ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ЛОКАЛЬНА КОМП'ЮТЕРНА МЕРЕЖА МАЛОГО ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ VLAN ТА СЕРВЕРНОЇ ІНФРАСТРУКТУРИ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Денис СЕМЕНЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-42
Денис СЕМЕНЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Віталій ВОЛОХІН
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Бакалавр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ
«_____» _____ 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Семененко Денис Юрійович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Локальна комп'ютерна мережа малого підприємства з використанням VLAN та серверної інфраструктури
керівник кваліфікаційної роботи Віталій ВОЛОХІН,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» 02 2026р. № 51
2. Строк подання кваліфікаційної роботи «08» 05 2026р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, методи системного аналізу, принципи IP-адресації та маршрутизації, математичний апарат, емпіричні методи

Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз технологій та архітектури сучасних локальних обчислювальних мереж малих підприємств
2. Розробка технічного та робочого проєкту локальної обчислювальної мережі підприємства з інтеграцією vlan та серверної інфраструктури
3. Проєктування логічної архітектури, налаштування сегментації vlan та програмна конфігурація активного мережевого обладнання
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «09» 02 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02-24.03.2026	Виконано
2	Обробка матеріалу	23.03-05.04.2026	Виконано
3	Розробка теоретичної частини	06.04-10.04.2026	Виконано
4	Розробка практичної частини	11.04-20.04.2026	Виконано
5	Висновки за результатами аналізу	21.04-06.05.2026	Виконано
6	Оформлення пояснювальної записки	07.05-08.05.2026	Виконано
7	Розробка презентації	09.05-11.05.2026	Виконано
8	Передзахист	27.05-29.05.2026	Виконано
9	Здача в деканат	02.06-05.06.2026	Виконано

Здобувач вищої освіти _____ Денис СЕМЕНЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій ВОЛОХІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 61 стор., 6 рис., 10 табл., 20 джерел.

Мета дослідження – розробка та проєктування відмовостійкої локальної обчислювальної мережі малого підприємства з використанням технології VLAN та інтеграцією серверної інфраструктури.

Об'єкт дослідження – локальна комп'ютерна мережа малого підприємства.

Предмет дослідження – архітектура, технології логічної сегментації та апаратно-програмні засоби побудови корпоративної локальної мережі.

Короткий зміст роботи: Сучасна локальна обчислювальна мережа вийшла за межі простого фізичного з'єднання комп'ютерів і є фундаментальним середовищем, що забезпечує безперервність бізнес-процесів та безпеку корпоративних даних. Історично малі підприємства часто будували мережі на базі некерованих комутаторів, що призводило до єдиного широкомовного домену, де будь-яка мережева аномалія могла паралізувати роботу всього офісу. Сучасний підхід вимагає впровадження логічної сегментації на базі керованих комутаторів рівня L2/L3.

У роботі проаналізовано існуючі мережеві топології та обґрунтовано вибір ієрархічної моделі «розширена зірка». На основі дослідження було розроблено технічний проєкт мережі для ПП «Веб-Інтеграція». Для забезпечення безпеки та оптимізації трафіку мережу було сегментовано на віртуальні підмережі відповідно до структури підприємства. Підібрано сучасне активне обладнання та серверну платформу. Працездатність розробленої логічної архітектури та налаштувань маршрутизації підтверджено шляхом імітаційного моделювання.

КЛЮЧОВІ СЛОВА: ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА, VLAN, МАРШРУТИЗАЦІЯ, КОМУТАТОР, СЕРВЕРНА ІНФРАСТРУКТУРА, CISCO, MIKROTIK, ТОПОЛОГІЯ МЕРЕЖІ, ВІДМОВОСТІЙКІСТЬ.

ABSTRACT

Textual part of the qualification work for the bachelor's degree: 61 pages, 6 figures, 10 tables, 20 sources.

The purpose of the work is the development and design of a fault-tolerant local area network for a small enterprise using VLAN technology and the integration of server infrastructure.The object of research is the local computer network of a small enterprise.The subject of research is the architecture, logical segmentation technologies, and hardware-software tools for building a corporate local area network.Brief summary of the work: A modern local area network has gone beyond a simple physical connection of computers and is a fundamental environment that ensures business continuity and corporate data security. Historically, small businesses often built networks based on unmanaged switches, leading to a single broadcast domain where any network anomaly could paralyze the entire office. The modern approach requires the implementation of logical segmentation based on managed L2/L3 switches.

The paper analyzes existing network topologies and justifies the choice of the hierarchical "extended star" model. Based on the research, a technical network project for the enterprise "Web-Integration" was developed. To ensure security and optimize traffic, the network was segmented into virtual local area networks according to the enterprise structure. Modern active equipment and a server platform were selected. The operability of the developed logical architecture and routing configurations was confirmed through simulation modeling.

KEYWORDS: LOCAL AREA NETWORK, VLAN, ROUTING, SWITCH, SERVER INFRASTRUCTURE, CISCO, MIKROTIK, NETWORK TOPOLOGY, FAULT TOLERANCE.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Семененко Д. Ю. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)
на тему: «Локальна комп'ютерна мережа малого підприємства з використанням VLAN та серверної інфраструктури».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Семененко Д. Ю. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Семененко Дениса Юрійовича на оцінку «відмінно», та присвоїти йому кваліфікацію «бакалавр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Віталій ВОЛОХІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«__» _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Семененко Д. Ю.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Семененко Денис Юрійович
(прізвище, ім'я, по батькові)
на тему: «Локальна комп'ютерна мережа малого підприємства з використанням VLAN та серверної інфраструктури»

Актуальність:

Бакалаврська кваліфікаційна робота присвячена одній із найактуальніших проблем розбудови IT-інфраструктури малого бізнесу — проєктуванню надійних, масштабованих та захищених локальних обчислювальних мереж. В умовах зростання обсягів корпоративних даних та підвищення вимог до безперервності бізнес-процесів, перехід від простих «плоских» мереж до сегментованих структур на базі керованого обладнання є критичною необхідністю.

Позитивні сторони:

1. У роботі наведено глибоке теоретичне обґрунтування вибору фізичної топології «розширена зірка». Автор вдало аргументував її переваги над іншими архітектурами в контексті гнучкості, локалізації збоїв та зручності для накладання логічної сегментації мережі.
2. Автор продемонстрував високу компетентність у питаннях логічної побудови інфраструктури, розробивши деталізований план IP-адресації та обґрунтовану матрицю доступу VLAN на реальному прикладі ПП «Веб-Інтеграція».
3. Практична цінність роботи підтверджується не лише грамотним підбором актуального обладнання корпоративного сегмента, але й успішним створенням імітаційної моделі.

Недоліки:

1. У роботі недостатньо уваги приділено економічному обґрунтуванню проєкту. Хоча вибір обладнання є технічно ідеальним, для малого підприємства було б доцільно додати кошторис витрат на закупівлю активного обладнання, кабельної продукції та оцінити орієнтовний термін окупності впровадженої інфраструктури.
2. Бажано було б розширити проєкт описом розгортання бездротового сегмента мережі. У сучасних офісних реаліях наявність захищених корпоративних та гостьових Wi-Fi мереж, ізольованих за допомогою тих самих VLAN, є невід'ємною частиною інфраструктури.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку " відмінно", а здобувач Семененко Д. Ю. заслуговує присвоєння кваліфікації: бакалавра з комп'ютерної інженерії.*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП 10
1 АНАЛІЗ ТЕХНОЛОГІЙ ТА АРХІТЕКТУРИ СУЧАСНИХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ МАЛИХ ПІДПРИЄМСТВ 11
1.1 Теоретичні основи, базове призначення та ключові характеристики корпоративних комп'ютерних мереж 11
1.2 Територіально-просторова класифікація комп'ютерних мереж та логічне позиціонування інфраструктури малого підприємства 13
1.3 Аналіз основних архітектурних схем побудови локальних мереж 22
2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ІНТЕГРАЦІЄЮ VLAN ТА СЕРВЕРНОЇ ІНФРАСТРУКТУРИ 39
2.1 Формулювання технічного завдання та обґрунтування архітектурних вимог до проєктування локальної мережі 39
2.2 Обґрунтування вибору активного комутаційного обладнання, серверної платформи та пасивної інфраструктури 41
2.3 Проєктування фізичної топології мережевої інфраструктури та схеми кабельних трас підприємства 45
3 ПРОЄКТУВАННЯ ЛОГІЧНОЇ АРХІТЕКТУРИ, НАЛАШТУВАННЯ СЕГМЕНТАЦІЇ VLAN ТА ПРОГРАМНА КОНФІГУРАЦІЯ АКТИВНОГО МЕРЕЖЕВОГО ОБЛАДНАННЯ 48
3.1 Планування простору IP-адресації, розробка логічної моделі VLAN та конфігурація інтерфейсів комутаційного обладнання 48
3.2 Програмна конфігурація активного мережевого обладнання та реалізація маршрутизації між VLAN 52
3.3 Моделювання комплексної мережевої інфраструктури та візуалізація логічної топології підприємства 55
ВИСНОВКИ 58

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 59
Додаток А 61

ВСТУП

В наш час мережева інфраструктура є фундаментальним середовищем, що забезпечує безперервність бізнес-процесів, централізоване управління інформаційними ресурсами та безпеку корпоративних даних. Сучасна локальна обчислювальна мережа малого підприємства являє собою складний апаратно-програмний комплекс, який вийшов за межі простого спільного використання периферійних пристроїв. Головне призначення такої мережі полягає у створенні надійного комунікаційного середовища для функціонування серверної інфраструктури, адже сучасна парадигма бізнесу передбачає використання виділених серверів для баз даних та корпоративних додатків замість децентралізованого зберігання інформації.

Проте, історично склалося, що малі підприємства часто будували мережі на базі некерованих комутаторів (unmanaged switches), створюючи єдиний широкомовний домен. Така архітектура є вкрай неефективною, оскільки будь-який мережевий збій на одному комп'ютері може миттєво паралізувати роботу всього офісу. Для того, щоб компанія мала стабільний доступ до ресурсів та глобальної мережі, сучасний підхід вимагає впровадження логічної сегментації на базі керованих комутаторів. Використання технології віртуальних локальних мереж дозволяє групувати користувачів, сервери та мережеве обладнання у незалежні підмережі, гарантуючи безпеку даних та абстрагуючись від фізичної топології. Саме тому проєктування надійної мережі малого підприємства з використанням сучасного комутаційного обладнання, технологій маршрутизації між VLAN та інтеграцією виділеної серверної інфраструктури є надзвичайно актуальним завданням для оптимізації роботи будь-якої компанії.

1 АНАЛІЗ ТЕХНОЛОГІЙ ТА АРХІТЕКТУРИ СУЧАСНИХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ МАЛИХ ПІДПРИЄМСТВ

1.1 Теоретичні основи, базове призначення та ключові характеристики корпоративних комп'ютерних мереж

Сучасна локальна обчислювальна мережа (ЛОМ) малого підприємства являє собою складний апаратно-програмний комплекс, який вийшов за межі простого фізичного з’єднання робочих станцій для спільного використання периферійних пристроїв. На сьогодні мережева інфраструктура є фундаментальним середовищем, що забезпечує безперервність бізнес-процесів, централізоване управління інформаційними ресурсами та безпеку корпоративних даних. В основі будь-якої корпоративної мережі лежить концепція об'єднання обчислювальних потужностей — від кінцевих пристроїв користувачів до високопродуктивних серверних систем — у єдиний логічний простір з керованою маршрутизацією та строгими політиками доступу[1].

Головне призначення локальної мережі в умовах малого підприємства полягає у створенні надійного та швидкісного комунікаційного середовища для функціонування серверної інфраструктури. Замість децентралізованого зберігання даних на окремих комп'ютерах, сучасна парадигма передбачає використання виділених серверів (як фізичних, так і віртуалізованих) для баз даних, файлових сховищ, контролерів домену та корпоративних додатків. Відповідно, мережа виступає транспортною артерією, яка повинна гарантувати безперебійний доступ клієнтських терміналів до цих централізованих ресурсів із мінімальними затримками, незалежно від поточного навантаження.

