маршрутизатора використовується параметр пріоритету, відповідно до якого пристрій з вищим значенням пріоритету отримує статус основного.

HSRP широко застосовується у корпоративних мережах, дата-центрах та мережах підприємств, де критично важливим є забезпечення безперервного доступу до мережесхемних ресурсів. Завдяки використанню механізмів резервування протокол дозволяє підвищити рівень надійності функціонування мережевої інфраструктури та забезпечити ефективне реагування на відмови мережевого обладнання.

HSRP є невід'ємною складовою сучасних відмовостійких мережесхемних рішень, оскільки забезпечує автоматичне перемикавання трафіку на резервний маршрутизатор без втручання адміністратора та практично без перерви в обслуговуванні кінцевих користувачів. Впровадження даного протоколу в

корпоративній мережі підприємства дозволяє досягти високого рівня доступності мережевих сервісів та відповідати сучасним вимогам щодо показників SLA та безперервності бізнес-процесів.

3.3 Налаштування списків контролю доступу

Списки контролю доступу (ACL, Access Control Lists) – це механізм мережевої безпеки, який використовується для фільтрації мережевого трафіку та контролю доступу до ресурсів мережі. ACL дозволяють визначати правила, за якими мережеві пакети можуть бути дозволені або заборонені залежно від IP-адреси джерела, адреси призначення, типу протоколу чи номера порту [17].

Основним призначенням списків контролю доступу є підвищення рівня безпеки комп'ютерної мережі, обмеження несанкціонованого доступу, а також оптимізація передачі даних шляхом фільтрації небажаного трафіку. ACL широко застосовуються на маршрутизаторах і комутаторах для реалізації політик безпеки в корпоративних мережах.

Розрізняють стандартні та розширені ACL. Стандартні списки контролю доступу здійснюють фільтрацію лише за IP-адресою джерела, тоді як розширені ACL дозволяють враховувати додаткові параметри, зокрема IP-адресу призначення, транспортні протоколи TCP або UDP, а також порти прикладних сервісів.

На рисунку 3.7 зображено налаштовані списки контролю доступу.

```
access-list INSIDE-OUTSIDE extended permit tcp any any eq www
access-list INSIDE-OUTSIDE extended permit udp any any eq domain
access-list INSIDE-OUTSIDE extended permit tcp any any eq domain
access-list INSIDE-OUTSIDE extended permit udp any any eq bootps
access-list INSIDE-OUTSIDE extended permit udp any any eq bootpc
access-list INSIDE-OUTSIDE extended permit icmp any any
access-list INSIDE-OUTSIDE extended permit tcp any any eq ftp
access-list INSIDE-OUTSIDE extended permit tcp any any eq 20
access-list INSIDE-OUTSIDE extended permit tcp any any eq 443
access-list INSIDE-DMZ extended permit icmp any any
access-list INSIDE-DMZ extended permit tcp any any eq www
access-list INSIDE-DMZ extended permit udp any any eq domain
access-list INSIDE-DMZ extended permit tcp any any eq domain
access-list INSIDE-DMZ extended permit udp any any eq bootps
access-list INSIDE-DMZ extended permit udp any any eq bootpc
access-list INSIDE-DMZ extended permit tcp any any eq ftp
access-list INSIDE-DMZ extended permit tcp any any eq 20
access-list INSIDE-DMZ extended permit tcp any any eq 443
```

Рисунок 3.7 – Налаштування ACL

3.4 Налаштування маршрутизації з використання протоколу OSPF

За замовчуванням пристрої, що знаходяться в різних VLAN, не можуть обмінюватися даними, тому необхідно налаштовувати протоколи, які забезпечують їхню взаємодію. При налаштуванні використано SVI як протокол для маршрутизації між VLAN. Цей підхід застосовано до всіх комутаторів ядра шляхом створення інтерфейсів VLAN, призначення їм IP-адрес та інкапсуляції Vlan ID для покращення процесу. Спочатку налаштовано інтерфейси на брандмауері ASA0_Nikitchuk (рис. 3.8).

