

Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж
Тернопільського національного технічного університету імені Івана Пулюя»

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму
та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: Розробка проєкту комп'ютерної мережі компанії "MidHub"

Виконав: студент IV курсу, групи КІ-406

Спеціальності 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

Соломія КРУШЕЛЬНИЦЬКА

(ім'я та прізвище)

Керівник Ігор КАПАЦІЛА

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

**ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»**

Відділення **інформаційних технологій, менеджменту, туризму
та підготовки іноземних громадян**

Циклова комісія **комп'ютерної інженерії**

Освітньо-професійний ступінь **фаховий молодший бакалавр**

Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**

Спеціальність: **123 Комп'ютерна інженерія**

Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ

Голова циклової комісії
комп'ютерної інженерії

_____ Андрій ЮЗЬКІВ

“30” березня 2026 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТЦІ**

Крушельницькій Соломії Юріївні

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі компанії
“MidHub**

керівник роботи **Капаціла Ігор Богданович**
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 27.03.2026р № 4/9-167.

2. Строк подання студентом роботи: 15 червня 2026 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - “Commercial Building Telecommunications Wiring Standart” і ANSI/EIA/TIA 569 - “Commercial Building Standart for Telecommunications Pathwais and Spaces

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Охорона праці та безпека життєдіяльності.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК викладач		
Охорона праці та безпека життєдіяльності	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	08.05	
3	Написання першого розділу	15.05	
4	Розробка технічного та робочого проекту	22.05	
5	Написання спеціального розділу	28.05	
6	Розрахунок економічної частини	1.06	
7	Написання розділу охорони праці	3.06	
8	Виконання графічної частини	8.06	
9	Оформлення проекту	10.06	
10	Погодження нормоконтролю	11.06	
11	Попередній захист роботи	12.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 31 березня 2026 року

Студент

_____ (підпис)

Керівник роботи

_____ (підпис)

Соломія КРУШЕЛЬНИЦЬКА
(ім'я та прізвище)

Ігор КАПАЦІЛА
ім'я та прізвище)

АНОТАЦІЯ

Розробка комп'ютерної мережі компанії “MidHub” // Кваліфікаційна робота // Крушельницька Соломія // Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя», група КІ-406// Тернопіль, 2026 // с. – 110, рис. –31, табл. – 16, кресл. – 5, додат. – 8.

Ключові слова: корпоративна мережа, MikroTik, VLAN, OSPF, НТВ.

Мета роботи – це розробка комп'ютерної мережі компанії “MidHub”

Пояснювальна записка складається з п'яти розділів.

Перший розділ охоплює технічне завдання, аналіз об'єкта проектування та вимоги до пропускну здатності каналів зв'язку.

У другому розділі обґрунтовано вибір топології, кабельної системи та активного обладнання, виконано розрахунок і розподіл IP-адресного простору.

Третій розділ містить налаштування VLAN, OSPF, NAT, брандмауера та управління трафіком за алгоритмом НТВ, а також методику тестування мережі.

У четвертому розділі розраховано собівартість проектних робіт, капітальні вкладення та термін окупності проекту.

П'ятий розділ присвячено охороні праці: електробезпеці, організації вентиляції та кондиціонування в серверних приміщеннях і протипожежним заходам.

ANNOTATION

Development of a computer network for the "MidHub" company // Qualification work // Krushelnytska Solomiia // Separate structural unit "Ternopil Professional College of Ternopil Ivan Puluj National Technical University", group KI-406 // Ternopil, 2026 // p. – 110, fig. – 31, tabl. – 16, draw. – 5, append. – 8.

Keywords: corporate network, MikroTik, VLAN, OSPF, HTB.

The purpose of the work is the development of a computer network for the "MidHub" company.

The explanatory note consists of five sections.

The first section covers the technical specification, analysis of the design object, and requirements for communication channel bandwidth.

The second section justifies the choice of topology, cabling system, and active equipment, and includes the calculation and distribution of the IP address space.

The third section contains the configuration of VLAN, OSPF, NAT, firewall, and traffic management using the HTB algorithm, as well as the network testing methodology.

The fourth section presents the calculation of project design costs, capital investments, and the project payback period.

The fifth section is dedicated to occupational safety: electrical safety, organization of ventilation and air conditioning in server rooms, and fire prevention measures.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ	9
ВСТУП.....	10
1 ЗАГАЛЬНИЙ РОЗДІЛ.....	11
1.1 Технічне завдання	11
1.1.1 Найменування та область застосування	11
1.1.2 Призначення розробки	11
1.1.3 Вимоги до апаратного та програмного забезпечення	12
1.1.4 Вимоги до документації	13
1.1.5 Техніко-економічні показники	14
1.1.6 Стадії та етапи розробки	15
1.1.7 Порядок контролю та прийому	16
1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі.....	17
2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ	19
2.1 Опис та обґрунтування вибору логічного типу мережі.....	19
2.2 Розробка схеми фізичного розташування кабелів та вузлів	22
2.2.1 Типи кабельних з'єднань та їх прокладка	22
2.2.2 Будова вузлів та необхідність їх застосування.....	24
2.3 Обґрунтування вибору обладнання для мережі.....	27
2.4 Особливості монтажу мережі	43
2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі	44
2.6 Тестування та налагодження мережі	45
3 СПЕЦІАЛЬНИЙ РОЗДІЛ.....	47
3.1 Інструкція з налаштування програмного забезпечення серверів	47

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>					
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	<i>Розробка проекту комп'ютерної мережі компанії "MidHUB" Пояснювальна записка</i>			<i>Літ.</i>	<i>Арк.</i>	<i>Аркушів</i>
<i>Розроб.</i>		Кришельницька С.Ю.								
<i>Перевір.</i>		Капацила І. Б.								
<i>Реценз.</i>										
<i>Н. Контр.</i>										
<i>Затверд.</i>					ВСП "ТФК ТНТУ" КІ-406 м. Тернопіль					