Аналізуючи загальні характеристики мережевої інфраструктури, першочергову увагу необхідно приділити пропускній здатності та продуктивності. Замість математичних розрахунків теоретичної межі передачі даних, на практиці продуктивність мережі описується здатністю комутаційного обладнання обробляти певну кількість пакетів за секунду без їх втрати або фрагментації. У сучасних реаліях для корпоративного сегмента стандартом де-факто є використання гігабітних або мультигігабітних каналів зв'язку на рівні доступу, тоді як магістральні з'єднання між серверами та ядром мережі вимагають пропускної здатності, що виключає появу так званих «вузьких місць» (bottlenecks) під час пікових навантажень на базу даних чи систему резервного копіювання.

Наступною критично важливою характеристикою є масштабованість та гнучкість топології. Історично малі підприємства часто будували мережі на базі некерованих комутаторів (unmanaged switches), що призводило до єдиного широкомовного домену. Така архітектура є вкрай неефективною, оскільки будь-який широкомовний шторм або мережева аномалія на одному комп'ютері миттєво паралізує роботу всього офісу. Сучасний підхід вимагає впровадження логічної сегментації на базі керованих комутаторів рівня L2/L3. Це дозволяє абстрагуватися від фізичної топології кабельної системи та групувати користувачів, сервери і мережеве обладнання (наприклад, IP-камери чи принтери) у незалежні віртуальні підмережі[2].

Не менш значущою характеристикою є відмовостійкість та рівень інформаційної безпеки на базовому (канальному та мережевому) рівнях еталонної моделі OSI. Локальна мережа підприємства повинна проектуватися з урахуванням мінімізації точок єдиної відмови. Це досягається впровадженням сучасного активного обладнання, такого як рішення корпоративного класу від Cisco, MikroTik або аналогічних вендорів, що підтримують протоколи резервування каналів, динамічну маршрутизацію та глибоку інспекцію трафіку. Безпекова складова вимагає жорсткої ізоляції корпоративних даних від гостьового трафіку та несанкціонованого доступу,

що технічно реалізується саме через правильне проектування внутрішньої логічної структури мережі, а не лише встановленням прикордонного маршрутизатора.

1.2 Територіально-просторова класифікація комп'ютерних мереж та логічне позиціонування інфраструктури малого підприємства

Історично склалося так, що масштаби та архітектурні особливості комп'ютерних мереж класифікувалися насамперед за критерієм їхнього фізичного та територіального охоплення. У класичній теорії телекомунікацій виділяють кілька фундаментальних ієрархічних рівнів: персональні (PAN), локальні (LAN), міські (MAN) та глобальні (WAN) мережі. Однак у контексті розбудови інформаційного середовища сучасного малого підприємства ця традиційна парадигма зазнає суттєвих концептуальних трансформацій. Базисом для розгортання корпоративної серверної інфраструктури виступає сегмент локальних обчислювальних мереж (ЛОМ), який забезпечує високошвидкісну взаємодію між робочими станціями та централізованими обчислювальними ресурсами в межах однієї або кількох суміжних будівель.

Сучасна локальна мережа підприємства кардинально відрізняється від своїх ранніх аналогів тим, що географічний чи просторовий критерій класифікації поступово відходить на другий план, поступаючись місцем логічній архітектурі. Завдяки масовому впровадженню технологій віртуальних локальних мереж (VLAN), фізичне розташування комп'ютера більше не визначає його мережеву приналежність. Це означає, що співробітники різних відділів, чиї робочі місця фізично підключені до одного комутатора, програмно розносяться по різних ізольованих підмережах. І навпаки, пристрої, рознесені по різних поверхах або корпусах, логічно об'єднуються в єдиний

широкомовний домен. Такий підхід дозволяє оптимізувати навантаження на сервери та гарантувати безпеку даних на канальному рівні абстракції.

Хоча ядром IT-інфраструктури малого бізнесу беззаперечно залишається мережа класу LAN, повноцінне функціонування внутрішнього серверного парку неможливе без тісної інтеграції з глобальними мережами (WAN). Прикордонне мережеве обладнання — сучасні корпоративні маршрутизатори та міжмережеві екрани (наприклад, рішення класу Next-Generation Firewall) — створює захищений шлюз між локальною інфраструктурою та глобальним інтернет-середовищем. Це забезпечує не лише доступ співробітників до зовнішніх ресурсів, але й дозволяє реалізувати технології віртуальних приватних мереж (VPN). Завдяки VPN віддалені користувачі отримують безпечний доступ до внутрішніх серверів компанії через зашифровані тунелі в глобальній мережі, що фактично розширює межі локальної мережі далеко за фізичні межі офісу[3].

Отже, позиціонуючи мережу малого підприємства в межах загальної територіальної класифікації, її слід розглядати не як статичну просторову структуру, а як гнучку мультисервісну локальну мережу з елементами гібридної взаємодії. Її архітектурні межі визначаються не стільки довжиною кабельних трас, скільки логічними правилами маршрутизації, політиками безпеки комутаторів рівня доступу та розподілу (Core/Distribution layer), а також вимогами до гарантованої пропускної здатності між кінцевими користувачами та корпоративними серверами.

Глобальна обчислювальна мережа (WAN — Wide Area Network) являє собою телекомунікаційну інфраструктуру вищого рівня, головним завданням якої є подолання географічних бар'єрів та об'єднання розрізнених локальних мереж у єдиний інформаційний простір. На відміну від локальної мережі підприємства, яка зосереджена в межах однієї будівлі або комплексу споруд, WAN оперує масштабами міст, країн та континентів. Для сучасного малого підприємства, яке розбудовує власну серверну інфраструктуру та сегментує трафік за допомогою VLAN, глобальна мережа виступає критично важливим

транспортним середовищем. Саме завдяки інтеграції з WAN локальна мережа отримує можливість взаємодіяти з хмарними платформами, забезпечувати публічну доступність корпоративних веб-сервісів та підтримувати повноцінну роботу віддалених співробітників.

Архітектура та фізична реалізація глобальних мереж суттєво відрізняються від принципів побудови локальних. Замість прокладання власних мідних чи оптичних кабельних трас, організація взаємодії з WAN базується на використанні орендованих каналів зв'язку та магістральної інфраструктури інтернет-провайдерів (ISP). Для забезпечення надійного та безперебійного доступу малого підприємства до глобальних ресурсів зазвичай використовуються високошвидкісні волоконно-оптичні канали, а як резервні підключення (Failover) — сучасні бездротові технології, такі як 4G/5G або термінали супутникового зв'язку. Передача даних у таких масштабах вимагає використання складних протоколів динамічної маршрутизації, які здатні автоматично адаптуватися до змін топології та ефективно керувати потоками інформації в сильно розподіленому середовищі.

На межі між локальною мережею малого підприємства та глобальним середовищем функціонує спеціалізоване прикордонне обладнання. Сучасний корпоративний підхід вимагає використання не просто базових маршрутизаторів, а комплексних шлюзів безпеки рівня Next-Generation Firewall (наприклад, актуальні рішення від Fortinet, Cisco або старші моделі MikroTik). Ці пристрої забезпечують не лише маршрутизацію транзитного трафіку, але й глибоку інспекцію пакетів, захист від мережевих атак та трансляцію мережевих адрес. Крім того, критично важливою функцією прикордонного обладнання є апаратна підтримка віртуальних приватних мереж (VPN), зокрема протоколів IPsec, OpenVPN або WireGuard. Це дозволяє створювати стійкі зашифровані тунелі через публічну мережу Інтернет, гарантуючи безпечний доступ віддалених користувачів безпосередньо до внутрішніх ресурсів та серверів компанії у відповідних ізольованих VLAN.

Найбільш яскравим та всеосяжним прикладом глобальної мережі є Інтернет, який об'єднує мільйони пристроїв по всьому світу. Проте існують і спеціалізовані корпоративні WAN, які створюються міжнародними холдингами, фінансовими установами або науковими організаціями для захищеного обміну даними між власними філіями. Незважаючи на незамінність глобальних мереж у сучасному бізнесі, взаємодія з ними має певні обмеження. До них належать залежність від стабільності роботи провайдера, потенційно вищі затримки при передачі пакетів (latency) у порівнянні з локальним сегментом, а також суттєві ризики інформаційної безпеки, оскільки зовнішнє середовище є джерелом постійних кіберзагроз. Підсумовуючи, у розрізі проектування мережі малого офісу, WAN розглядається як життєво необхідний, але потенційно небезпечний зовнішній простір, підключення до якого вимагає ретельного налаштування міжмережевих екранів та чіткого розмежування доступу на рівні локальної логічної архітектури[4].

Міська обчислювальна мережа (MAN — Metropolitan Area Network) виступає концептуальною та технологічною проміжною ланкою між локальними інфраструктурами окремих підприємств та глобальними трансконтинентальними магістралями. Її просторове охоплення зазвичай обмежується межами одного великого мегаполіса або міської агломерації. З архітектурної точки зору, MAN становить собою високошвидкісну транспортну магістраль, покликану об'єднати географічно рознесені локальні мережі в єдиний керований комунікаційний простір. Для малого підприємства, яке планує масштабування, розширення виробничих площ або відкриття додаткових філій у межах міста, технології рівня MAN дозволяють зберегти цілісність корпоративної логічної структури. Це дає можливість прозоро маршрутизувати або навіть розширювати внутрішні VLAN між віддаленими офісами без необхідності складної тунельної інкапсуляції через непередбачуваний глобальний Інтернет.

Основною рушійною силою використання міських мереж є потреба організацій у централізованому управлінні розподіленими інформаційними ресурсами. Завдяки гарантовано високій пропускній здатності MAN-з'єднань, підприємства отримують можливість виносити свою серверну інфраструктуру (наприклад, файлові сховища або сервери віртуалізації) у спеціалізовані міські центри обробки даних (ЦОД). При цьому швидкість доступу до них з локальної мережі офісу залишається такою ж високою, як і при фізичному розміщенні серверів у сусідній кімнаті. Це створює ідеальні умови для синхронізації баз даних, функціонування систем корпоративного документообігу та реалізації надійних стратегій резервного копіювання і аварійного відновлення (Disaster Recovery). Крім корпоративного сектора, ресурси міських магістралей є фундаментальною базою для телекомунікаційних компаній, що надають високошвидкісні послуги зв'язку абонентам.

З технічного боку міські мережі будуються переважно на базі сучасних волоконно-оптичних ліній зв'язку, часто з використанням технологій спектрального ущільнення (CWDM або DWDM) та концепції Metro Ethernet. Для забезпечення безперервності надання сервісів у MAN активно застосовується фізична топологія "кільце" в поєднанні з протоколами швидкого відновлення (наприклад, Ethernet Ring Protection Switching — ERPS). Це гарантує перемикання трафіку на резервний маршрут за лічені мілісекунди у разі фізичного обриву оптичного кабелю. Важливою відмінністю від розрізнених WAN-підключень є те, що сучасні міські мережі дозволяють операторам надавати клієнтам послуги передачі даних безпосередньо на канальному (L2) рівні. Завдяки технологіям на кшталт подвійного тегування (Q-in-Q або IEEE 802.1ad), трафік малого підприємства із внутрішніми мітками VLAN інкапсулюється у зовнішній тег провайдера, що дозволяє об'єднувати комутатори різних філій так, ніби вони з'єднані прямим патч-кордом.

Активне мережеве обладнання міського рівня включає потужні оптичні мультиплексори, високопродуктивні магістральні комутатори операторського

класу (Carrier-grade switches, наприклад, з лінійок Cisco Nexus або аналогічні рішення від Juniper) та сервери широкосмугового агрегування трафіку. Пропускна здатність сучасних магістралей MAN еволюціонувала від сотень мегабіт до десятків та сотень гігабіт за секунду на магістральних портах, що дозволяє обслуговувати тисячі абонентів без деградації якості обслуговування (QoS)[5].

Типовими сценаріями розгортання міських мереж є створення єдиного інформаційного середовища для великих університетських кампусів, об'єднання адміністративних будівель органів місцевого самоврядування або розбудова опорної інфраструктури кабельних провайдерів. У контексті проектування локальної мережі сучасного малого офісу з розгорнутою серверною інфраструктурою, підключення до MAN розглядається як високоякісний транспортний інтерфейс зовнішнього середовища. Він виступає надійним оптичним шлюзом для доступу в глобальну мережу з симетричною пропускною здатністю, або ж слугує виділеним високошвидкісним транзитом для зв'язку між міськими підрозділами компанії, дозволяючи їхнім локальним мережам функціонувати в єдиному домені Active Directory та безпечно обмінюватися даними.