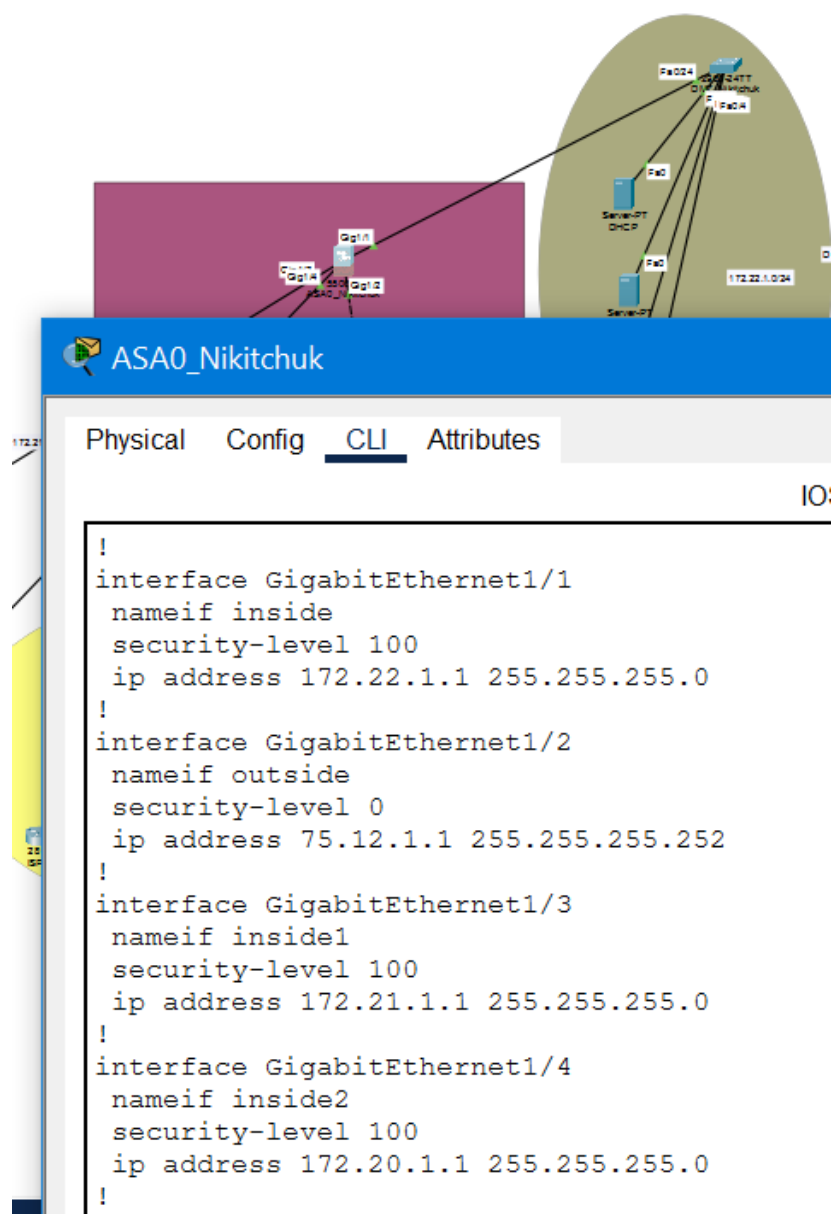


Рисунок 3.8 – Налаштування інтерфейсів на брандмауері ASA0_Nikitchuk

Далі налаштовується протокол маршрутизації ospf на брандмауері ASA0_Nikitchuk, перетворення внутрішніх адрес в зовнішні та маршруту за замовчуванням (рис. 3.9-3.11).