ВИСНОВКИ	89
ПЕРЕЛІК ПОСИЛАНЬ	90
ДОДАТКИ.....	93
Додаток А. Схема логічної топології мережі компанії "MidHub"	93
Додаток Б. Схема фізичної топології мережі компанії "MidHub"	94
Додаток В. Лістинг конфігурації комутатора SW_1	95
Додаток Г. Лістинг конфігурації комутатора SW_3.....	97
Додаток Д. Лістинг конфігурації комутатора SW_2.....	100
Додаток Е. Лістинг конфігурації маршрутизатора R_1.....	103
Додаток Є. Лістинг конфігурації точки доступу AP_1.....	107
Додаток Ж. Лістинг конфігурації точки доступу AP_2.....	109

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

AD (Active Directory) – служба каталогів для централізованого управління;

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного налаштування вузла;

DNS (Domain Name System) – система доменних імен;

FTP (File Transfer Protocol) – протокол передачі файлів;

HTB (Hierarchical Token Bucket) – алгоритм керування смугою пропускання.

IEEE 802.11ax – міжнародний стандарт бездротових мереж (Wi-Fi 6);

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

LLM (Large Language Model) – велика мовна модель (сервер штучного інтелекту);

MAC (Media Access Control) – апаратна адреса пристрою;

MPTL (Modular Plug Terminated Link) – модульний лінк із вишкою на кінці; PoE (Power over Ethernet) – технологія передачі живлення по крученій парі; SMB (Server Message Block) – мережевий протокол спільного доступу до файлів;

NAT (Network Address Translation) – трансляція мережевих адрес;

SNMP (Simple Network Management Protocol) – протокол керування та моніторингу мережі;

STP (Shielded Twisted Pair) – кабель типу екранована скручена пара;

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара; VLAN (Virtual Local Area Network) – віртуальна локальна комп'ютерна мережа;

VPN (Virtual Private Network) – віртуальна приватна мережа;

ЛОМ – локальна обчислювальна мережа;

ОС – операційна система;

ПЗ – програмне забезпечення;

СКС – структурована кабельна система;

									Арк.
									9
Змн.	Арк.	№ док.м.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ				

ВСТУП

Функціональне призначення теперішніх мереж вийшло далеко за межі звичайного доступу до веб-ресурсів та стало фундаментом для складних систем. Сучасна мережа повинна гарантувати високу пропускну здатність, мінімальні затримки мережі при передачі важливої інформації, забезпечувати сегментацію трафіку для підвищення рівня безпеки та підтримувати високий рівень відмовостійкості.

Комп'ютерна мережа – це система зв'язку між двома чи більше комп'ютерами, периферійними пристроями, мобільними телефонами та засобами автоматизації. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи бездротове середовище [9].

Мережі компаній використовують можливість колективної роботи в локальній мережі, але з доступом до глобальної. Таким чином, створюється певна екосистема, де швидкість обміну даними впливає на загальну продуктивність всього колективу. Ефективність використання локальних ресурсів разом із стабільним виходом у глобальну мережу дозволяє автоматизувати більшу частину роботи, забезпечуючи миттєвий доступ до хмарних сервісів, баз даних та систем віддаленої взаємодії. Оптимізація є ключовим фактором, вона дозволяє усунути часові затримки при обробці запитів та гарантувати безперебійну роботу всіх ланок компанії.

Метою кваліфікаційної роботи є розробка проєкту комп'ютерної мережі компанії “MidHub”. В цій роботі буде розроблено комплекс документації для планування, впровадження системи, валідації та верифікації параметрів мережі, що є надзвичайно важливим для забезпечення стабільної життєдіяльності ІТ-інфраструктури.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ док.м.</i>	<i>Підпис</i>	<i>Дата</i>		10

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Тема кваліфікаційної роботи полягає у розробці проєкту комп'ютерної мережі компанії "MidHub". Ця розробка призначена для впровадження в конкретній компанії. Проте її складові, зокрема розроблені алгоритми дій, є універсальними та можуть бути експортовані в бізнес-процеси невеликих фірм або компаній для підвищення їхньої ефективності.

1.1.2 Призначення розробки

Основним завданням розробки є створення цілісної мережі, яка забезпечить об'єднання робочих станцій, організацію швидкісного зв'язку між робочими станціями та серверами, налаштування безпечного та стабільного виходу в Інтернет та створення фундаменту для впровадження автоматизованих систем управління і моніторингу мережевої активності.

Призначення кваліфікаційної роботи полягає у створенні єдиного інформаційного простору, який об'єднує 37 робочих станцій, забезпечуючи швидку взаємодію між відділами компанії.

Архітектурно розробка базується на використанні трьох комутаторів, де один з них виконує роль ядра для агрегації трафіку та централізованого управління, тоді як інші забезпечують стабільне підключення робочих станцій та іншого мережевого обладнання.

Також в роботі задіяно дві точки доступу з підтримкою сучасних протоколів бездротового зв'язку для забезпечення мобільності співробітників та гнучкості робочих процесів.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
						11
<i>Змн.</i>	<i>Арк.</i>	<i>№ докum.</i>	<i>Підпис</i>	<i>Дата</i>		

Бездротовий зв'язок дозволяє організувати безпечний доступ до мережі з будь-якої точки офісу, що є необхідним для ІТ-компаній.

Не менш важливим функціональним пріоритетом є інтеграція потужного серверного сегмента, що включає сервер збереження інформації, призначений для ведення корпоративних баз і надійного архівування даних, також спеціалізований сервер штучного інтелекту, що забезпечує необхідні обчислювані потужності для розгортання та донавчання LLM-моделей. Це дозволить компанії реалізовувати повний цикл розробки складних продуктів у межах власної інфраструктури. Окрім того, якщо в подальшому компанія захоче розширитись, то запропоноване рішення дозволяє зробити це без повної перебудови структури.