Персональна обчислювальна мережа (PAN — Personal Area Network) являє собою найменший за територіальним охопленням архітектурний рівень телекомунікаційної взаємодії, радіус дії якого традиційно обмежується особистим робочим простором одного користувача. У класичному розумінні така інфраструктура створюється для прямої, тимчасової комунікації між персональними цифровими пристроями без залучення транзитних вузлів маршрутизації, комутаторів чи виділених серверів. Проте в контексті функціонування комплексної корпоративної мережі малого підприємства концепція PAN набуває принципово іншого змісту. Вона розглядається не просто як набір бездротових гаджетів, а як мікропериметр кінцевого користувача (Endpoint Micro-perimeter), що динамічно інтегрується з його робочою станцією. Ця робоча станція, у свою чергу, є частиною загальної

локальної мережі з жорсткою сегментацією на базі віртуальних підмереж (VLAN) і має регламентований доступ до серверного ядра компанії[6].

Апаратно-технологічний стек сучасних персональних мереж базується переважно на енергоефективних протоколах бездротового зв'язку малого радіуса дії, які еволюціонували під потреби бізнесу. Домінуючими стандартами сьогодні є актуальні специфікації Bluetooth (зокрема Bluetooth Low Energy версій 5.x), високошвидкісні прямі з'єднання Wi-Fi Direct та технології ближнього поля (NFC). Крім бездротових рішень, фізичний рівень PAN у корпоративному середовищі активно реалізується через високошвидкісні дротові інтерфейси нового покоління, такі як Thunderbolt 4 або USB4. Ці інтерфейси використовуються для об'єднання ноутбуків співробітників із док-станціями, біометричними сканерами або зовнішніми криптографічними модулями. Завдяки таким протоколам навколо співробітника формується локалізована екосистема пристроїв (смартфони, смарт-годинники, апаратні ключі авторизації, бездротові гарнітури), яка суттєво підвищує мобільність та ергономіку робочого процесу.

Незважаючи на автономність та відсутність потреби у складному налаштуванні, інтеграція пристроїв PAN у середовище малого підприємства вимагає пильної уваги до політик інформаційної безпеки. Оскільки персональні мережі функціонують поза прямим апаратним контролем офісних комутаторів рівня доступу, вони формують потенційну вразливість та розширюють поверхню потенційної кібератаки. Наприклад, несанкціоноване підключення персонального смартфона до корпоративного ПК через Bluetooth або USB може створити неконтрольований інформаційний міст (Data Leakage channel), який дозволить зловмиснику оминути корпоративний фаєрвол. Саме тому взаємодія між PAN та загальною локальною мережею повинна суворо регламентуватися системами захисту кінцевих точок (Endpoint Detection and Response) та політиками Active Directory. Такі програмні обмеження блокують несанкціоноване перенесення даних із зони особистої мережі співробітника у

захищені VLAN, де розташовані фінансові бази даних чи критичні файлові сервери підприємства.

Підсумовуючи, у загальній топології IT-інфраструктури підприємства персональні мережі виконують допоміжну, периферійну функцію. Вони не є логічною частиною транспортної архітектури локальної мережі, проте активно з нею співіснують у рамках сучасних концепцій організації праці, таких як BYOD (Bring Your Own Device). За умови правильного конфігурування систем безпеки, використання PAN є абсолютно доцільним: це дозволяє співробітникам оперативно використовувати персональні мобільні пристрої, а також застосовувати апаратні токени для багатофакторної автентифікації під час доступу до серверної інфраструктури, не створюючи при цьому ризиків для цілісності та ізольованості корпоративних VLAN.

Локальні комп’ютерні мережі, які найчастіше позначають абревіатурою LAN (від англійського Local Area Network), на сьогоднішній день виступають найбільш розповсюдженим та фундаментальним типом комунікаційної інфраструктури. Їхнє головне призначення полягає в надійному об’єднанні робочих станцій, різноманітних серверів, периферійної техніки та спеціалізованого мережевого обладнання в межах чітко обмеженої географічної зони. Такою локацією зазвичай виступає простір одного сучасного офісу, приватна квартира, навчальний заклад або ж окремий поверх великої корпоративної будівлі. Ключовою технічною особливістю та беззаперечною перевагою будь-якої локальної мережі є здатність забезпечувати надзвичайно високу швидкість обміну інформацією при мінімальних затримках передачі пакетів. Саме цей фактор дозволяє організувати максимально ефективну, безперервну та комфортну взаємодію між усіма авторизованими учасниками внутрішньої мережі, незалежно від обсягів даних, що пересилаються.

Якщо детальніше розглядати архітектуру типової локальної мережі, то до її складу обов'язково входять такі активні та пасивні компоненти, як маршрутизатори для зв'язку із зовнішнім світом, комутатори для

інтелектуальної внутрішньої маршрутизації трафіку, бездротові точки доступу, а також безпосередньо кінцеві вузли: персональні комп’ютери, мережеві принтери та системи зберігання даних (NAS). Уся ця цифрова екосистема фізично або логічно з’єднується в єдине ціле за допомогою ретельно спланованої структурованої кабельної системи або ж сучасних бездротових засобів зв’язку. Традиційно LAN може будуватися виключно на надійній дротовій основі за стандартами сімейства Ethernet, використовувати виключно радіоканали Wi-Fi для забезпечення максимальної мобільності співробітників, або ж, що на практиці зустрічається найчастіше, мати гнучку комбіновану структуру. У реаліях сучасних офісних приміщень золотим стандартом дедалі частіше стає використання гігабітних або навіть мультигігабітних з’єднань, оскільки лише вони здатні гарантувати належну продуктивність під час інтенсивної колективної роботи[7].

Фундаментальні переваги розгортання локальних мереж охоплюють відносну простоту їхнього практичного впровадження, загальну економічну доступність необхідного обладнання, а також широкі можливості для гнучкого налаштування та легкого адміністрування. Завдяки наявності грамотно спроєктованої LAN будь-яке підприємство отримує змогу ефективно централізувати управління всією корпоративною документацією, суворо контролювати рівні доступу до конфіденційних ресурсів та організувати зручне спільне використання дорогої периферії, такої як багатофункціональні пристрої. Крім того, локальна інфраструктура створює ідеальні умови для розгортання власних потужних внутрішніх серверів, серед яких можуть бути виділені файлові сховища, корпоративні поштові сервери або ж автоматизовані системи регулярного резервного копіювання критично важливої інформації.

З огляду на те, що LAN зазвичай фізично локалізована в межах одного або кількох сусідніх приміщень і юридично повністю належить одній конкретній організації, це дає адміністраторам змогу здійснювати всеосяжний контроль над власною мережевою інфраструктурою. Така централізація суттєво спрощує впровадження комплексних заходів кібербезпеки: від

налаштування апаратних чи програмних фаєрволів та жорсткого розмежування прав доступу користувачів до впровадження глибокого шифрування внутрішнього трафіку та постійного моніторингу подій. З часом добре побудована локальна мережа може слугувати надійним фундаментом для створення значно складніших комунікаційних систем, поступово об'єднуючись у міські (MAN) чи глобальні (WAN) мережі. Відтак, у контексті виконання даної кваліфікаційної роботи проєктування локальної мережі розглядається як найбільш раціональне та оптимальне технологічне рішення для потреб малого офісу. Вона здатна гарантувати блискавичний обмін корпоративною інформацією, забезпечити стабільний і захищений зв’язок між усіма робочими пристроями та створити міцне внутрішнє цифрове середовище для ефективної щоденної діяльності компанії, при цьому уникаючи невиправданих витрат на надмірно складну та дорогу інфраструктуру.

1.3 Аналіз основних архітектурних схем побудови локальних мереж

Розробка та безпосереднє проєктування будь-якої сучасної локальної комп'ютерної мережі невіддільно пов'язані з критично важливим етапом — вибором найбільш оптимальної мережевої топології. Цей термін визначає конкретний спосіб фізичного прокладання ліній зв'язку або логічного алгоритму з'єднання всіх інтелектуальних пристроїв у єдину робочу екосистему. Від того, наскільки грамотно буде обрано цю базову архітектуру, напряму залежать ключові експлуатаційні характеристики майбутньої інфраструктури: її загальна продуктивність, безвідмовність у роботі, потенціал для подальшого масштабування без втрати швидкості, а також рівень складності щоденного технічного обслуговування й, безперечно, підсумкові фінансові витрати на закупівлю необхідного мережевого обладнання[8].

Розглядаючи історичний розвиток мережевих технологій, варто виокремити топологію «шина», яка заслужено вважається однією з найдавніших та архітектурно найпростіших форм організації комп'ютерної взаємодії. Фундаментальний принцип її побудови полягає в тому, що абсолютно всі мережеві вузли (робочі станції, сервери чи периферійна техніка) паралельно підключаються до єдиного спільного каналу передачі даних. Ця центральна комунікаційна лінія виконує роль своєрідної магістралі. Інформаційний обмін у такій системі відбувається за принципом розсилання широкомовних повідомлень: будь-який електричний сигнал, згенерований і відправлений одним комп'ютером, безперешкодно поширюється по всьому кабелю і стає фізично доступним для зчитування всіма іншими пристроями в мережі. Проте програмно цей сигнал обробляється виключно тим вузлом, чия мережева адреса збігається з адресою призначення у відправленому пакеті даних. Критично важливою фізичною вимогою для стабільного функціонування «шини» є обов'язкова наявність на обох кінцях магістрального кабелю спеціальних пристроїв — термінаторів. Це узгоджувальні резистори, головне завдання яких полягає в поглинанні залишкового електричного сигналу на кінцях лінії, що унеможливлює його відбиття у зворотному напрямку та запобігає виникненню перешкод чи критичних помилок під час передачі інформації.

Незважаючи на простоту реалізації, суворі реалії та високі вимоги сучасних корпоративних умов експлуатації накладають надзвичайно жорсткі обмеження на практичне застосування шинної топології. Її найголовнішим і найболючішим недоліком фахівці одноголосно називають вкрай слабку здатність до масштабування. З кожним новим підключеним до системи пристроєм експоненціально зростає загальне навантаження на єдиний спільний канал зв'язку. Це неминуче призводить до стрімкого падіння загальної продуктивності мережі, появи відчутних затримок у передачі пакетів та суттєвого підвищення ймовірності виникнення так званих колізій — ситуацій, коли два або більше пристроїв намагаються здійснити передачу

даних в один і той самий момент часу, руйнуючи сигнали один одного. До того ж, архітектура «шини» відзначається низьким рівнем загальної відмовостійкості: фізичне пошкодження центрального магістрального кабелю бодай у одному місці або ж раптовий вихід з ладу хоча б одного термінатора миттєво паралізує роботу абсолютно всієї мережі, розриваючи зв'язок між усіма її учасниками[9].

Окремо варто наголосити на серйозних труднощах, пов'язаних із технічною підтримкою та діагностикою несправностей. Оскільки всі мережеві клієнти в шинній топології підключені до однієї лінії, процес пошуку точного місця фізичного обриву кабелю чи виявлення пошкодженого конектора перетворюється на вкрай складне та тривале завдання для системних адміністраторів. Ситуацію суттєво ускладнює ще й той факт, що банальне додавання нового комп'ютера до існуючої магістралі або відключення старого обладнання зазвичай вимагає тимчасової зупинки функціонування всієї мережі. У сучасних динамічних офісних середовищах, де безперервність бізнес-процесів є критичною умовою успіху, такі простої вважаються абсолютно неприйнятними.

Разом з тим, було б помилкою стверджувати, що топологія «шина» повністю зникла з технологічної мапи. Її специфічні властивості досі знаходять своє застосування у певних вузькоспеціалізованих нішах. Наприклад, подібна архітектура залишається затребуваною при проєктуванні промислових мереж передачі даних (зокрема, на базі стандарту RS-485), розгортанні базових систем телеметрії та моніторингу, або ж у специфічних ситуаціях, де комунікаційну інфраструктуру потрібно розгорнути як тимчасове рішення з максимально обмеженим фінансовим бюджетом. Для більш наочного розуміння специфіки цього архітектурного рішення, детальна порівняльна характеристика, табл.1.1, дозволяє комплексно оцінити базові параметри, ключові переваги та найсуттєвіші недоліки шинної топології у зіставленні з вимогами до сучасних схем побудови мереж.