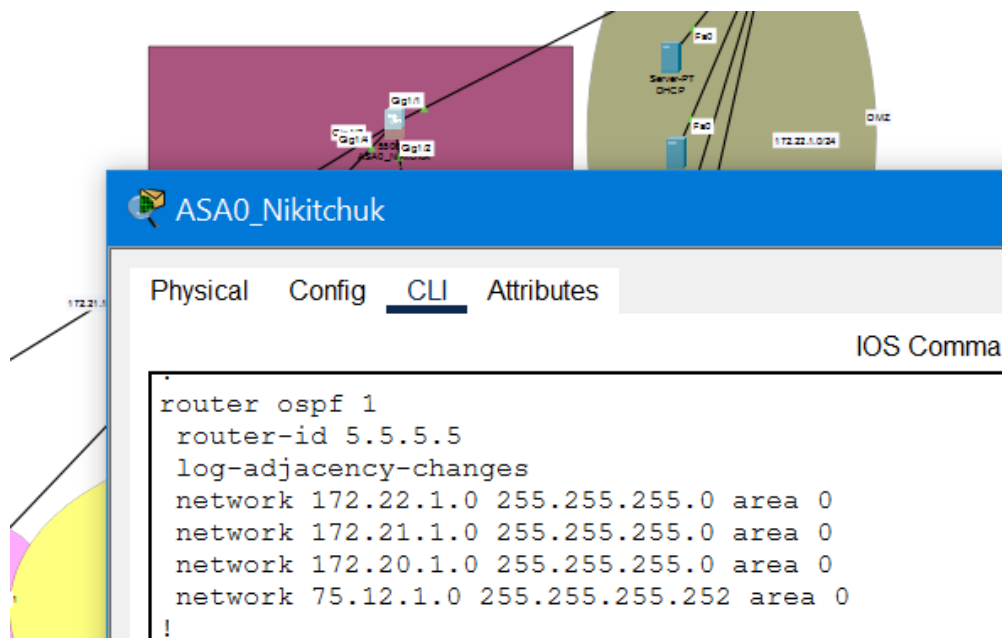


Рисунок 3.9 – Налаштування маршрутизації на брандмауері ASA0_Nikitchuk

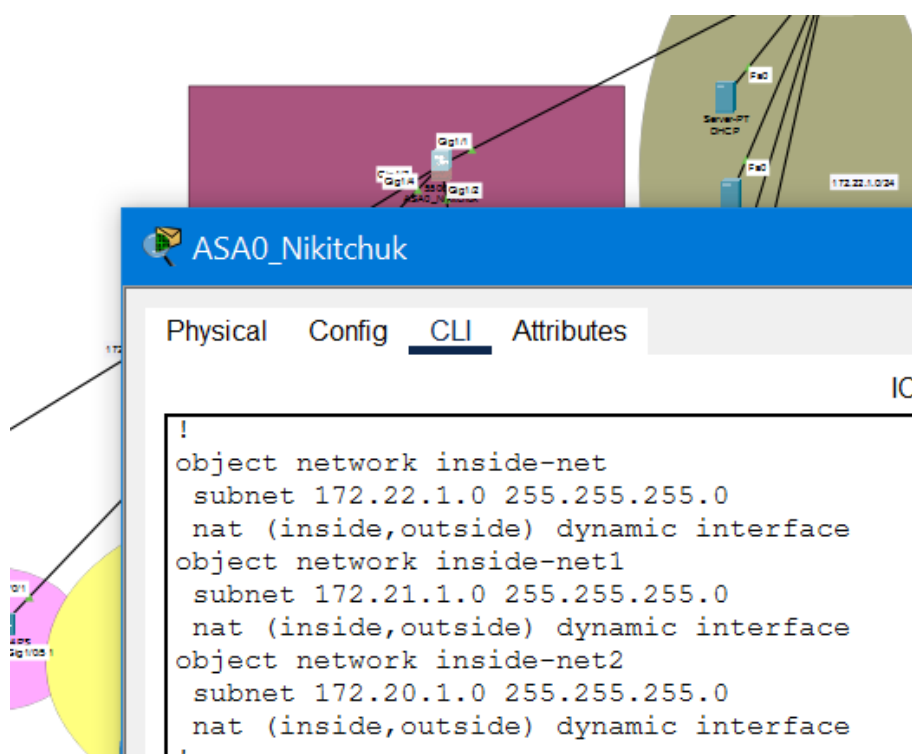


Рисунок 3.10 – Налаштування перетворення внутрішніх адрес в зовнішні на брандмауері ASA0_Nikitchuk

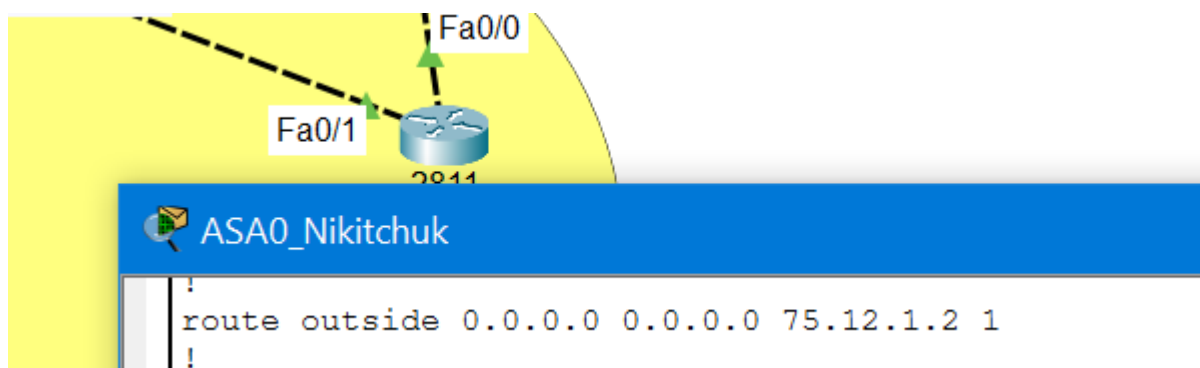


Рисунок 3.11 – Налаштування маршруту за замовчуванням на брандмауері ASA0_Nikitchuk

Маршрутизатори провайдера виконують роль ядра зовнішньої мережі та забезпечує обмін маршрутною інформацією між автономною системою провайдера та корпоративною мережею підприємства. Для забезпечення коректної маршрутизації налаштовано процес OSPF, визначено ідентифікатор процесу та налаштовано оголошення мереж у відповідній області.

На маршрутизаторі провайдера активовано протокол OSPF із визначенням process ID, після чого додано мережеві сегменти, які беруть участь у маршрутизації. Всі інтерфейси, що підключені до внутрішніх або транзитних мереж, включені до області backbone (area 0), що відповідає стандартній практиці побудови ієрархічних OSPF-мереж (рис. 3.12-3.14).