1.1.3 Вимоги до апаратного та програмного забезпечення

Оскільки, розробка цього проєкту направлена на потужну ІТ-компанію, то вимоги до апаратної та програмної частини повинні бути відповідні. Програмне забезпечення – це набір інструкцій, які виконуються на комп'ютері, а апаратна частина – це фізичні компоненти, які ці інструкції виконують [13].

Вимоги до програмного забезпечення:

- стабільне виконання прикладного ПЗ під сильним навантаженням, підтримка багатокористувацького режиму;
- забезпечення правильної роботи протоколів мережі, щоб забезпечити стабільну взаємодію пристроїв із центральними серверами;
- безперешкодне об'єднання програмного середовища та GPU-обчислень для роботи LLM-моделей;
- надійний захист інформації від несанкціонованого втручання та розмежування політик доступу;
- регулярне формування архівних копій даних та швидкий доступ до спільних ресурсів на сервері;

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		12

- можливість віддаленого моніторингу мережевої безпеки та налаштування конфігурацій;

- компанія має придбану ліцензію Windows Server 2022 та клієнтські ліцензії CAL, що повинно бути враховано при виборі серверного обладнання.

Вимоги до апаратного забезпечення:

- магістраль і порти доступу повинні працювати на швидкості 1 Гбіт/с для безперебійної роботи;

- повинні використовуватись графічні процесори, які забезпечують високу обчислювану потужність для запуску та донавчання LLM-моделей;

- за допомогою ієрархічної структури передбачити можливості масштабування;

- забезпечити логічний розподіл трафіку для розмежування відділів компанії.

1.1.4 Вимоги до документації

Документація комп'ютерної мережі компанії "MidHub" повинна складатись із:

- логічної топології, де зображено як дані передаються по мережі;

- фізичної топології, де показано розміщення всіх мережевих пристроїв, робочих станцій та магістральних каналів;

- плану приміщень, на якому представлено призначення кожної кімнати та її номер;

- таблиці техніко-економічних показників, де розрахована вартість всієї мережі;

- таблиці IP адресації, де вказано назва пристрою чи робочої станції, IP-адреса і маска, шлюз, номер VLAN та назва, фізичне розміщення;

- пояснювальної записки, де описана мережа, її характеристики, вимоги до програмного та апаратного забезпечення.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		13

Таким чином, вся вище перерахована документація дозволяє організувати дані про логічну та фізичну структуру мережі. Також забезпечує фундамент для впровадження і високу ефективність подальшої експлуатації мережі, тим самим мінімізує час на усунення можливих поломок та технічне обслуговування.

1.1.5 Техніко-економічні показники

Мережева інфраструктура, що розробляється для компанії “MidHub”, потребує поєднання високопродуктивного обчислення, ефективного керування ресурсами та відмовостійкості. Під час розробки пріоритетом було забезпечення стабільності роботи при високих навантаженнях та забезпечення безпеки внутрішніх даних.

Основні технічні параметри зосереджені на гігабітному доступі для всіх робочих станцій, дозволяючи організувати безперебійний цикл роботи та швидкий зв'язок до репозиторіїв, що надає стабільну роботу під час постійного обміну трафіком. Також невід'ємною частиною проєкту є сервер адаптований для штучного інтелекту. Таке проєктне рішення надає компанії можливість створювати власні високоінтелектуальні продукти, але надзвичайно важливе є питання безпеки. Коли компанія використовуватиме сторонні сервіси, вона фактично передає всю інформацію на сервери іншої компанії, тому питання конфіденційності вирішується таким чином.

Програмний стек компанії використовує інструменти для підтримки повного циклу впровадження та експлуатації LLM-моделей, що включає в себе елементи автоматизації, системи віртуалізації та спеціалізовані бібліотеки для обчислень. Таким чином, ПЗ гарантує ефективну та стабільну роботу робочих станцій та дозволяє уникнути надзвичайних витрат на комерційні ліцензії.

Економічний підхід до реалізації комп'ютерної мережі опирається на ефективне управління фінансами. Купуючи високоякісне обладнання гарантується високий цикл експлуатації. Також сервер з штучним інтелектом

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		14

також певна інвестиція. Оскільки, компанія більше не залежить від цінової політики інших провайдерів та отримує повний контроль над процесами.

Враховуючи зазначені фактори, параметри проєктованої мережі компанії “MidHub” повинні відповідати наступним вимогам:

- пропускна здатність повинна становити 1 Гбіт/с для всіх робочих станцій;
- сервер штучного інтелекту має підключатись до головного комутатора на високій швидкості 10 Гбіт/с для усунення затримок трафіку;
- головний сервер повинен мати багатоядерну архітектуру для швидкої паралельної обробки запитів;
- виділений сервер потребує значного об’єму оперативної пам’яті для стабільного локального запуску моделей.

Підсумковий техніко-економічний розрахунок включатиме капітальні витрати для придбання обладнання, основного та додаткових серверів, бездротових точок доступу та периферії. Також у розрахунок закладається вартість пасивного обладнання, враховуючи кабельну систему, патч-корди, коробки та розетки. Сукупна вартість усіх зазначених компонентів повинна не перевищувати ліміт у 1 000 000 грн.

Розгортання цієї мережі гарантує надійний фундамент для розширення діяльності компанії. Рішення відповідає стандартам ІТ-систем, прискорюючи випуск програмних продуктів на ринок і є кроком, що сприяє підвищенню технічних можливостей.

1.1.6 Стадії та етапи розробки

Стадії та етапи розробки комп’ютерної мережі [15]:

1. Першим етапом є планування, тобто детальне визначення цілей мережі. Встановлення вимог до пропускної здатності та безпеки даних.

2. Наступним етапом проєктування. На основі минулого етапу розробляються топології мережі. Етап включає розробку таблиці ІР-адресації та

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		15

налаштування мережевих протоколів. Також сюди входить вибір обладнання і кабельної системи, вони повинні забезпечити стабільний зв'язок між секціями.