Таблиця 1.1 – Оцінка технічних та експлуатаційних параметрів шинної архітектури

Критерій оцінки	Технічна специфіка та опис
Механізм комунікації та швидкість	Обмін інформацією відбувається через спільний магістральний канал за принципом широкомовного розсилання. Пропускна здатність є нестабільною: зі збільшенням кількості активних пристроїв стрімко зростає ризик колізій та падіння швидкості.
Апаратні вимоги та бюджет	Мережа відзначається максимальною фінансовою доступністю. Вона не потребує дорогих активних комутаторів чи маршрутизаторів — для коректної роботи достатньо лише кабелю та пасивних термінаторів на його кінцях.
Відмовостійкість та обслуговування	Архітектура має критично низьку надійність. Найменше фізичне пошкодження головної магістралі миттєво паралізує всю мережу. При цьому специфіка з'єднання робить процес локалізації місця обриву дуже складним і тривалим для адміністраторів.
Гнучкість та потенціал масштабування	Хоча базове розгортання відбувається швидко й просто, система не призначена для зростання. Додавання нових вузлів суворо лімітоване (оптимальна межа — 10–20 комп'ютерів), оскільки подальше розширення руйнує стабільність з'єднання.
Сучасна актуальність технології	У розрізі побудови повноцінних офісних чи корпоративних інфраструктур це рішення є повністю застарілим. Сьогодні його доцільно застосовувати лише для вузькопрофільних промислових завдань, тимчасових підключень або як наочний навчальний макет.

Підсумовуючи вищенаведені факти, можна впевнено констатувати, що мережева топологія «шина», маючи беззаперечні історичні заслуги на етапі зародження комп'ютерних комунікацій, на сьогоднішній день є об'єктивно застарілою для широкого впровадження у повноцінних корпоративних умовах. У сучасних реаліях проєктування локальних мереж її цілком закономірно витіснили значно більш надійні, безвідмовні та гнучкі до масштабування архітектурні структури. Головним наступником та беззаперечним лідером у цьому сегменті стала топологія типу «зірка», яка незрівнянно краще відповідає жорстким сучасним стандартам щодо високої швидкості обміну даними, надійної інформаційної безпеки, безперебійної доступності ресурсів та загальної гнучкості адміністрування.

На сьогоднішній день архітектурне рішення під назвою «зірка» займає домінуючі позиції та є найбільш затребуваним стандартом під час побудови локальних обчислювальних систем. Її можна зустріти практично всюди: у сучасних корпоративних офісах, державних та навчальних установах, на об'єктах малого бізнесу, а також у звичайних житлових будинках. Концептуальна суть цієї топології полягає в тому, що кожен окремий цифровий пристрій чи робоча станція не взаємодіють між собою напряму, а підключаються за допомогою індивідуальної лінії зв'язку до єдиного спільного центру. Роль такого центрального вузла зазвичай виконує мережевий комутатор або маршрутизатор, який бере на себе всі функції з інтелектуального керування, аналізу та перенаправлення інформаційних потоків між усіма учасниками мережі[10].

Процес безпосередньої передачі пакетів даних у межах «зіркової» структури повністю підпорядкований цьому централізованому принципу. Коли певний комп'ютер ініціює відправку інформації іншому адресату, сформований сигнал спочатку надходить на центральний комутатор. Пристрій миттєво зчитує службові заголовки пакета, визначає кінцевого одержувача і відправляє дані саме в той порт, до якого підключено потрібний девайс. Завдяки такому підходу повністю нівелюється потреба у широкомовному

засміченні всієї лінії зв'язку, адміністратори отримують повний контроль над маршрутами пересування корпоративного трафіку, а ймовірність виникнення мережевих або апаратних колізій зводиться до абсолютного мінімуму.

Головним аргументом на користь вибору цієї схеми є її безпрецедентно високий рівень відмовостійкості та загальної надійності. Якщо в процесі експлуатації стається фізичний обрив мережевого кабелю або виходить з ладу конкретна робоча станція, це жодним чином не впливає на життєздатність усієї системи — від мережі від'єднується лише один цей ізольований вузол. Така особливість значно спрощує сервісне обслуговування та повсякденне адміністрування інфраструктури, адже фахівець може за лічені хвилини локалізувати точне джерело виникнення несправності та оперативно його усунути, абсолютно не порушуючи звичний робочий ритм інших співробітників офісу.

Не менш важливою перевагою «зірки» вважається її виняткова еластичність та практично необмежений потенціал для подальшого розширення. За необхідності інтегрувати в систему нове обладнання, створити додаткове робоче місце чи підключити мережевий принтер, системному адміністратору достатньо лише прокласти один окремий кабель від нового пристрою до вільного порту на центральному комутаторі. Цей процес не вимагає зупинки мережі чи переконфігурації існуючих підключень, що робить дану топологію ідеальним вибором для компаній, які динамічно розвиваються, де чисельність штату або технічні вимоги можуть поступово зростати.

Проте, незважаючи на очевидні плюси, централізована архітектура має і власне слабке місце, яке називають залежністю від єдиної точки відмови. Якщо з ладу раптово виходить головний комутатор або маршрутизатор (наприклад, через апаратне пошкодження чи збій у системі живлення), абсолютно вся локальна мережа миттєво паралізується. Саме тому під час проєктування та практичного впровадження таких рішень особливу увагу приділяють купівлі високоякісного брендового обладнання, забезпеченню його безперебійним

електроживленням за допомогою лінійно-інтерактивних UPS, а в масштабних проєктах — і дублюванню ключових комутаційних вузлів[11].

З погляду фізичної реалізації, побудова «зірки» вимагає створення розгалуженої структурованої кабельної системи. Кожен комп'ютер індивідуальною лінією (найчастіше на основі витої пари) тягнеться до комутаційної шафи чи патч-панелі. Для умов невеликого офісного приміщення з парком техніки в межах 10–20 одиниць така організація простору є найбільш виправданою з економічного погляду, оскільки витрати на кабель повністю компенсуються стабільністю роботи та легкістю контролю. Детальний аналіз усіх експлуатаційних параметрів цієї архітектурної моделі наведено нижче, табл.1.2.

Таблиця 1.2– Оцінка технічних та експлуатаційних параметрів шинної архітектури

Параметр оцінки	Технологічна специфіка та параметри інфраструктури
Архітектура розподілу даних	Весь трафік обов'язково проходить через єдиний інтелектуальний центр (switch або router).
Апаратне забезпечення	Наявність активного комутаційного пристрою є критично необхідною умовою функціонування.
Рівень безвідмовності	Максимально високий, оскільки локальні пошкодження ліній повністю ізольовані від загальної системи.
Локалізація збоїв та ремонт	Здійснюється швидко і без зусиль завдяки автономності кожного підключеного кабельного сегмента.
Складність монтажних робіт	Помірна, вимагає попереднього планування розміщення центрального вузла та прокладання індивідуальних ліній.

Можливості модернізації	Високі, система легко масштабується шляхом простого підключення нових клієнтів до вільних портів.
Фінансові інвестиції	Трохи вищі порівняно з найпростішими схемами через витрати на активне обладнання та більший метраж кабелю.
Швидкісні показники	Забезпечує максимальну пропускну здатність, особливо за умови впровадження гігабітних технологій.
Рекомендована сфера застосування	Сучасні бізнес-центри, офіси будь-якого масштабу, освітні простори та приватний сектор.
Рівень актуальності	На сьогодні це безальтернативний лідер і загальноприйнятий стандарт для побудови локальних мереж.

Таким чином, топологія «зірка» успішно поєднує в собі простоту щоденного використання, високий ступінь захищеності від внутрішніх збоїв, легкість масштабування та ідеальну адаптивність до специфічних потреб малого бізнесу. Саме тому в межах даної роботи вона обґрунтовано розглядається як єдине базове та найбільш раціональне рішення для розгортання надійної сучасної мережі.

Мережева архітектура, відома під назвою «кільце», пропонує принципово інший підхід до організації взаємодії між пристроями порівняно з іншими стандартами. Її концепція полягає в тому, що кожен комп'ютер, сервер або інший мережевий вузол фізично з'єднується рівно з двома сусідніми пристроями — одним попереднім та одним наступним. У результаті такого послідовного підключення утворюється суцільне замкнене коло. Цифрова інформація в такій екосистемі передається виключно по цьому контуру, естафетно переходячи від одного вузла до іншого у чітко визначеному напрямку (залежно від специфіки налаштувань, рух може бути одностороннім

або ж двостороннім), аж поки пакети даних не досягнуть своєї кінцевої адреси. Для того щоб сигнал не згасав і не втрачав своєї якості під час проходження довгих дистанцій, у кожен такий транзитний вузол часто вбудовується спеціальний апаратний повторювач[12].

Фундаментальною відмінністю та водночас ключовою особливістю цієї структури є суворо послідовна маршрутизація. Оскільки всі інформаційні пакети неминуче проходять через проміжні комп'ютери, це дає змогу підтримувати максимально стабільне та прогнозоване навантаження на всю мережу. Завдяки такій логіці система надійно захищена від так званих широкомовних штормів (коли мережа перевантажується хаотичним розсиланням даних усім підряд), а час доставки будь-якого повідомлення можна розрахувати з високою точністю. Для ще більшої ефективності в багатьох варіаціях кільцевих мереж впроваджено інтелектуальний механізм маркерного доступу. Його суть нагадує передачу естафетної палички: у мережі безперервно циркулює спеціальний електронний маркер, і лише той пристрій, який у конкретний момент часу володіє ним, отримує ексклюзивне право на відправлення власних даних. Цей підхід елегантно і повністю усуває саму можливість виникнення інформаційних колізій.

Аналізуючи сильні сторони кільцевої топології, варто обов'язково відзначити ідеально збалансоване використання загальної смуги пропускання, відсутність фонового сміттєвого трафіку та здатність системи гарантувати доставку кожного відправленого пакета. Проте ці вагомі переваги, на жаль, повністю нівелюються вкрай серйозними експлуатаційними обмеженнями. Найбільш критичним і болючим недоліком є феноменальна вразливість такої мережі: раптовий вихід з ладу бодай одного комп'ютера або ж випадкове пошкодження кабелю на будь-якій ділянці миттєво розриває замкнене коло. Це автоматично призводить до повного паралічу всієї інфраструктури. Щоб обійти цю проблему, інженери розробили топологію подвійного кільця, де передбачено дублюючий резервний шлях для руху трафіку в протилежному

напрямку. Однак таке резервування вимагає вдвічі більше кабелю та значно складнішого обладнання, що робить проєкт суттєво дорожчим.

Процедура пошуку та усунення несправностей у кільці перетворюється на справжнє випробування для фахівців, адже кожен вузол тут є життєво важливим транзитним пунктом, особливо якщо мова йде про застарілі аналогові системи. Навіть банальне планове перезавантаження одного робочого місця чи спроба підключити новий принтер вимагає фізичного втручання в магістраль, що зупиняє роботу інших користувачів. Саме через ці незручності сучасні офіси практично повністю відмовилися від використання цієї топології. Історично вона була надзвичайно популярною в епоху домінування корпоративних рішень від IBM, проте сьогодні її застосування звузилося до специфічних ніш. Найчастіше кільцеву структуру можна зустріти у високошвидкісних оптоволоконних транспортних магістралях або ж у суворо ізольованих сегментах промислових систем відеоспостереження[13].

Що стосується проєктування мережі для малого офісу, то розгортання кільцевої архітектури є об'єктивно недоцільним. Вона є надто крихкою перед повсякденними збоями, вкрай незручною в питаннях швидкої модернізації та не здатна забезпечити необхідну гнучкість робочого процесу. Сучасні компанії абсолютно виправдано віддають перевагу централізованим зіркоподібним рішенням, табл. 1.3.

Таблиця 1.3– Оцінка технічних та експлуатаційних параметрів шинної архітектури

Критерій оцінки	Технічна специфіка та особливості функціонування
Механізм трансляції та швидкісні показники	Обмін даними відбувається суворо послідовно по замкненому контуру. Завдяки технології маркерного доступу пропускна здатність залишається максимально стабільною та прогнозованою.