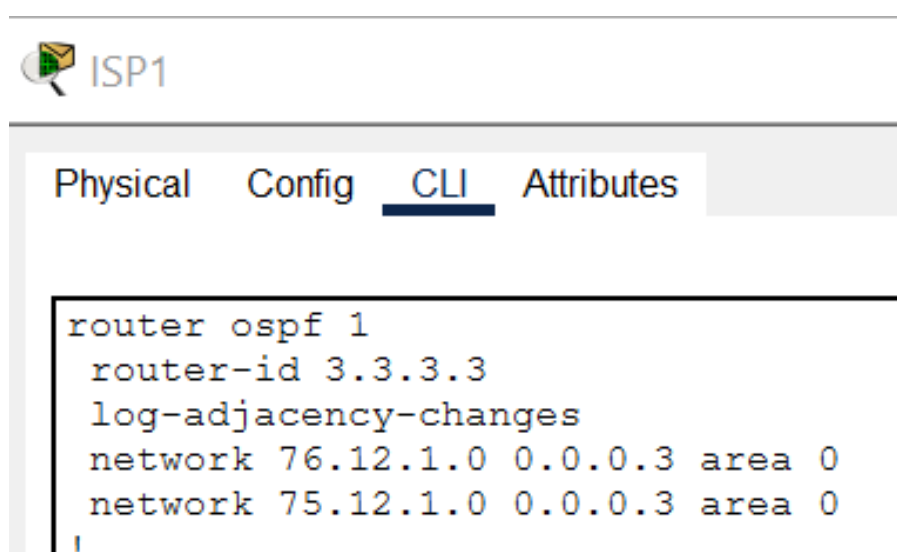


Рисунок 3.12 – Налаштування маршрутизації на маршрутизаторі ISP1

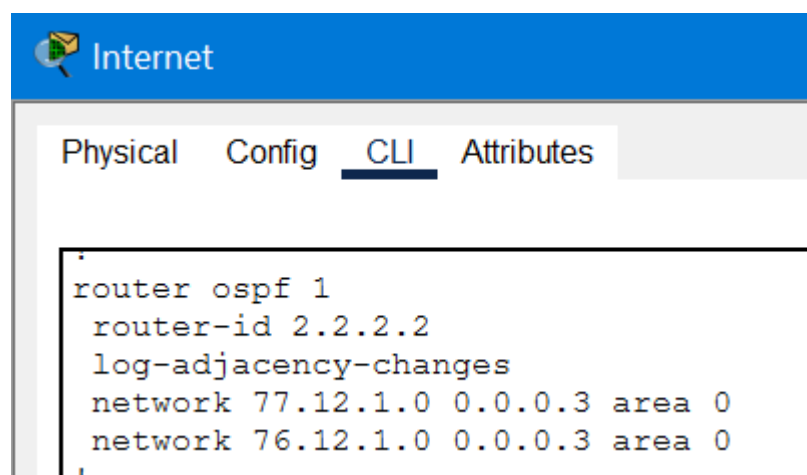


Рисунок 3.13 – Налаштування маршрутизації на маршрутизаторі Internet

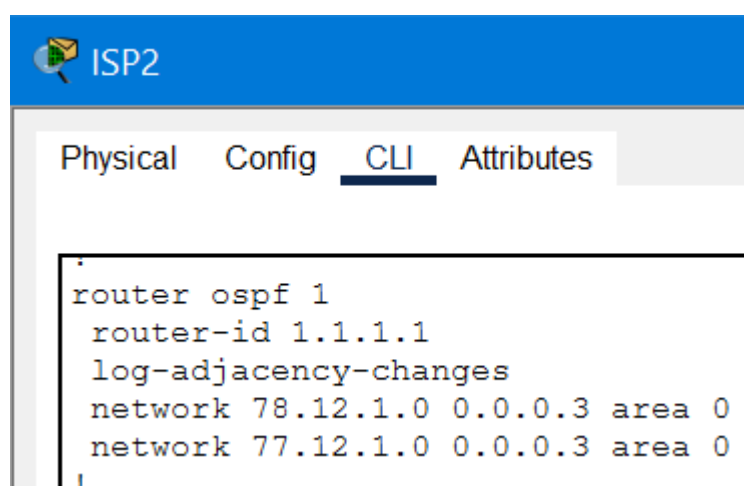


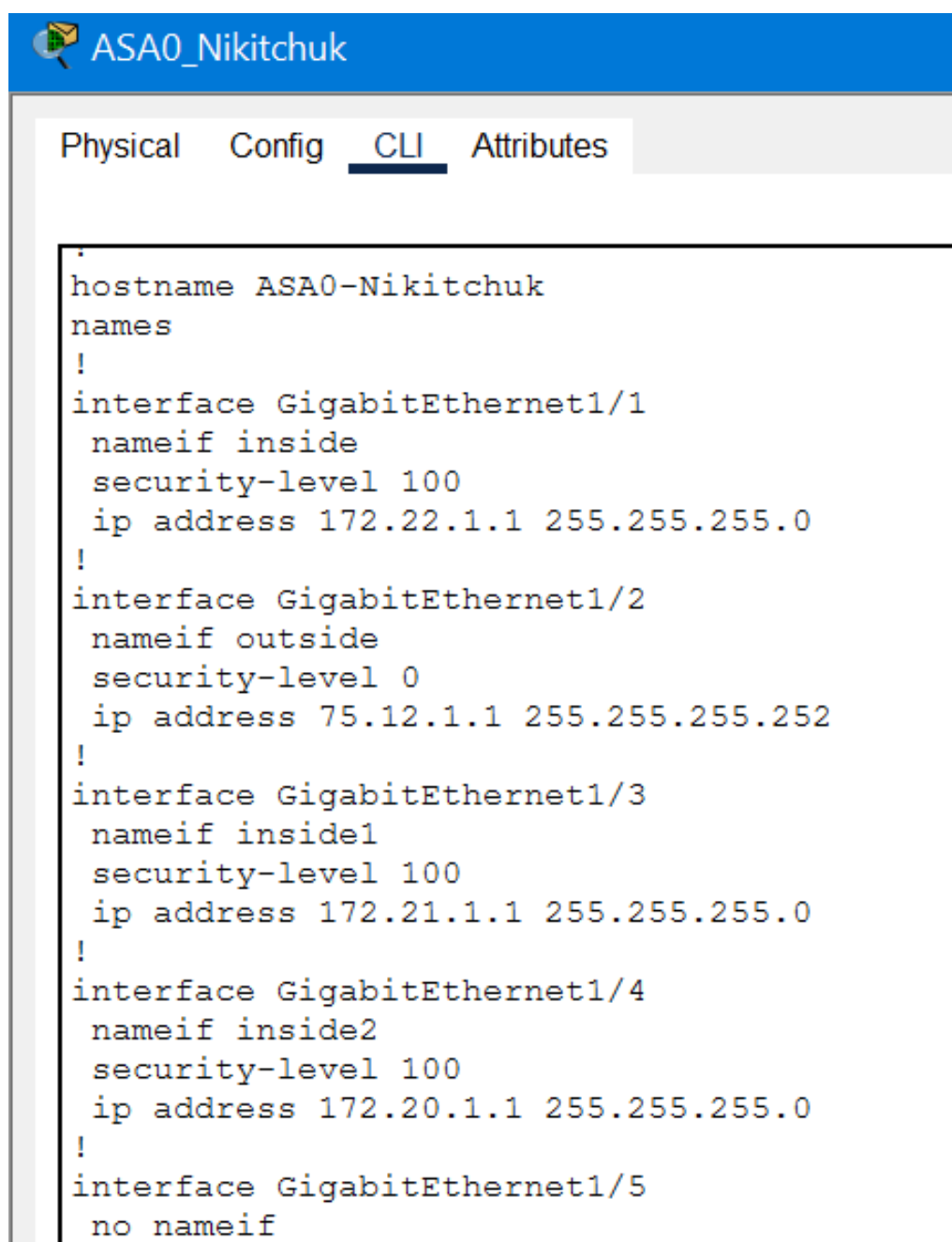
Рисунок 3.14 – Налаштування маршрутизації на маршрутизаторі ISP2

У сучасних корпоративних мережах міжмережевий екран Cisco ASA (Adaptive Security Appliance) використовується для забезпечення захисту внутрішнього периметра мережі та контролю доступу між внутрішніми й зовнішніми сегментами. Одним із базових етапів конфігурації є визначення ролей інтерфейсів, зокрема внутрішнього (inside) та зовнішнього (outside), що дозволяє реалізувати політику безпеки та механізми NAT.

Інтерфейс inside призначений для підключення внутрішньої корпоративної мережі, яка є довіреною зоною. Інтерфейс outside, у свою чергу, підключається до зовнішньої мережі провайдера або Інтернету та вважається недовірим середовищем. Рівень довіри (security level) для inside зазвичай встановлюється на

значення 100, тоді як для outside – на значення 0, що визначає пріоритетність трафіку та правила його фільтрації.

На початковому етапі виконується базове налаштування інтерфейсів ASA, включаючи призначення IP-адрес та визначення їх ролей у мережевій архітектурі. Далі налаштовується зовнішній інтерфейс outside, який забезпечує підключення до провайдера або маршрутизатора зовнішньої мережі (рис. 3.15-3.16).



```
ASA0_Nikitchuk
Physical  Config  CLI  Attributes
hostname ASA0-Nikitchuk
names
!
interface GigabitEthernet1/1
  nameif inside
  security-level 100
  ip address 172.22.1.1 255.255.255.0
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 75.12.1.1 255.255.255.252
!
interface GigabitEthernet1/3
  nameif inside1
  security-level 100
  ip address 172.21.1.1 255.255.255.0
!
interface GigabitEthernet1/4
  nameif inside2
  security-level 100
  ip address 172.20.1.1 255.255.255.0
!
interface GigabitEthernet1/5
  no nameif
```