3. Третім етапом є монтаж і конфігурація. Проводиться практична реалізація, монтаж кабельної системи та встановлення пристроїв. Після цього реалізується налаштування мережевих параметрів. Таких як розмежування VLAN, конфігурація рівнів доступу та підготовка серверів до експлуатації.

4. Четвертим етапом є тестування і відладка. Після завершення конфігурації здійснюється перевірка зв'язку між вузлами та швидкості обміну трафіком. Особлива увага приділяється безпеці та усуненню помилок.

5. Останнім етапом є обслуговування і моніторинг. Після введення мережі в експлуатацію необхідно забезпечити супровід системи. Сюди входить впровадження резервного копіювання даних, оновлення ПЗ, застосування засобів моніторингу для попередження інцидентів та відстеження продуктивності.

1.1.7 Порядок контролю та прийому

Введення мережі в експлуатацію передбачає здійснення випробувань для підтвердження правильності встановленого обладнання. Щоб забезпечити надійність роботи мережі та відповідність технічним вимогам, контроль здійснюється поетапно [15]:

1. Перевірити маркування робочих станцій та мережевого обладнання на відповідність з вказаним в документації.

2. Перевірити надійність встановлення обладнання та цілісність термінування кабельних ліній.

3. Перевірити правильність видачі IP-адрес маршрутизатором R_1 та доступність серверів з відповідних сегментів.

4. Перевірити правильність обробки DNS-запитів і наявність зовнішнього інтернет-шлюзу.

5. Перевірити пропускну здатність каналів передачі даних між робочими станціями та сервером.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		16

6. Перевірити доступність ресурсів графічного процесора для забезпечення продуктивної роботи обчислень LLM-моделей.

По завершенню всіх етапів необхідно скласти акт випробувань, де буде зафіксовано результати доступності всіх мережевих вузлів.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі.

У цій роботі описується проектування мережі для ІТ-компанії. Вона займається розробкою програмних рішень з використанням власної технології штучного інтелекту. Надмірне зростання в сфері ІТ ставить нелегку задачу сучасному підприємству. На сьогоднішній день мало просто виконувати базову мережеву комунікацію, необхідна високопродуктивна платформа, яка зможе справлятися з надмірними обчислювальними процесами та обробкою великих обсягів даних.

Підприємство розташоване в бізнес-центрі, план приміщення представлений в графічній частині кваліфікаційної роботи 2026.КВР.123.406.11.00.00 ПП. Ця компанія містить тридцять сім робочих місць та має наступні відділи:

- відділи DevOps;
- відділ тестування;
- маркетингу;
- бухгалтерії;
- HR-відділ.

Також присутня кімната для співбесід та окремі дві кімнати, де можна провести конференцію окремо від інших працівників.

Локальна обчислювана мережа (ЛОМ) для ІТ-компанії повинна відповідати високим вимогам. Вона повинна забезпечити централізоване зберігання і безпеку даних, швидке передавання інформації та стабільний зв'язок із зовнішньою мережею. Не менш важливим аспектом є можливість масштабування, розширення структури не повинно призводити до високих капітальних витрат.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		17

Крім того, якщо в майбутньому підключатимуться нові вузли, то це не повинно призводити до падіння ефективності та продуктивності мережі.

Наступна вимога це є максимальне використання можливостей програмного та апаратного забезпечення для інтенсивнішої обробки даних.

Основним рішенням архітектури цієї ЛОМ є централізована схема, в якій всі блоки з'єднанні через головний комутатор. Для того, щоб оптимізувати кабельну інфраструктуру та збалансувати навантаження робочі станції та точки доступу згруповані в блоки на основі їх розташування в офісі.

Перший блок складається з комутатора другого рівня, що з'єднує два відділи DevOps. Оскільки, ці відділи працюють із розгортанням сервісів та здійсненням передачі великих обсягів даних, цей блок потребує стабільного дротового з'єднання.

Другий блок реалізований з окремим комутатором доступу для відділів керівництва та бухгалтерії. Такий розподіл дозволяє логічно та фізично відокремити фінансовий трафік від загального.

Третій блок стосується точки доступу, яка забезпечує покриття в трьох зонах: тестовій зоні та у двох DevOps-відділах. Це дозволяє спеціалістам не бути прив'язаним до свого робочого місця разом із тим використовувати певні портативні пристрої.

Четвертий блок також точка доступу яка покриває відділ кадрів та маркетингу. Перевага такого поєднання полягає в гнучкості роботи з клієнтами і персоналом. До того ж дає можливість організувати гостьовий доступ.

У центрі цієї мережі знаходиться головний комутатор, який об'єднує всі ці пристрої за допомогою двох комутаторів та двох точок доступу. Також до головного комутатора підключений маршрутизатор, який дозволяє підключатись до глобальної мережі Інтернет і відіграє роль мережевого захисту, та два сервери – один з них спеціалізується на обробці запитів штучного інтелекту, інший – для зберігання даних та резервного копіювання. Вони потребують швидкого обміну даними з іншими блоками для продуктивної роботи компанії. Така архітектура реалізовується для централізованого управління всіма робочими станціями.

									Арк.
									18
Змн.	Арк.	№ док.м.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ				

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

При виборі топології потрібно враховувати наступні фактори [12]: інтенсивність трафіку, пропускна здатність, тип з'єднань, агрегація потоків даних, метод доступу до середовища передачі також на можливість масштабованості обсягів зберігання.

Топологією називається структура взаємозв'язків пунктів і з'єднуючих їх ліній. Топологія фізичних зв'язків відображає схему з'єднань елементів мережі. Логічна топологія відображає розподіл інформаційних потоків між вузлами. Фактично логічна топологія визначає алгоритм, згідно із яким мережеві вузли будуть здійснювати доступ до середовища передачі даних [3].

Для визначення найоптимальнішої структури побудови ЛОМ компанії, здійснено порівняння наступних топологій: “шина”, “кілеце”, “розширена зірка”.