Апаратне забезпечення та бюджет	Для коректної роботи часто потрібні вбудовані повторювачі сигналу. Вартість розгортання перевищує найпростіші лінійні схеми, але залишається дешевшою за складні багатовузлові структури.
Відмовостійкість та обслуговування	У класичному (одинарному) виконанні надійність є критично низькою, оскільки аварія на одній ділянці зупиняє всю мережу. Процес локалізації місця розриву вимагає часу та зусиль системного адміністратора.
Можливості розширення інфраструктури	Потенціал масштабування суворо лімітований. Інтеграція будь-якого нового обладнання передбачає обов'язкове переривання цілісності кільця, що призводить до простою всієї системи.
Актуальність застосування на сьогодні	Технологія є морально застарілою для облаштування офісних чи домашніх просторів. Нині вона успішно використовується лише у вузькопрофільних промислових мережах та надійних оптоволоконних каналах.

Мережева архітектура, відома під назвою «дерево», являє собою багаторівневу ієрархічну модель побудови телекомунікаційної інфраструктури, яка надзвичайно вдало поєднує в собі найкращі технічні риси як централізованої «зірки», так і лінійної «шини». Концептуально така система розгортається у вигляді потужної розгалуженої структури: вона складається з множини окремих локальних сегментів (кожен з яких побудований за класичним принципом зіркоподібної мережі), що органічно під'єднуються до центрального магістрального каналу або потужного комутаційного вузла вищого рівня.

У результаті формується чітка деревоподібна ієрархія розподілу даних, де кожен нижній комутаційний рівень нерозривно пов'язаний із вищим через відповідне мережеве обладнання[14].

Кожна окрема гілка такого ієрархічного дерева фактично виступає як абсолютно самостійний робочий сегмент зі своїм власним локальним комутатором, до якого кабелями підведені кінцеві споживачі інформації: персональні комп’ютери співробітників, мережеві принтери, бездротові точки доступу та інша периферія. У подальшому ці відокремлені гілки агрегуються та підключаються до потужнішого розподільчого пристрою або безпосередньо до головного магістрального комутатора мережі (ядра). Така продумана організація простору та інформаційних потоків відкриває колосальні можливості для масштабування: якщо в компанії з'являється новий відділ або відкривається додатковий офісний поверх, системному адміністратору не потрібно переробляти всю інфраструктуру — достатньо просто приєднати нову комутаційну гілку до відповідного вільного порту на вищому рівні дерева.

Беззаперечною та найголовнішою перевагою цієї топології є її вражаюча еластичність та високий потенціал до розширення. Завдяки ієрархічній природі побудови, ІТ-відділ отримує змогу логічно та фізично розділити єдину корпоративну мережу на ізольовані керовані зони, які відповідають реальній структурі підприємства — наприклад, розбити її за відділами, поверхами чи навіть окремими будівлями. Це не лише суттєво спрощує загальне управління мережею, але й дає змогу надійно ізолювати специфічний трафік певних сегментів, підвищуючи безпеку та зменшуючи навантаження на магістраль. До того ж, кожен такий локальний сегмент здатний продовжувати свою автономну роботу в межах власного комутатора навіть у тому випадку, якщо в інших частинах глобальної корпоративної мережі виникли серйозні технічні неполадки[15].

Проте, як і будь-яка складна система, структура «дерево» не позбавлена суттєвих недоліків, головним з яких є критична залежність нижніх рівнів від стабільності роботи вузлів вищого ешелону. Якщо з ладу несподівано виходить

центральний агрегуючий комутатор або пошкоджується головний магістральний оптичний канал, це неминуче призводить до відключення та повної ізоляції цілих підмереж, залишаючи сотні користувачів без доступу до спільних ресурсів. Саме через цей фактор ризику при проєктуванні критично важливих інфраструктур фахівці в обов'язковому порядку застосовують технології резервування основних ліній зв'язку, а також використовують виключно висококласне відмовостійке обладнання, оснащене дубльованими блоками живлення та апаратним захистом від збоїв[16].

Топологія «дерево» об'єктивно визнана найбільш ефективним та раціональним рішенням для середніх і великих організацій, де виникає гостра потреба об'єднати в єдиний керований простір велику кількість розрізнених локальних мереж. Її найчастіше розгортають на територіях університетських кампусів, у багатоповерхових бізнес-центрах, гіпермаркетах та масштабних медичних установах, де логічна структура мережі повинна чітко відображати фізичне або функціональне планування самого об’єкта, табл.1.4.

Таблиця 1.4 – Аналітичний огляд експлуатаційних властивостей деревоподібної топології

Критерій оцінки	Технічна специфіка та архітектурні особливості
Логіка маршрутизації трафіку	Дані передаються через чітко структуровану ієрархію комутаційних рівнів (від периферії до ядра і навпаки).
Вимоги до апаратної бази	Наявність активного мережевого обладнання є критично обов'язковою на кожному рівні розгалуження.
Ступінь відмовостійкості	Варіюється від середнього до високого; безпосередньо залежить від наявності резервних каналів для магістрального ядра.

Локалізація несправностей	Проблеми на рівні кінцевих гілок виявляються та усуваються відносно легко, не зачіпаючи глобальну роботу системи.
Складність проєктування та монтажу	Вимагає високого рівня інженерної експертизи для грамотного планування ієрархії, кабельних трас та пропускної здатності.
Еластичність та розширення	Надзвичайно висока; архітектура ідеально пристосована для безболісного підключення нових великих сегментів чи філій.
Економічний аспект впровадження	Потребує значних фінансових інвестицій, оскільки вимагає великої кількості кабельної продукції та дорогого обладнання різних рівнів.
Пропускна здатність та затримки	У межах одного локального сегмента швидкість максимальна; при зверненні до інших гілок можливі мікрозатримки через обробку даних вузлами вищих рівнів.
Рекомендований спектр застосування	Масштабні корпоративні мережі, державні установи, навчальні заклади, промислові комплекси та багатоповерхові споруди.
Актуальність технології на ринку	Залишається абсолютно актуальною та є загальноприйнятим світовим стандартом для побудови великих сегментованих мереж.

Мережева архітектура, відома як топологія «сітка» (Mesh), являє собою найбільш стійку та фундаментально захищену структуру побудови комунікацій. Її головний принцип полягає в тому, що кожен вузол системи має безпосереднє фізичне або логічне підключення одразу до кількох, а в ідеалі — до абсолютно всіх інших учасників мережі. Завдяки такій щільній павутині з'єднань створюється величезна кількість альтернативних маршрутів для передавання інформаційних пакетів. У сучасній інженерній практиці

розрізняють два фундаментальні підходи до реалізації цієї концепції. Перший — це повна сітка (full mesh), еталонна модель, де кожен без винятку комп'ютер чи маршрутизатор має виділений прямий кабель до кожного іншого пристрою в системі. Другий підхід — часткова сітка (partial mesh), яка є більш прагматичним рішенням: тут прямими множинними зв'язками об'єднуються лише найважливіші, критичні вузли, тоді як другорядні пристрої підключаються до них через транзитні канали[17].

Беззаперечною та найважливішою перевагою сітчастої топології є її феноменальна відмовостійкість і здатність до самовідновлення. Якщо в мережі раптово стається аварія — наприклад, фізично обривається оптичний кабель, виходить з ладу порт або навіть повністю «падає» кілька проміжних комутаторів, — система не зупиняється. Інтелектуальні протоколи миттєво і в автоматичному режимі перенаправляють весь потік даних через інші доступні обхідні шляхи. Саме ця властивість робить сітчасту структуру безальтернативним вибором для об'єктів критичної інфраструктури, де навіть секундна втрата зв'язку може призвести до катастрофічних наслідків: у банківському секторі, реанімаційних відділеннях медичних установ, на військових базах, у системах глобального відеонагляду та у великих центрах обробки даних (ЦОД). Крім того, наявність багатьох паралельних шляхів дозволяє максимально ефективно балансувати мережеве навантаження. Трафік рівномірно розподіляється між усіма доступними каналами, що повністю виключає появу так званих «вузьких місць» і забезпечує найвищу можливу пропускну здатність[18].

Однак впровадження повноцінної сітки супроводжується колосальними технічними та фінансовими труднощами. Основна проблема полягає у специфіці масштабування: з додаванням до мережі кожного нового пристрою кількість необхідних кабелів та вільних портів зростає не поступово, а стрімкими темпами, адже новачка потрібно фізично з'єднати з усіма існуючими учасниками. Це перетворює монтажні роботи на справжній хаос, робить управління такою інфраструктурою надзвичайно складним завданням

для адміністраторів і вимагає астрономічних бюджетів на закупівлю обладнання. Саме тому часткова сітка виступає ідеальним компромісом. Вона зберігає високий рівень надійності там, де це дійсно необхідно (наприклад, між головними серверами), але дозволяє економити ресурси, підключаючи рядових користувачів за більш простими та дешевими схемами, на кшталт «зірки» або «дерева»[19].

Якщо розглядати цю архітектуру в контексті проєктування комп'ютерної мережі для малого офісу, то побудова повної сітки є абсолютно недоцільною через її невиправдану складність та надмірність. Штатні завдання невеликого підприємства просто не потребують такого рівня резервування. Водночас інтеграція окремих елементів часткової сітки є вкрай розумним кроком. Наприклад, прокладання додаткового резервного кабелю між двома головними офісними комутаторами або створення дублюючого маршруту до файлового сервера гарантуватиме, що у разі пошкодження основної лінії робота офісу не зупиниться. Більш наочно оцінити специфіку цієї архітектури допоможе наведений нижче комплексний аналіз, табл.1.5.

Таблиця 1.4 – Аналітичний огляд експлуатаційних властивостей сітчастої архітектури

Критерій оцінки	Технічна специфіка та архітектурні особливості
Логіка маршрутизації трафіку	Інформація передається через множинні паралельні канали; система здатна динамічно обирати найшвидший та найбезпечніший шлях з десятків доступних.
Вимоги до апаратної бази	Критично високі. Для повної сітки кожен пристрій повинен мати величезну кількість мережевих інтерфейсів (портів) для прямого підключення до сусідів.
Ступінь відмовостійкості	Безпрецедентно високий. Фізичне руйнування кількох ліній зв'язку або поломка окремих вузлів жодним чином не впливає на цілісність мережі в цілому.

Локалізація несправностей	Здійснюється відносно просто: пошкоджена ділянка легко ізолюється системою, при цьому адміністратор може проводити ремонт без зупинки робочих процесів.
Складність проєктування та монтажу	Максимальна для повної архітектури (через павутину кабелів) та помірна для часткової (де дублюються лише головні магістралі).
Еластичність та розширення	Вкрай обмежена. Інтеграція нових робочих місць у повну сітку супроводжується геометричним зростанням кількості необхідних з'єднань, що швидко вичерпує ліміт портів.
Економічний аспект впровадження	Вимагає найбільших фінансових вкладень з-поміж усіх топологій через шалені витрати на метраж кабелю та преміальне багатопортове обладнання.
Пропускна здатність та затримки	Стабільно максимальна, оскільки розумне балансування навантаження між резервними лініями повністю запобігає перевантаженню мережі.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ІНТЕГРАЦІЄЮ VLAN ТА СЕРВЕРНОЇ ІНФРАСТРУКТУРИ

2.1 Формулювання технічного завдання та обґрунтування архітектурних вимог до проєктування локальної мережі

Об'єктом дослідження та впровадження мережевої інфраструктури виступає приватне підприємство «Веб-Інтеграція», ключовим профілем діяльності якого є повний цикл розробки, технічного супроводу, контентного наповнення та надання послуг корпоративного хостингу для веб-сайтів і порталів електронної комерції різноманітних фінансових установ та громадських організацій. Стратегічною метою модернізації є консолідація розрізнених робочих місць усіх структурних підрозділів у єдиний, керований та високопродуктивний інформаційний простір. Проєкт передбачає розгортання комплексу сучасних мережевих і серверних служб, які гарантуватимуть надійну комунікацію між робочими станціями на локальному рівні. Водночас критичною вимогою для ІТ-компанії є забезпечення безперебійного та захищеного доступу до сервісів глобальної мережі Інтернет, що дозволить співробітникам максимально ефективно взаємодіяти із зовнішніми репозиторіями, хмарними середовищами та інструментами веб-розробки.