Рисунок 3.15 – Налаштування інтерфейсів на брандмауері ASA0_Nikitchuk

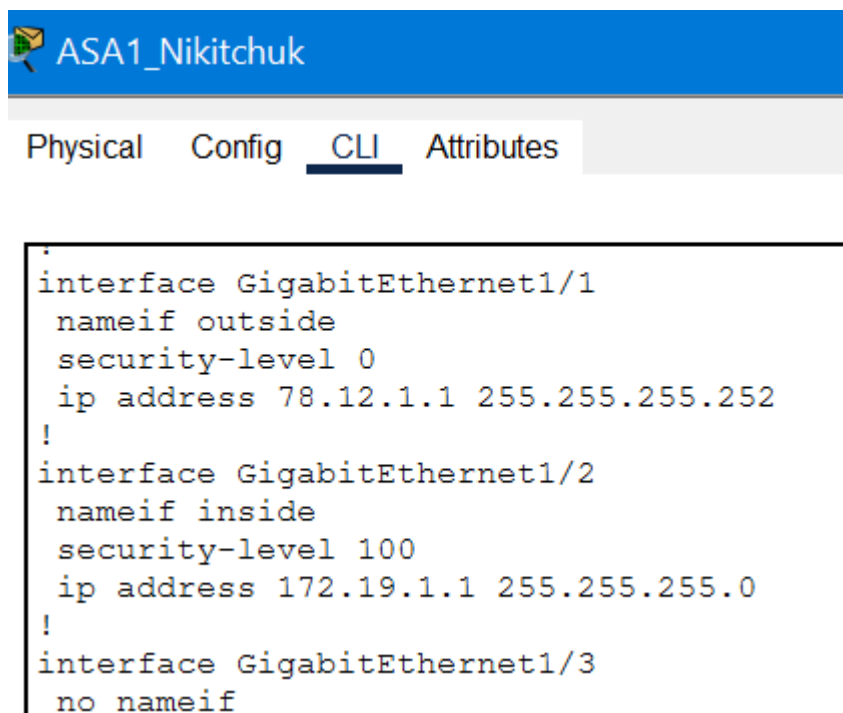


Рисунок 3.16 – Налаштування інтерфейсів на брандмауері ASA0_Nikitchuk

Між inside та outside інтерфейсами налаштовано NAT (Network Address Translation), що дозволяє внутрішнім вузлам отримувати доступ до зовнішніх ресурсів із використанням однієї публічної IP-адреси. За замовчуванням Cisco ASA дозволяє трафік із більш високого рівня безпеки (inside) до нижчого (outside), однак зворотний доступ блокується без явних правил доступу або NAT-конфігурації.

Налаштування inside та outside інтерфейсів на Cisco ASA дозволило реалізувати базову модель захищеного периметра мережі, забезпечити сегментацію трафіку та контроль доступу між внутрішньою корпоративною мережею та зовнішніми ресурсами.

3.5 Налаштування VPN

IPSec VPN (Internet Protocol Security Virtual Private Network) – це технологія створення захищених віртуальних приватних мереж, яка забезпечує конфіденційність, цілісність та автентичність даних під час їх передавання через незахищені мережі, зокрема мережу Інтернет. IPSec функціонує на мережевому

рівні моделі OSI та використовує криптографічні алгоритми для шифрування мережевого трафіку [18-20].

Налаштування IPSec VPN передбачає створення захищеного тунелю між двома мережевими пристроями, наприклад маршрутизаторами або міжмережевими екранами. Процес конфігурації включає визначення політик безпеки, вибір алгоритмів шифрування та автентифікації, створення криптографічних ключів і налаштування параметрів тунелю.

Робота IPSec VPN здійснюється у два основні етапи. На першому етапі за допомогою протоколу IKE (Internet Key Exchange) встановлюється захищений канал для обміну ключами та автентифікації сторін. На другому етапі формується IPSec-тунель, через який передається зашифрований трафік між мережами.

Для забезпечення захисту даних IPSec використовує протоколи АН (Authentication Header) та ESP (Encapsulating Security Payload). Протокол АН забезпечує автентифікацію та контроль цілісності даних, тоді як ESP додатково підтримує шифрування трафіку, що робить його найбільш поширеним у сучасних VPN-рішеннях.

У мережевому обладнанні Cisco Systems налаштування IPSec VPN виконується через створення ISAKMP-політик, ACL для визначення цікавого трафіку, трансформаційних наборів та криптографічних карт, які застосовуються до мережевих інтерфейсів. IPSec VPN широко використовується для безпечного з'єднання віддалених офісів, організації віддаленого доступу працівників та захисту корпоративного трафіку.

При успішному встановленні IPSec-тунелю міжмережеві екрани забезпечують шифрування трафіку між локальними мережами, що підвищує рівень конфіденційності та захисту корпоративної інформації під час передачі даних через зовнішні мережі. Налаштування обладнання подано в додатках А та Б.

Використання IPSec-тунелів між філіями підприємства дозволяє організувати захищений канал зв'язку, що відповідає сучасним стандартам інформаційної безпеки та забезпечує цілісність і автентичність даних, що передаються. Такий підхід до побудови захищеної корпоративної мережі є економічно доцільним рішенням, оскільки дозволяє використовувати існуючу

публічну мережеву інфраструктуру для організації приватних захищених з'єднань між віддаленими об'єктами підприємства.