Спільна шинна є доволі розповсюдженою топологією. Ця топологія побудована на одному коаксіальному кабелі, до якого приєднуються всі пристрої. Передача даних в такому типі мережі є ширококомвною, тому канали закінчуються пасивними терміналами, які поглинають передані сигнали [3].

На рисунку 2.1 зображено вигляд цієї топології.

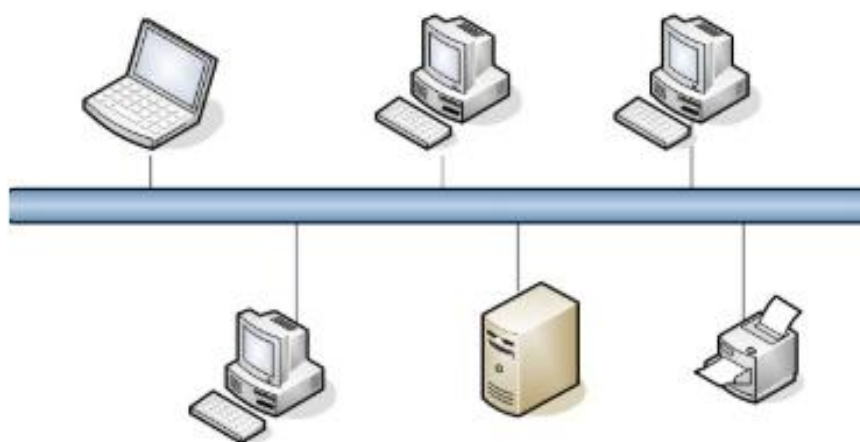


Рисунок 2.1 – Шинна топологія

Змн.	Арк.	№ докцм.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

19

Основні недоліки:

- не передбачена масштабованість;
- низька продуктивність, ця топологія виконує одночасну передачу даних лише з одної робочої станції;
- якщо виникає якась проблема, її важко знайти і тоді перестає працювати вся мережа.

Переваги:

- легко налаштовується та встановлюється;
- доволі дешева, якщо встановлюється не на великі відстані;
- якщо ламається робоча станція, то мережа працює, як і працювала.

Наступна топологія – кільце. Ця топологія визначається тим, що дані передаються по колу в одному напрямку. Відповідно, якщо комп'ютер бачить свою MAC-адресу, то копіює дані в буфер. Вузли підключаються до регенераторів сигналу, таким чином утворюють логічне кільце.

На рисунку 2.2 зображено топологію кільце.

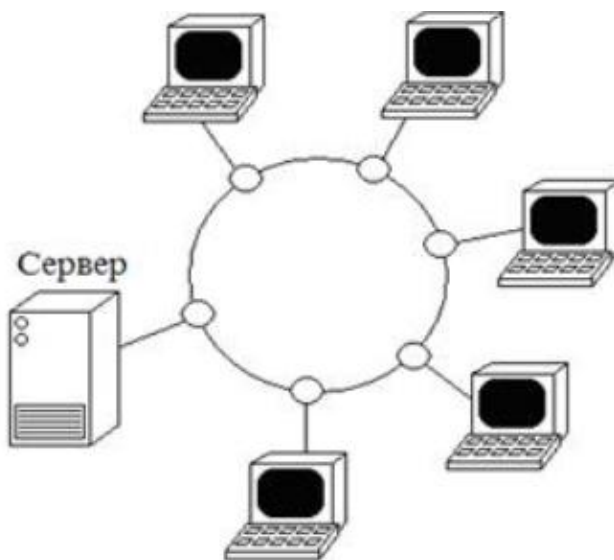


Рисунок 2.2 – Топологія кільце

Недоліки:

- низька надійність, оскільки відмова одного вузла тягне відмову всієї мережі;

									Арк.
									20
Змн.	Арк.	№ док.м.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ				

- при великому навантаженні на мережу швидкість роботи зменшується;
- для підключення нового вузла потрібно зупинити роботу цілої мережі;
- для того щоб знайти причину поломки, потрібно перевірити кожен вузол.

Переваги:

- робочі станції легко об'єднати в мережу;
- не потребує додаткового устаткування.

Остання топологія, яку було розглянуто – розширена зірка. Її робота полягає в тому, що замість того, щоб підключати всі станції до одного комутатора, як би це було б в простій зірці, підключення розподіляється на рівні.

На рисунку 2.3 зображено топологію розширена зірка.

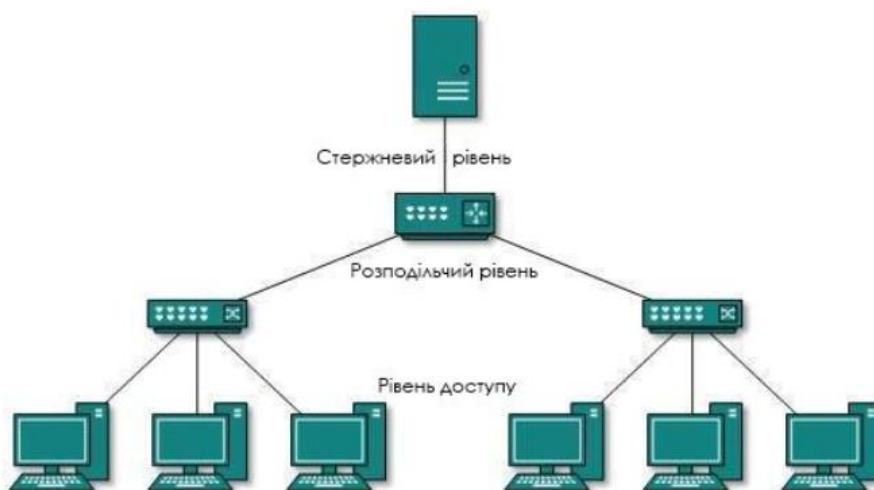


Рисунок 2.3 – Топологія розширена зірка

Її недоліки полягають в:

- всі пристрої залежні від центрального вузла;
- порівняно висока вартість;
- потребує ретельного проектування.