Для забезпечення високого рівня керованості інфраструктури, оптимізації навантаження від широкомовного трафіку та дотримання жорстких політик інформаційної безпеки, архітектурним планом передбачено логічну декомпозицію єдиного фізичного середовища. Замість використання застарілої "плоскої" топології, загальна локальна мережа розбивається на менші, ізольовані віртуальні підмережі з використанням технології VLAN

(згідно зі стандартом IEEE 802.1Q). Ці логічні групи повністю віддзеркалюють організаційну та адміністративну структуру підприємства. На основі глибокого аналізу внутрішніх інформаційних потоків ПП «Веб-Інтеграція» та з урахуванням суворих вимог до захисту комерційної таємниці, було розроблено комплексну багаторівневу модель розмежування доступу.

Відповідно до цієї моделі, комутаційне обладнання налаштовується на підтримку чітко визначених категорій користувачів, кожна з яких розміщується у власному ізольованому сегменті. Зокрема, створюється виділений захищений VLAN для відділу програмування, де локалізуються процеси написання коду та тестування на внутрішніх серверах розробки. Співробітники відділу дизайну виділяються в іншу підмережу, архітектура якої передбачає підвищену пропускну здатність для постійного обміну об'ємними графічними файлами з корпоративним файловим сховищем. Менеджери та маркетологи об'єднуються у свій сегмент із налаштованим доступом до серверів CRM-систем. Фахівці з SEO-оптимізації, спеціалісти технічної підтримки, співробітники відділу контентного наповнення та керівники проєктів групуються у спільний логічний пул, оптимізований для оперативної міжвідомчої комунікації[20].

Окремої уваги при проєктуванні вимагає фінансовий блок: для бухгалтерії створюється максимально захищений VLAN із впровадженням суворих списків контролю доступу (ACL) на рівні ядра мережі. Це повністю унеможливлює будь-яке несанкціоноване звернення до фінансових баз даних та бухгалтерських серверів з боку інших відділів. Завершують логічну топологію привілейовані сегменти для заступника директора та безпосередньо директора підприємства. Ці віртуальні підмережі отримують найвищий пріоритет якості обслуговування трафіку (QoS) та забезпечують керівництву безпечний, наскрізний доступ до систем аналітики, відеонагляду та управління всією інформаційною інфраструктурою компанії.

2.2 Обґрунтування вибору активного комутаційного обладнання, серверної платформи та пасивної інфраструктури

Проєктування надійної локальної мережі для ПП «Веб-Інтеграція» вимагає ретельного підбору апаратної бази, здатної забезпечити високу продуктивність маршрутизації між VLAN, стабільну роботу серверного сегмента та загальну відмовостійкість системи. Під час вибору обладнання було проведено аналіз сучасних рішень корпоративного класу, що дозволило відмовитися від використання застарілих пристроїв (таких як комутатори серій HP V1910 чи Cisco 3750, а також маршрутизаторів ранніх поколінь) на користь актуальних моделей, що підтримують розширені функції управління трафіком та апаратну маршрутизацію пакетів на швидкостях портів. Усі порівняльні табличні дані були трансформовані в комплексні технічні вимоги для побудови цілісної логічної архітектури.

Для забезпечення ефективної взаємодії між різними віртуальними підмережами відділів розробки, дизайну та адміністрації, в якості ядра мережі (Core/Distribution Layer) було обрано сучасний керований комутатор третього рівня (L3) Cisco Catalyst 9200L. Цей пристрій відповідає за динамічну та статичну маршрутизацію між VLAN, агрегацію каналів зв'язку від комутаторів доступу та впровадження списків контролю доступу (ACL) для захисту фінансового і серверного сегментів. Згідно з технічною документацією виробника, пристрій оснащений двадцятьма чотирма гігабітними портами та чотирма оптичними інтерфейсами SFP+ (з пропускною здатністю 10 Гбіт/с), що гарантує відсутність вузьких місць під час передачі об'ємних баз даних. Комутатор має внутрішню пропускну здатність матриці понад 104 Гбіт/с, оснащений багатоядерним процесором, сучасним стеком протоколів безпеки на базі операційної системи Cisco IOS XE та підтримує резервування джерел живлення. Зовнішній вигляд пристрою наведено на рис.2.1.



Рисунок 2.1 – Сучасний корпоративний комутатор рівня агрегації та маршрутизації (Cisco Catalyst серії 9200L)

Для рівня доступу (Access Layer), до якого безпосередньо підключаються робочі станції співробітників ПП «Веб-Інтеграція» у відповідних портах VLAN, доцільно використовувати лінійку комутаторів Cisco Catalyst 1000-24T. Відмова від застарілих моделей рівня SOHO (на кшталт D-Link DGS-1216T) обумовлена необхідністю жорсткого дотримання стандарту IEEE 802.1Q на рівні кожного порту, а також підтримки протоколів сімейства Spanning Tree (MSTP/RSTP) для запобігання утворенню мережевих петель. Кожен такий комутатор забезпечує двадцять чотири мідні порти 10/100/1000 Мбіт/с та високошвидкісні Uplink-інтерфейси для підключення до центрального ядра. Обладнання має пасивну (безвентиляторну) систему охолодження, що дозволяє розміщувати його безпосередньо в робочих зонах без створення додаткового шумового навантаження, забезпечуючи при цьому повноцінне віддалене керування через протоколи SNMP та SSH. Зовнішній вигляд комутатора рівня доступу наведено на рис.2.2.



Рисунок 2.2 – Зовнішній вигляд керованого комутатора рівня доступу для підключення робочих станцій (Cisco Catalyst серії 1000)

Функції організації безпечного виходу в глобальну мережу Інтернет, термінації VPN-тунелів для віддалених працівників та загального захисту

периметра мережі покладено на високопродуктивний апаратний маршрутизатор MikroTik CCR2004-16G-2S+. Це актуальне рішення операторського класу, яке прийшло на зміну попереднім поколінням (таким як серія RB1100). Пристрій працює під управлінням сучасної операційної системи RouterOS версії 7 (рівень ліцензії 6) і побудований на базі потужного 64-бітного чотирьохядерного процесора AL32400. Маршрутизатор оснащений шістнадцятьма гігабітними портами та двома роз'ємами SFP+ для підключення магістральних оптичних ліній від інтернет-провайдерів. Наявність 4 ГБ оперативної пам'яті типу DDR4 та двох резервованих блоків живлення дозволяє йому без затримок обробляти складні правила брандмауера, глибоку інспекцію пакетів та апаратне шифрування IPsec для захищеного зв'язку з хмарними сервісами. Зовнішній вигляд маршрутизатора наведено на рис.2.3.



Рисунок 2.3 – Високопродуктивний апаратний маршрутизатор та шлюз безпеки мережі (MikroTik CCR2004-16G-2S+)

Основою обчислювальної інфраструктури, що забезпечує функціонування внутрішніх сервісів підприємства (контролер домену, файлове сховище, бази даних та платформи для тестування веб-проєктів), виступає сучасна серверна платформа HPE ProLiant DL360 Gen11. На відміну від морально застарілих серверів попередніх поколінь, ця модель формату 1U призначена для інтенсивних навантажень та глибокої віртуалізації (на базі гіпервізорів VMware ESXi або Microsoft Hyper-V). Сервер комплектується масштабованими процесорами лінійки Intel Xeon Scalable 4-го покоління,

оперативною пам'яттю стандарту DDR5 (з можливістю розширення до кількох терабайт) та апаратним RAID-контролером. Дискова підсистема базується на поєднанні швидкісних твердотільних накопичувачів NVMe для операційних систем і баз даних та ємних SAS-дисків корпоративного класу для зберігання резервних копій і архівів проєктів відділу контенту. Сервер оснащений інтегрованою багатопортовою мережевою картою, яка налаштовується в режимі агрегації (LACP) для забезпечення відмовостійкого підключення до серверного VLAN. Зовнішній вигляд серверного обладнання наведено на рис.2.4.



Рисунок 2.4 – Сучасний сервер формату 1U для розгортання віртуалізованої корпоративної інфраструктури (HPE ProLiant DL360 Gen11)

Фізичний фундамент локальної мережі будується на базі оновленої високоякісної пасивної інфраструктури. Враховуючи вимоги до пропускної здатності та потенціал майбутнього масштабування до стандартів 10 Gigabit Ethernet, у проєкті замість застарілого кабелю категорії 5e використовується неекранована вита пара (UTP) категорії 6a. Центром комутації виступає телекомунікаційна шафа стандарту 19 дюймів ємністю 24U, у якій монтуються патч-панелі відповідної категорії, металеві кабельні організатори для правильного укладання шнурів, а також блоки безперебійного живлення (UPS). Використання якісної мідної інфраструктури та строге дотримання стандартів монтажу гарантує відсутність електромагнітних наведень,

стабільну роботу мережевих протоколів на канальному рівні та повну відповідність фізичної топології запланованій логічній структурі VLAN.

2.3 Проєктування фізичної топології мережевої інфраструктури та схеми кабельних трас підприємства

Фундаментальним етапом проєктування будь-якої корпоративної обчислювальної мережі є обґрунтований вибір її фізичної топології, оскільки саме вона визначає базову архітектуру прокладання кабельних трас, просторове розташування комутаційних вузлів та загальну надійність зв'язків між робочими станціями і серверним ядром. Для розгортання інформаційної інфраструктури приватного підприємства «Веб-Інтеграція», яка базується на актуальних стандартах сімейства Gigabit Ethernet, найбільш доцільним та технологічно виправданим рішенням є використання фізичної топології типу «розширена зірка» (Extended Star). Ця архітектурна модель концептуально віддзеркалює сучасний підхід до ієрархічної побудови мереж. Згідно з цим підходом, центральний комутатор третього рівня або маршрутизатор виконує роль головного вузла агрегації (ядра), до якого високошвидкісними магістральними каналами підключаються комутатори рівня доступу. Саме останні безпосередньо забезпечують підключення кінцевих пристроїв користувачів та серверного обладнання у відповідних відділах.

Вибір саме такої топології зумовлений низкою критично важливих експлуатаційних характеристик, які формують основу стабільної та безперервної роботи сучасного IT-підприємства. Насамперед, архітектура розширеної зірки забезпечує безпрецедентний рівень локальної відмовостійкості на периферії: у разі фізичного пошкодження або обриву мідного кабелю, що веде до конкретного комп'ютера, ізолюється виключно ця робоча станція, тоді як уся інша мережа продовжує функціонувати без жодних

втрат пакетів. Крім того, така схема відзначається високим ступенем гнучкості та модульності при масштабуванні. Додавання нових робочих місць або навіть цілих відділів вимагає лише прокладання кабелю до найближчого комутатора доступу без необхідності реструктуризації всієї мережі.

З точки зору системного адміністрування та інформаційної безпеки, ієрархічна структура у формі розширеної зірки значно спрощує процеси моніторингу трафіку, оскільки всі інформаційні потоки сходяться до чітко визначених вузлів. Найважливішою перевагою у контексті теми даної роботи є те, що фізична розширена зірка слугує ідеальним фундаментом для накладання логічної структури віртуальних локальних мереж. Вона дозволяє гнучко сегментувати порти на комутаторах доступу (присвоюючи їм відповідні теги VLAN) та централізовано маршрутизувати або блокувати трафік між цими сегментами на рівні центрального комутатора ядра за допомогою списків контролю доступу (ACL). Економічна ефективність такого рішення також є високою, оскільки вартість кабельної продукції та портів комутаторів доступу на сьогодні є цілком прийнятною для бюджету малого бізнесу.

Незважаючи на беззаперечні переваги, класична топологія розширеної зірки має один суттєвий архітектурний ризик, який полягає в наявності потенційної єдиної точки відмови (Single Point of Failure). У разі критичної апаратної поломки центрального магістрального комутатора відбувається повна зупинка обміну даними між усіма підмережами та відділами компанії. Проте в сучасних реаліях, за умови використання підібраного в попередньому підрозділі високотехнологічного обладнання корпоративного класу, цей ризик зведено до мінімуму. Актуальні комутатори ядра відзначаються надзвичайно високим показником середнього часу напрацювання на відмову (MTBF), а стабільність їхньої роботи підкріплюється використанням джерел безперебійного живлення, дублюванням магістральних ліній (LACP) та надійною пасивною інфраструктурою.