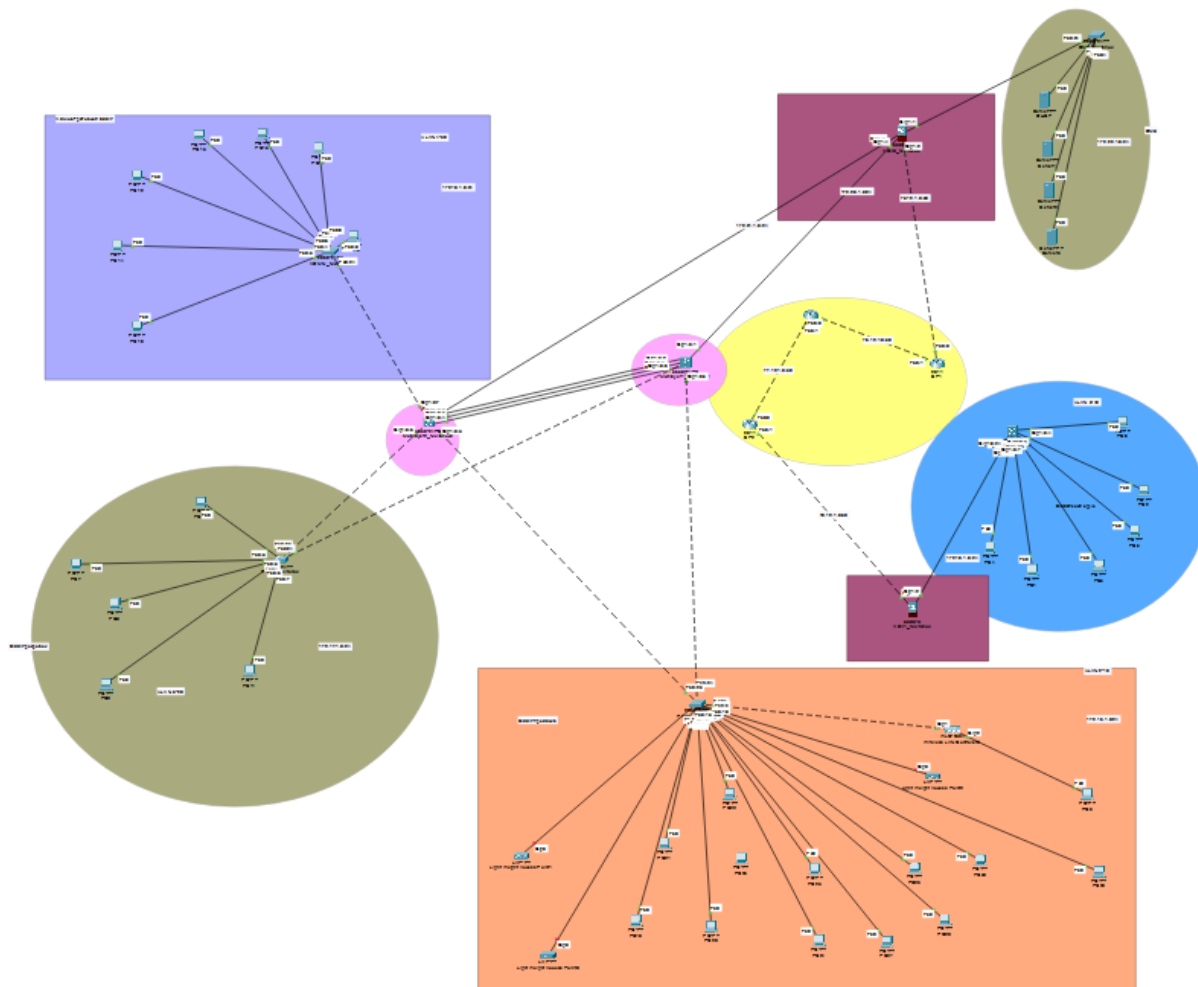


Рисунок 3.17 – Спроектована мережа підприємства

В результаті спроектована мережа забезпечує конфіденційність, цілісність та доступність корпоративних даних при передачі між вузлами розподіленої інфраструктури підприємства.

ВИСНОВКИ

У результаті виконання проєкту спроектовано та реалізовано корпоративну комп'ютерну мережу, що забезпечує ефективну взаємодію між центральним офісом та філією підприємства. Розроблена топологія характеризується ієрархічною побудовою, що сприяє підвищенню масштабованості та надійності системи.

Встановлено, що технологія VPN залишається фундаментальним інструментом забезпечення захищеної міжфілійної взаємодії, оскільки поєднує економічну доступність з високим рівнем конфіденційності та цілісності даних. Визначено, що ринок корпоративних VPN-рішень демонструє стаłe зростання, зумовлене розширенням практики дистанційної роботи та потребою у захисті корпоративного трафіку в умовах зростання кіберзагроз.

Дослідження основних протоколів та стандартів VPN дозволило обґрунтувати вибір оптимального протоколу для корпоративного середовища підприємства. За критеріями безпеки, продуктивності, масштабованості та простоти адміністрування як основний протокол обрано IPsec у режимі site-to-site для з'єднання філії, що забезпечує шифрування трафіку на мережевому рівні без зниження пропускної здатності каналів.

Розроблено топологію корпоративної мережі підприємства, яка включає центральний офіс та відокремлену філію. Така архітектура забезпечує централізоване управління мережею, спрощує адміністрування та дозволяє ефективно контролювати трафік між усіма вузлами. Для філії спроектовано окрему локальну мережу, де виконує функція VPN-шлюзу та міжмережевого екрана. Запропонована топологія відповідає вимогам відмовостійкості та дозволяє нарощувати кількість філій без суттєвої реструктуризації наявної інфраструктури.

Спроектовано адресний простір корпоративної мережі підприємства на основі приватних діапазонів IPv4 відповідно до RFC 1918. Для центрального офісу та кожної філії виділено окремі підмережі з маскою /24, що забезпечує достатній простір для підключення робочих станцій, серверів та мережевого обладнання.