Переваги:

- масштабованість, можна з легкістю розширювати мережу без значних витрат;

Змн.	Арк.	№ докцм.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

21

- якщо якийсь з вузлів виходить з ладу, то це впливає лише на той вузол, а не на всю мережу;
- ієрархічна структура, кожен відділ має свій комутатор, ці комутатори підключені до головного пристрою;
- всі точки зібрані в одному місці, що спрощує моніторинг.

В проєкті використано топологію розширена зірка. Враховуючи велику кількість робочих станцій, ця топологія є найоптимальнішою. Головним комутатором виступає SW_2. Крім того, в серверній окрім комутатора знаходяться 2 сервери (S_1, S_2) та маршрутизатор (R_1), через який буде відбуватись доступ до глобальної мережі Інтернет.

Сегментування відбувається за допомогою 2 точок доступу (AP_1, AP_2) та 2 комутаторів (SW_1, SW_3). Точка доступу AP_1 покриває 2 відділи DevOps та відділ тестування. Точка доступу AP_2 покриває відділ кадрів та маркетингу. Комутатор SW_1 покриває 2 відділи DevOps. Комутатор SW_3 відділ керівництва та бухгалтерію. Таким чином навантаження на головний комутатор менше і відповідно мережа стає більш витривалою до навантажень.

Повну схему логічної топології мережі компанії наведено на листі графічного матеріалу 2026.КВР.123.406.11.00.00 ЛТ, який міститься в додатку А до цієї кваліфікаційної роботи.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

Типи середовища передавання даних можна поділити на 4 типи:

- коаксіальний кабель;
- вита пара;
- волоконно-оптичний кабель;
- бездротова лінія зв'язку.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

Для того, щоб обрати необхідне середовище потрібно розібратись в характеристиках. Окрім того, при виборі потрібно враховувати топологію мережі, необхідну пропускну здатність також завадостійкість кабелю та його обмеження по довжині.

Основним середовищем передавання даних для проєктованої мережі була обрана вита пара. Оскільки, вита пара є фактичним стандартом для побудови локальних мереж через баланс вартості, продуктивністю та простотою встановлення. Окрім того, в мережі використовується бездротова лінія зв'язку. Для того, щоб обґрунтувати вибір, розглянемо типи та категорії витої пари. Є основні три класифікації [3]:

1. UTP (неекранована вита пара), виготовлена з мідних провідників, попарно скручених всередині спільної оболонки.
2. FTP (фольгована вита пара), відрізняється тим, що покриває всі пари або окремі виті пари шаром алюмінієвої фольги як екран від перешкод.
3. STP (екранована вита пара), додатково до спільного зовнішнього екрану, кожна пара має власний екран.

Окрім цих трьох класифікацій, кабелі сортуються за класами від CAT1 до CAT8, вони регулюються стандартами ISO/IEC 11801, ANSI/TIA/EIA-568 та EN 50173. Категорія визначається робочим діапазоном частот та максимальною швидкістю передачі даних [7]. Категорії CAT3 та CAT5 відходять на задній план, оскільки працювали лише на частотах до 100 МГц та зі швидкістю до 100 Мбіт/с.

Клас CAT6 підтримує частоту до 250 МГц та швидкість до 1 Гбіт/с для довжини 100 метрів та 10 Гбіт/с до 55 метрів. Категорія CAT7 збільшує діапазон частот до 600 МГц, а CAT8, яка розробляється для дата-центрів, має частоти 2000 МГц та швидкість 25-40 Гбіт/с, але з меншою довжиною ліній [7].

Для пропускну здатності 1 Гбіт/с на робочих вузлах основний середовищем передачі даних обрано неекранований кабель U/UTP типу CAT6.

Обґрунтувати такий вибір можна тим, що в кабелі є вбудований пластиковий розділювач, який зменшує перехресні перешкоди на ближньому кінці (NEXT) у ближньому діапазоні частот, що досягає 250 МГц. Для підключення кінцевих

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

пристроїв використовується роз'єм RJ-45, відповідно до схеми T568B з використанням прямої конфігурації. Сучасне обладнання підтримує Auto-MDIX, вона автоматично підлаштовує контакти під тип підключеного кабелю.

Для мобільності персоналу та можливості підключення портативних пристроїв в окремих кабінетах організовано бездротовий канал передачі даних на основі стандарту IEEE 802.11ax в зонах 2,4 ГГц і 5 ГГц, але для 5 ГГц відповідно до цього стандарту забезпечується вищий рівень продуктивності. Завдяки OFDMA й MU-MIMO мережа працює стабільно не залежно від кількості підключених користувачів, а безпеку трафіку забезпечує шифрування за протоколом WPA3-Enterprise з аутентифікацією через RADIUS-сервер.

Живлення точок доступу відбувається через мережевий кабель за стандартом PoE, відповідно усуваючи прокладання окремих ліній.

Монтаж кабельної системи здійснюється відповідно до вимог стандарту СКС ТІА/EIA-568B, де відстань до 90 метрів є допустимою довжиною сегмента середнього кабелю від головного розподільчого вузла до розетки чи точки доступу [22]. Горизонтальні кабельні лінії прокладаються над підвісною стелею в металевих перфорованих лотках, в той час вертикальні спуски розташовуються в настінних коробах, де допускається заповнення до 60%. Для того, щоб зменшити вплив електромагнітних навантажень від 220 В, слабкоструміві системи розташовуються не ближче ніж 20 сантиметрів одна від одної. Після встановлення системи відбувається випробовування цифровими аналізаторами на відповідність категорії CAT6 та тесту на бездротовий сигнал.