Візуальне представлення обраної архітектурної моделі, яке демонструє ієрархічні зв'язки між головним розподільчим вузлом, комутаторами відділів та кінцевим клієнтським обладнанням, наведено на рис. 2.5.

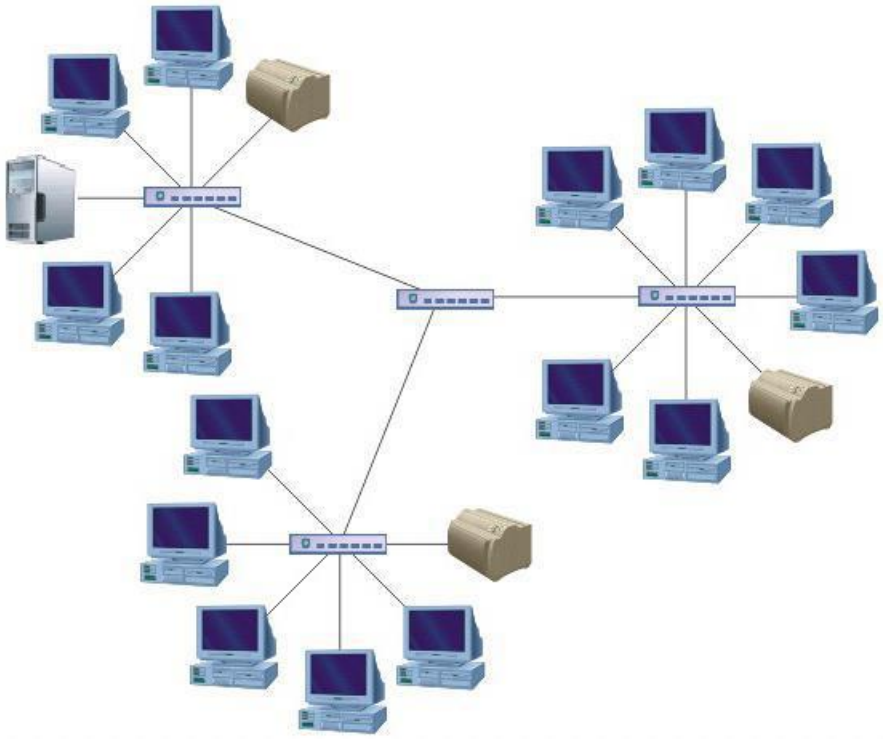


Рисунок 2.5 – Структурна схема організації мережевої інфраструктури на базі фізичної топології типу «розширена зірка»

3 ПРОЄКТУВАННЯ ЛОГІЧНОЇ АРХІТЕКТУРИ, НАЛАШТУВАННЯ СЕГМЕНТАЦІЇ VLAN ТА ПРОГРАМНА КОНФІГУРАЦІЯ АКТИВНОГО МЕРЕЖЕВОГО ОБЛАДНАННЯ

3.1 Планування простору IP-адресації, розробка логічної моделі VLAN та конфігурація інтерфейсів комутаційного обладнання

Створення відмовостійкої та захищеної локальної мережі для ПП «Веб-Інтеграція» вимагає переходу від фізичної архітектури до побудови глибоко продуманої логічної топології. Основою цього процесу є сегментація єдиного широкомовного простору на незалежні віртуальні локальні мережі (VLAN) згідно з раніше визначеною організаційною структурою підприємства. Кожному структурному підрозділу, а також виділеному серверному ядру, призначається унікальний ідентифікатор (VLAN ID) та відповідний діапазон логічних IP-адрес. Для забезпечення гнучкості масштабування та спрощення маршрутизації у проєкті обрано приватний адресний простір класу А, а саме мережу 10.0.0.0. Однак, з метою оптимізації розміру широкомовних доменів та запобігання надмірному мережевому трафіку, цей масив розділено на підмережі з маскою 255.255.255.0 (префікс /24). Такий підхід гарантує, що кожен відділ отримує до 254 доступних хостів, чого абсолютно достатньо для поточних потреб і майбутнього розширення штату без необхідності реструктуризації адресації.

З метою адаптації початкових даних до специфіки IT-підприємства, назви деяких відділів були оптимізовані для відповідності реальним процесам розробки та підтримки веб-проєктів. Особлива увага приділяється сегменту з ідентифікатором VLAN 111, який виділено виключно під серверну інфраструктуру (сервер S_1) та прикордонний маршрутизатор (R_1). Ця підмережа є критичною зоною, доступ до якої з інших користувацьких VLAN

буде суворо регламентуватися правилами міжмережевого екранування. Детальний розподіл адресного простору, ідентифікаторів віртуальних мереж та прив'язку до конкретних груп робочих станцій (WS) наведено у табл.3.1. Дана таблиця була структурно модернізована для кращого сприйняття інформації та логічного групування вузлів.

Таблиця 3.1 – Логічна структура віртуальних мереж (VLAN) та план IP-адресації підприємства

Ідентифікатор VLAN	Назва структурного підрозділу / Зони	Діапазон IP-адрес (Маска /24)	Кількість вузлів
101	Відділ технічної підтримки та системного адміністрування	10.10.1.0/24	6
102	Відділ менеджменту та маркетингу	10.10.2.0/24	4
103	Відділ дизайну та контенту	10.10.3.0/24	4
104	Бухгалтерія та фінансовий відділ	10.10.4.0/24	4
105	Відділ SEO-оптимізації	10.10.5.0/24	6
106	Кабінет директора	10.10.6.0/24	1
107	Приймальня та секретаріат	10.10.7.0/24	1
108	Кабінет заступника директора	10.10.8.0/24	1
109	Відділ веб-розробки (Програмісти)	10.10.9.0/24	5

110	Відділ тестування та впровадження (QA)	10.10.10.0/24	4
111	Серверна інфраструктура та ядро мережі	10.10.11.0/24	3

Наступним кроком після логічного розподілу адрес є проєктування фізичних підключень на рівні портів комутаційного обладнання. Згідно з технологією IEEE 802.1Q, порти комутаторів поділяються на два принципово різні типи: порти доступу (Access) та магістральні порти (Trunk). Порти в режимі Access призначені для підключення кінцевого обладнання (комп'ютерів користувачів, серверів, принтерів). Вони передають нетегований трафік, тобто комп'ютер не знає про існування VLAN, а маркування пакетів відповідним ідентифікатором здійснює сам комутатор під час отримання кадру. У свою чергу, магістральні Trunk-порти використовуються для об'єднання комутаторів між собою (зв'язки між комутаторами доступу SW_1, SW_2 та центральним комутатором ядра SW_3). Вони пропускають через себе тегований трафік відразу всіх або дозволених VLAN, гарантуючи, що дані з різних підрозділів не змішаються під час передачі магістральним оптичним або мідним кабелем.

Центральним елементом агрегації виступає комутатор ядра SW_3, до якого не лише підключаються магістральні лінії від периферійних пристроїв, але й безпосередньо комутуються критично важливі вузли: сервер (S_1), шлюз доступу до Інтернету (R_1) та робочі станції керівного складу. Детальна таблиця комутації, яка повністю регламентує режим роботи кожного інтерфейсу та його приналежність до відповідного логічного домену, подана у табл.3.2. Ця таблиця була оптимізована для відображення налаштувань у розрізі кожного мережевого пристрою, що значно спрощує подальше конфігурування обладнання через інтерфейс командного рядка (CLI).

Таблиця 3.2 – Фізична комутація та логічна конфігурація інтерфейсів мережевого обладнання

Обладнання	Номери інтерфейсів (Порти)	Підключені кінцеві вузли / Пристрої	Режим порту (Switchport Mode)	Призначений VLAN
Комутатор SW_1	Порти 1 – 6	Робочі станції WS_1 – WS_6	Access (Доступ)	VLAN 101
Комутатор SW_1	Порти 7 – 10	Робочі станції WS_7 – WS_10	Access (Доступ)	VLAN 102
Комутатор SW_1	Порти 11 – 14	Робочі станції WS_11 – WS_14	Access (Доступ)	VLAN 103
Комутатор SW_1	Порт 15	Зв'язок із ядром мережі (на SW_3)	Trunk (Магістральний)	Усі дозволені (All)
Комутатор SW_2	Порти 1 – 4	Робочі станції WS_15 – WS_18	Access (Доступ)	VLAN 104
Комутатор SW_2	Порти 5 – 10	Робочі станції WS_19 – WS_24	Access (Доступ)	VLAN 105
Комутатор SW_2	Порт 15	Зв'язок із ядром мережі (на SW_3)	Trunk (Магістральний)	Усі дозволені (All)
Комутатор SW_3	Порт 1	Робоча станція WS_25 (Директор)	Access (Доступ)	VLAN 106

Комутатор SW_3	Порт 2	Робоча станція WS_26 (Приймальня)	Access (Доступ)	VLAN 107
Комутатор SW_3	Порт 3	Робоча станція WS_27 (Заступник)	Access (Доступ)	VLAN 108
Комутатор SW_3	Порти 4 – 8	Робочі станції WS_28 – WS_32	Access (Доступ)	VLAN 109
Комутатор SW_3	Порти 9 – 12	Робочі станції WS_33 – WS_36	Access (Доступ)	VLAN 110
Комутатор SW_3	Порти 13 – 15	Сервер S_1, Маршрутизатор R_1	Access (Доступ)	VLAN 111
Комутатор SW_3	Порт 21	Зв'язок із комутатором доступу SW_1	Trunk (Магістральний)	Усі дозволені (All)
Комутатор SW_3	Порт 22	Зв'язок із комутатором доступу SW_2	Trunk (Магістральний)	Усі дозволені (All)

3.2 Програмна конфігурація активного мережевого обладнання та реалізація маршрутизації між VLAN

Після розробки логічної топології та детального розподілу адресного простору, критичним етапом розгортання інформаційної інфраструктури ПП «Веб-Інтеграція» є безпосередня програмна конфігурація комутаторів.

Оскільки в проєкті обґрунтовано використання надійного обладнання корпоративного класу лінійки Cisco Catalyst, базове та розширене налаштування здійснюється через інтерфейс командного рядка (CLI) під управлінням операційної системи Cisco IOS. Головна мета цього етапу — перенести розроблену теоретичну матрицю доступу на фізичні пристрої, забезпечити ізоляцію трафіку на канальному рівні та налаштувати безпечну маршрутизацію пакетів між відділами компанії.

Процес конфігурації периферійного рівня, до якого належать комутатори доступу відділів (SW_1 та SW_2), розпочинається з ініціалізації глобальної бази даних VLAN. Через режим глобальної конфігурації на пристрої створюються відповідні ідентифікатори віртуальних мереж, кожному з яких присвоюється текстова мітка, що репрезентує конкретний структурний підрозділ (наприклад, vlan 101 з іменем TechSupport, vlan 104 з іменем Accounting). Після створення логічної структури здійснюється переведення фізичних інтерфейсів комутатора у режим доступу користувачів (команда switchport mode access) із подальшою жорсткою прив'язкою до конкретного VLAN згідно з раніше наведеною таблицею комутації.

Особлива увага на рівні доступу приділяється налаштуванню магістральних з'єднань. Порти, які фізично з'єднують комутатори SW_1 та SW_2 із центральним ядром мережі (наприклад, 15-й порт на обох пристроях), переводяться в транковий режим (команда switchport mode trunk). На цих портах обов'язково активується стандарт інкапсуляції IEEE 802.1Q. Це налаштування є фундаментальним: воно дозволяє комутатору прикріплювати до кожного мережевого кадру спеціальний тег із номером VLAN перед тим, як відправити його по загальному кабелю до серверної. Завдяки цьому центральний комутатор чітко розпізнає, з якого саме відділу надійшов запит.

Найбільш складним та комплексним елементом програмної конфігурації є ядро мережі — комутатор третього рівня SW_3 (Cisco Catalyst 9200L). Окрім стандартного призначення портів доступу для робочих станцій керівного складу та серверного обладнання (VLAN 106-111), на цей пристрій

покладається функція обробки трафіку між підмережами (Inter-VLAN Routing). За замовчуванням пристрої в різних VLAN не можуть обмінюватися даними. Щоб дозволити, наприклад, відділу розробки звертатися до тестового сервера, на комутаторі SW_3 глобально активується маршрутизація (команда ip routing).