Налаштовано маршрутизацію між підмережами через VPN-тунелі та визначено вимоги до мережевого обладнання.

Розроблено та налаштовано VPN-тунель між філією підприємства на основі протоколу IPsec у режимі тунелювання. Тестування мережі підтвердило забезпечення конфіденційності, цілісності та автентичності корпоративних даних при передачі між усіма вузлами мережі.

Сформульовано комплекс рекомендацій щодо політики інформаційної безпеки та адміністрування спроектованої мережної інфраструктури підприємства.

Розроблений проєкт корпоративної мережі підприємства із застосуванням технології VPN забезпечує надійний захищений зв'язок між філіями, відповідає сучасним вимогам інформаційної безпеки. Запропоновані рішення мають практичну цінність і можуть слугувати основою для проектування аналогічних мережних інфраструктур інших підприємств із розподіленою організаційною структурою.

Таким чином, поставлені завдання щодо проектування корпоративної мережі виконано повністю, а отримані результати можуть бути використані як основа для впровадження мережевої інфраструктури.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Загальні принципи побудови корпоративної мережі. StudFiles. URL: <https://studfile.net/preview/5470625/> (дата звернення: 23.02.2026).
2. Структура корпоративної мережі. Основні сегменти мережі. Презентації українською мовою. URL: <https://svitppt.com.ua/informatika/struktura-korporativnoi-merezhi-osnovni-segmenti-merezhi.html> (дата звернення: 25.02.2026).
3. Державна служба спеціального зв'язку та захисту інформації України. Access Denied. URL: <https://cip.gov.ua/ua/faqs/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis> (дата звернення: 05.03.2026).
4. Цифровий посібник з інформатики 2.4 Криптографічні методи захисту інформації. Surl.lt short link service from Surli. URL: <https://surl.lt/qxxjww> (дата звернення: 07.03.2026).
5. Учасники проєктів Вікімедіа. VPN – Вікіпедія. Вікіпедія. URL: <https://uk.wikipedia.org/wiki/VPN> (дата звернення: 08.03.2026).
6. Як налаштувати підключення VPN в роутерах Cudy? Мережеві рішення: маршрутизатори, WiFi роутери, комутатори, точки доступу, репітери. URL: <https://cudy.com.ua/yak-nalashtuvaty-pidklyuchennya-vpn-v-routerah-cudy/> (дата звернення: 13.03.2026).
7. What Is a Site-to-Site VPN? Setup, Benefits and How It Works. PIA. URL: <https://www.privateinternetaccess.com/blog/site-to-site-vpn/> (date of access: 15.03.2026).
8. TLS протокол. URL: <https://cityhost.ua/uk/blog/scho-take-protokol-tls-yak-vin-pracyu-ta-vid-chogo-zahischa.html> (дата звернення: 20.03.2026).
9. Що таке IPsec? Терміни та визначення кібербезпеки. KeepSolid VPN Unlimited. URL: <https://surli.cc/iwyzcm> (дата звернення: 24.03.2026).
10. AH and ESP protocols. IBM. URL: <https://surli.li/ljartk> (date of access: 24.03.2026).
11. What Is an IPsec Encapsulating Security Payload (ESP)?. JumpCloud. URL: <https://jumpcloud.com/it-index/what-is-an-ipsec-encapsulating-security-payload-esp> (date of access: 01.04.2026).

12. Логічна структуризація мережі. StudFiles. URL: <https://studfile.net/preview/7669189/page:6/> (дата звернення: 02.04.2026).
13. SSH, SSL, HTTPS, IPsec OSI model layer. XYZ NETWORK. URL: <https://xyznetwork.blogspot.com/2016/04/ssh-ssl-ipsec-osi-model-layer.html> (date of access: 03.04.2026).
14. DHCP – PortaOne Education Center. PortaOne Education Center – Навчальний центр PortaOne. URL: <https://education.portaone.com/dhcp/> (date of access: 07.04.2026).
15. Що таке DNS, як працює DNS-сервер та як прописати NS-сервери. Хостинг в Україні от Cityhost – лучший хостинг сайта. URL: <https://cityhost.ua/uk/blog/scho-take-dns-ta-yak-pracyu-sistema-domennih-imen.html> (дата звернення: 12.04.2026).
16. Naj Qazi. What is HSRP? | Overview & Configuration, 2022. YouTube. URL: <https://www.youtube.com/watch?v=hPb7Dc4S1wo> (date of access: 15.04.2026).
17. Etheridge E. Access Control List (ACL) in cyber security: Beneficial for all, critical for some. Data Privacy & Information Security DataGuard. URL: <https://www.dataguard.com/blog/acl-access-control-list/> (date of access: 20.04.2026).
18. Державна служба спеціального зв'язку та захисту інформації України. Access Denied. URL: <https://cip.gov.ua/ua/faqs/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis> (дата звернення: 25.04.2026).
19. Навіщо потрібен протокол захисту IPsec? Resit. Resit. URL: <https://resit.com.ua/navisho-potriben-ipsec-protokol/> (дата звернення: 27.04.2026).
20. NIST Technical Series Publications. URL: <https://surl.li/nhzqsh> (date of access: 28.04.2026).