2.2.2 Будова вузлів та необхідність їх застосування

Відповідно до попереднього пункту, проєктована мережа реалізовується на основі комбінованої архітектури, що поєднує дротову систему, яка розгорнута за топологією розширеної ієрархічної зірки та локальний бездротовий сегмент. Така структура дозволяє використання комутаційних пристроїв як центральних вузлів для підключення кінцевого обладнання.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		24

Оскільки, обраним кабельним середовищем є неекранований кабель категорії CAT6, то усі комутатори мають відповідні швидкісні порти RJ-45 для забезпечення пропускної здатності до 1 Гбіт/с.

Враховуючи розміщенні кабінетів, локалізації трафіку та вимог до надійності, мережа структура поділена на три пов'язані функціональні рівні:

- магістральний вузол керування та серверної інфраструктури (серверна 103) – формується на базі маршрутизатора R_1 та головного комутатора рівня L3 SW_2. Цей вузол розподіляє потоки даних між усіма підрозділами компанії та фільтрує трафік. Порти комутатора SW_2 використовуються для підключення серверів S_1 та S_2, двох точок бездротового доступу AP_1 та AP_2, комутаторів SW_1 та SW_3 через магістральні Trunk-канали, а також маршрутизатора R_1 для виходу в глобальну мережу Інтернет;

- провідний комутаційний сегмент (кабінети 117, 114, 109, 110) – реалізований на базі двох комутаторів рівня L2. Комутатор SW_1 обслуговує кабінети 117 та 114 і забезпечує дротове з'єднання робочих станцій WS_1-WS_11. Комутатор SW_3 розгорнуто в кабінетах 109 та 110 для підключення робочих станцій WS_25-WS_32 та мережевого принтера R_1;

- бездротовий сегмент (кабінети 101, 102, 118, 112, 111) – організований за допомогою двох точок доступу, підключених до портів центрального комутатора SW_2. Точка доступу AP_1 забезпечує покриття кабінетів 101, 102 та 118 для бездротового підключення пристроїв WS_12-WS_24. Точка доступу AP_2 обслуговує кабінети 112 та 111 і забезпечує підключення станцій WS_33-WS_37.

Для розподілу мережі на ізольовані сегменти та обмеження широкомовного трафіку налаштовуються віртуальні мережі VLAN за стандартом IEEE 802.1Q.

Сервери виділено в окремий захищений сегмент для захисту критично важливих даних.

Схема адресації, розподіл пристроїв по кабінетах та параметри віртуальних підмереж наведено в таблиці 2.1.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		25

Таблиця 2.1 – Логічна адресація ЛОМ

№ п / п	Діапазон позначен ня вузлів	Робоча група/ К- сть вузлів		Назва кабінету та його номер		№ VLAN	Адреса підмережі/ Маска
		3	4	5	6		
1	SW_1 WS_1- WS_11	Dev_Wired	12	Кабінети DevOps	117, 114	10	192.168.10.0/24 192.168.10.2 192.168.10.10 – 192.168.10.20
2	AP_1 WS_12- WS_24	QA_Dev_Wi Fi	14	Відділ QA та DevOps	101, 102, 118	20	192.168.20.0/24 192.168.20.2 192.168.20.10 – 192.168.20.22
3	SW_3 PR_1 WS_25- WS_32	Management	10	Керівництво та бухгалтерія	109, 110	30	192.168.30.0/24 192.168.30.2 192.168.30.5 192.168.30.10 – 192.168.30.17
4	AP_2 WS_33- WS_37	Staff_WiFi	6	Відділ кадрів та маркетологи	112, 111	40	192.168.40.0/24 192.168.40.2 192.168.40.10 – 192.168.40.14
5	SW_2 S_1 S_2	Infrastructure	3	Серверна	103	50	192.168.50.0/24 192.168.50.2 192.168.50.10 192.168.50.11

У таблиці 2.2 наведено схему фізичного підключення та програмного конфігурування інтерфейсів активного обладнання.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

Таблиця 2.2 – Таблиця конфігурації VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мережевого пристрою	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	SW_1	Te1/0/1	SFP+ trunk	SW_2	Te1/0/17	SFP+ trunk	10, 50
2	SW_3	Te1/0/1	SFP+ trunk	SW_2	Te1/0/18	SFP+ trunk	30, 50
3	R_1	SFP+	trunk	SW_2	Te1/0/20	SFP+ trunk	10-50
4	AP_1	ether1	Access	SW_2	Gi1/0/1	Access	20
5	AP_2	ether1	Access	SW_2	Gi1/0/2	Access	40
6	S_1	SFP	Access	SW_2	Te1/0/19	SFP+ Access	50
7	S_2	Eth0	Access	SW_2	Gi1/0/3	Access	50
8	WS_1- WS_11	-	Access	SW_1	Gi1/0/2-12	Access	10
9	WS_12- WS_24	-	WiFi	AP_1	-	WiFi	20
10	WS_25- WS_32	-	Access	SW_3	Gi1/0/2-9	Access	30
11	PR_1	-	Access	SW_3	Gi1/0/10	Access	30
12	WS_33- WS_37	-	WiFi	AP_2	WiFi	WiFi	40

Наведена схема комутації в таблиці 2.2 відображає логічну структуру підключення пристроїв із чітким розділенням трафіку на VLAN.

2.3 Обґрунтування вибору обладнання для мережі

Для того, щоб спроектувати комп'ютерну мережу потрібно використовувати пасивне і активне обладнання.

Активне мережеве обладнання кінцеве і комунікаційне обладнання, функціонування якого забезпечується за рахунок споживання електроенергії від зовнішніх джерел живлення. Активне мережеве обладнання виконує комплексних функцій мережі, які реалізуються в апаратурі [3]. Щоб мережа працювала ефективно та без збоїв, при побудові потрібно всі елементи пасивного

обладнання обирати так, щоб вони були в тій же категорії що кабель. Тоді робота пристроїв буде коректною та чіткою.