Після активації маршрутизації для кожної віртуальної мережі створюється логічний інтерфейс — Switch Virtual Interface (SVI). Кожному такому інтерфейсу присвоюється перша IP-адреса з відповідного діапазону підмережі. Наприклад, для VLAN 101 створюється інтерфейс interface vlan 101, якому призначається адреса 10.10.1.1 із маскою 255.255.255.0. Ця логічна адреса інтегрується безпосередньо в процесор комутатора ядра і виступає в ролі шлюзу за замовчуванням (Default Gateway) для всіх комп'ютерів відповідного відділу. Таким чином, коли комп'ютер бухгалтера намагається передати звіт на центральний файловий сервер (VLAN 111), пакет спочатку надходить на шлюз свого VLAN, а комутатор ядра, аналізуючи внутрішню таблицю маршрутизації, перенаправляє його у серверний сегмент.

Завершальним кроком конфігурації є забезпечення базової мережевої безпеки та виходу в глобальну мережу. На рівні ядра (SW_3) впроваджуються розширені списки контролю доступу (Extended ACL), які застосовуються до віртуальних інтерфейсів SVI. Ці політики фізично блокують спроби ініціалізації з'єднань з непріоритетних відділів (наприклад, маркетологів) до серверів з вихідним кодом проєктів чи фінансових баз даних, дозволяючи при цьому легітимний трафік. Для зв'язку підприємства із зовнішнім світом на комутаторі SW_3 прописується статичний маршрут останньої надії (Default Route), який спрямовує всі невідомі запити (наприклад, звернення до веб-сайтів в Інтернеті) на прикордонний маршрутизатор MikroTik R_1. Там ці пакети проходять процес трансляції мережевих адрес (NAT) та інспектуються корпоративним фаєрволом, що завершує повний цикл безпечної маршрутизації даних у мережі.

3.3 Моделювання комплексної мережевої інфраструктури та візуалізація логічної топології підприємства

Для практичної перевірки розробленої логічної архітектури, підтвердження коректності розподілу адресного простору та верифікації налаштувань віртуальних локальних мереж (VLAN), фінальним етапом проєктування є створення деталізованої імітаційної моделі. Візуалізація топології в спеціалізованому програмному середовищі дозволяє наочно продемонструвати ієрархічні зв'язки між усіма активними та пасивними вузлами корпоративної мережі підприємства «Веб-Інтеграція». Побудована модель повністю підтверджує правильність вибору концепції «розширеної зірки» та ілюструє інтеграцію робочих станцій користувачів, комутаційного обладнання рівня доступу, серверного сегмента та прикордонного маршрутизатора в єдину, функціонально завершену інформаційну екосистему.

Як показано на розробленій схемі, рис. 3.1, центральним ядром комутації виступає багатошаровий магістральний комутатор третього рівня (Multilayer Switch). Цей вузол відіграє найважливішу роль у всій інфраструктурі: він відповідає за високошвидкісну апаратну маршрутизацію трафіку між ізольованими підмережами різних відділів (Inter-VLAN Routing) та агрегацію інформаційних потоків. Саме до ядра мережі безпосередньо підключено виділений корпоративний сервер (Server1), що утворює захищений серверний сегмент для зберігання баз даних та веб-проєктів. Крім того, до центрального комутатора під'єднано прикордонний маршрутизатор (Router1), який слугує шлюзом для трансляції внутрішніх адрес (NAT) та забезпечує захищений вихід усієї локальної інфраструктури у глобальну мережу Інтернет. Для забезпечення мінімальних затримок (latency) безпосередньо до портів ядра також підключені робочі станції керівництва та критично важливих відділів розробки (PC25 – PC36).

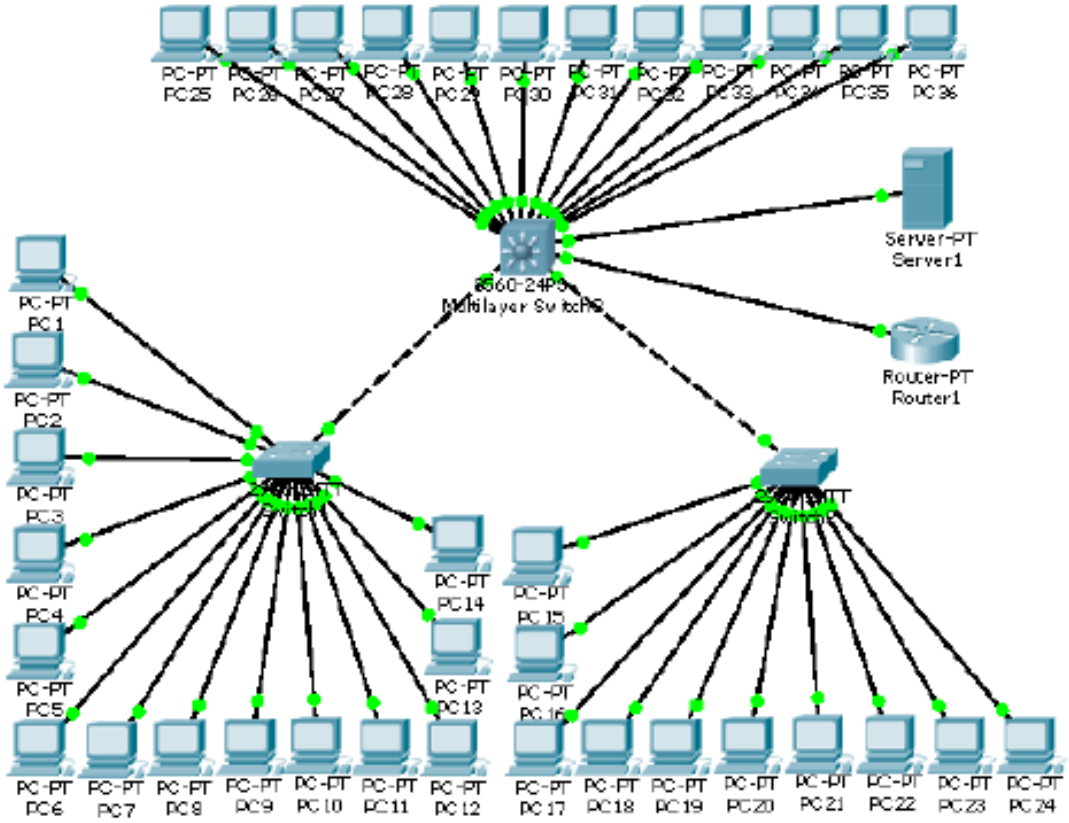


Рисунок 3.1 – Імітаційна модель та логічна топологія локальної обчислювальної мережі підприємства

Нижній ієрархічний щабель моделі формує рівень доступу, який реалізовано на базі підпорядкованих комутаторів другого рівня (Switch1 та Switch2). Ці пристрої з'єднуються з головним магістральним комутатором за допомогою транкових (Trunk) каналів зв'язку. Відповідно до стандарту 802.1Q, ці транкові лінії виконують функцію мультиплексування: вони здатні одночасно передавати теговані кадри від різних віртуальних мереж єдиним фізичним кабелем. До портів доступу (Access ports) периферійних комутаторів підключені робочі станції рядових співробітників підприємства (PC1 – PC24). Кожен із цих комп'ютерів логічно прив'язаний до свого конкретного VLAN (бухгалтерія, маркетинг, дизайн тощо), що унеможливлює несанкціоноване перехоплення широкомовних запитів між відділами.

Підсумовуючи результати проєктування, можна стверджувати, що змодельована топологія повністю задовольняє технічне завдання та вимоги

щодо інформаційної безпеки ПП «Веб-Інтеграція». Вона забезпечує сувору ізоляцію користувацького трафіку на канальному рівні, гарантує безперебійний доступ до централізованих серверних ресурсів через оптимізовані маршрути та має високий потенціал для подальшого масштабування без необхідності кардинальної перебудови кабельної системи чи заміни активного обладнання.

ВИСНОВКИ

Аналізуючи теоретичні основи та дослідивши практичні вимоги до розгортання інформаційного середовища, можна дійти висновку, що сучасна локальна мережа вимагає глибокого архітектурного планування. В рамках кваліфікаційної роботи було проведено аналіз основних топологій побудови мереж. Визначено, що для потреб малого підприємства найбільш доцільним та технологічно виправданим рішенням є використання фізичної топології типу «розширена зірка». Вона забезпечує високий рівень відмовостійкості на периферії та є ідеальним фундаментом для накладання логічної структури VLAN.

На основі розробленого технічного завдання було спроєктовано локальну обчислювальну мережу для приватного підприємства «Веб-Інтеграція». Здійснено логічну декомпозицію єдиного фізичного середовища на ізольовані віртуальні підмережі відповідно до відділів компанії, що суттєво підвищило рівень інформаційної безпеки.

Для реалізації проєкту було обґрунтовано вибір сучасного обладнання корпоративного класу: магістрального комутатора L3 Cisco Catalyst 9200L для ядра мережі, комутаторів доступу Cisco Catalyst 1000-24T, високопродуктивного маршрутизатора MikroTik CCR2004-16G-2S+ для захисту периметра та серверної платформи HPE ProLiant DL360 Gen11. Було розроблено детальний план IP-адресації та проведено програмну конфігурацію інтерфейсів обладнання.

Фінальне імітаційне моделювання розробленої топології підтвердило коректність маршрутизації між відділами, доступність серверної інфраструктури та повну відповідність проєкту вимогам надійності, масштабованості та безпеки, що висуваються до сучасних корпоративних мереж малого бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі: навчальний посібник. КПІ ім. Ігоря Сікорського, 2020. 336 с.

2 CentOS [електронний ресурс] – URL: https://wiki.centos.org/Manuals/ReleaseNotes/CentOS8.1911

3 Рамський Ю., Олексюк В., Балик А. Адміністрування комп'ютерних мереж та систем. Богдан НК, 2010. 196 с.

4 Методичні вказівки до виконання дипломного проекту за спеціальністю 123 «Комп'ютерна інженерія»

5 Коммутатори HP [електронний ресурс] – URL: http://www.hp.com/rnd/support/manuals/2510.htm

6 Микитишин А.Г., Митник М.М., Стухляк П.Д., В.В. Пасічник. Комп'ютерні мережі: навчальний посібник. Львів: «Магнолія 2006», 2013. 256 с.

7 Охорона праці – Москальова В.М. URL: http://studentbooks.com.ua/ content/view/1327/76/

8 Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій. Київ: КПІ ім. І. Сікорського, 2018. 225 с.

9 Гищук М. В. Основи охорони праці: Підручник. -К.: Кондор, 2005. - 238с.

10 Воробієнко П., Нікітюк Л., Резниченко П. Телекомунікаційні та інформаційні мережі. Саміт-книга, 2010. 640 с.

11 Fluke Networks LinkRunner Pro Network Multimeter. [електронний ресурс] – URL: http://www.testequipmentdepot.com /flukenetworks/network-testers/linkrunner-pro.htm

12 Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Львівська політехніка, 2022. 228 с.

13 MikroTik documentation [електронний ресурс] – URL: http://wiki.mikrotik.com/wiki/Manual :TOC

14 Персональні компютери в мережах TCP/IP. Крейг Хант ; з англ. - BHV-Київ, 2012.

15 Олексюк В., Балик Н., Балик А. Організація комп’ютерної локальної мережі. Тернопіль: Підручники та посібники, 2006. 80 с.

16 Інформація про NAT [електронний ресурс] – URL: https://uk.wikipedia.org/wiki/NAT

17 Жидецький В.Ц. Охорона праці користувачів комп’ютерів. Навчальний посібник. – Вид. 2-ге., доп. – Львів.: Афіша, 2000. – 176с.

18 Zabbix Network Monitoring [електронний ресурс] – URL: https://www.zabbix.com/network_monitoring

19 Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Київ: "Юніор", 2015. 397 с.

20 Сайт забезпечення розрахунку [електронний ресурс] – URL: https://www.proliant.com/

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)