Оскільки, мережа компанії “MidHub” проєктована на топології розширеної зірки, то основні пристрої в мережі є: головний комутатор, два комутатори робочих груп, дві точки доступу та маршрутизатор. Ці пристрої створюють спільну систему, забезпечують продуктивну роботу всіх ланок компанії та миттєвий доступ до ресурсів.

При виборі моделі комутатора висунуто наступні критерії порівняння.

Основні критерії для порівняння моделей обрано:

- тип комутатора повинен бути рівня L2+;
- наявність високошвидкісних магістральних інтерфейсів 10G SFP+;
- забезпечення логічної сегментації на базі стандарту IEEE 802.1Q VLAN;
- підтримка швидкості 1Гбіт/с на портах доступу.

Порівняльна характеристика вибору моделі центрального комутатора наведена в таблиці 2.3

Таблиця 2.3 – Порівняльна характеристика головних комутаторів

Моделі	Cisco Catalyst 1200 24xGE, PoE, 4x10G SFP+	HPE Aruba Instant On 1930 24 GE	TP-LINK JetStream TL-SG3428XMP
1	2	3	4
Тип комутатора	Керований рівня L3	Керований рівня L2+	Керований рівня L2+
Кількість портів Gigabit Ethernet	24	24	24
Інші порти	4 x 10G SFP+	4 x 10G SFP+	4 x 10G SFP+
Безпека та захист	Захист від DoS-атак , ACL, 802.1X	ACL, 802.1X	ACL, 802.1X
Комутаційна здатність, Гбіт/с	128	128	128
PoE бюджет, Вт	195	195	384
Монтаж у стійку	Так, 1U	Так, 1U	Так, 1U
Розміри, мм	445 x 299 x 44	442 x 264 x 44	440 x 330 x 44
Управління	Web GUI, Cisco Dashboard	Web/Cloud	Web GUI, Omada SND
Вартість, грн	35 000	26 000	32 000

Базуючись на аналізі інформації, наведеної в порівняльній таблиці 2.3, для реалізації проєкту було обрано модель Cisco Catalyst 1200 24xGE, 4x10G SFP+, як головний комутатор SW_2 локальної мережі.

На рисунку 2.4 зображено вигляд комутатора Cisco Catalyst 1200 24xGE, 4x10G SFP+.



Рисунок 2.4 - Комутатор Cisco Catalyst 1200 24xGE, 4x10G SFP+3

Основні характеристики Cisco Catalyst 1200 24xGE, 4x10G SFP+3 [16]:

- порти – 24 x Gigabit Ethernet (10/100/1000) RJ-45 з підтримкою PoE та 4 x 10G SFP+ uplink порти;
- форм-фактор – для монтажу в стійку (1U).

Продуктивність:

- швидкість пересилання пакетів – 95.23 Mpps;
- комутаційна здатність – 128 Гбіт/с;
- буфер пакетів – 1.5 МБ (динамічний розподіл);
- таблиця MAC-адрес – до 8000 записів.

Живлення:

- підтримка PoE – для живлення точок доступу;
- максимальний бюджет PoE – 195 Вт, до 30 Вт на порт.

Функціональні можливості:

- підтримка VLAN-інтерфейсів;
- статична маршрутизація IPv4/IPv6;
- агрегація каналів;
- підтримка IGMP.

Безпека:

- контроль доступу за стандартом IEEE 802.1X;

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		29

- списки контролю доступу;
- контроль підключення пристроїв до портів;
- захист від DoS-атак;
- захист від мережевих штормів.

Керування трафіком:

- 8 рівнів пріоритету трафіку;
- механізми пріоритезації та чергування пакетів.

Для реалізації нижнього рівня ієрархії необхідно обрати два комутатори (SW_1, SW_3), завданням яких є підключення робочих станцій та периферійних пристроїв і передача трафіку до головного комутатора SW_2.

Модель комутатора повинна відповідати наступним вимогам:

- наявність портів 1 Гбіт/с для підключення робочих станцій;
- наявність портів 10 Гбіт/с для підключення комутаторів до головного;
- підтримка VLAN;
- віддалене керування через єдину панель.

В таблиці 2.4 наведено порівняльну характеристику комутаторів доступу.

Таблиця 2.4 – Порівняльна характеристика для вибору комутатора доступу

Моделі	Cisco Catalyst 1300 (C1300-16P-4X)	TP-LINK Omada SG3218XP-M2	HP Aruba Instant On 1960-12XGT- 4SFP+
1	2	3	4
Тип комутатора	Керований L2/L3 Lite	Керований L2+	Керований L2+/L3 Lite
Порти доступу	16 x 1G RJ-45 PoE+	16 x 2.5G RJ-45 (8 PoE+)	12 x 10G RJ-45
Інші порти	4 x 10G SFP+	2 x 10G SFP+	4 x 10G SFP+
PoE бюджет, Вт	120	240	-
Продуктивність	83.32 Mpps	89.28 Mpps	238 Mpps
Пропускна здат.	112 Гбіт/с	120 Гбіт/с	320 Гбіт/с
Керування	Web GUI, CLI, Cisco Dashboard	Omada SND	Aruba Instant On
Монтаж у стійку	Так, 1U	Так, 1U	Так, 1U
Ціна, грн	34 700	28 400	39 556

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

30

Аналізуючи таблицю 2.4 модель для комутаторів SW_1 та SW_2 обрано Cisco Catalyst 1300 (C1300-16P-4X). Він гарантує стабільну роботу, а також ефективне керування трафіком та сегментацію мережі. Завдяки 16 GE PoE портам та 10G SFP+ інтерфейсів комутатор дозволяє підключати робочі станції та забезпечувати високу швидкість передачі даних. Це робить Cisco Catalyst C1300-16P-4X хорошим рішенням для впровадження його на рівні доступу в мережах малого та середнього бізнесу, де основними вимогами є стабільність, надійність і масштабованість. На рисунку 2.5 зображено Cisco Catalyst C1300-16P-4X.

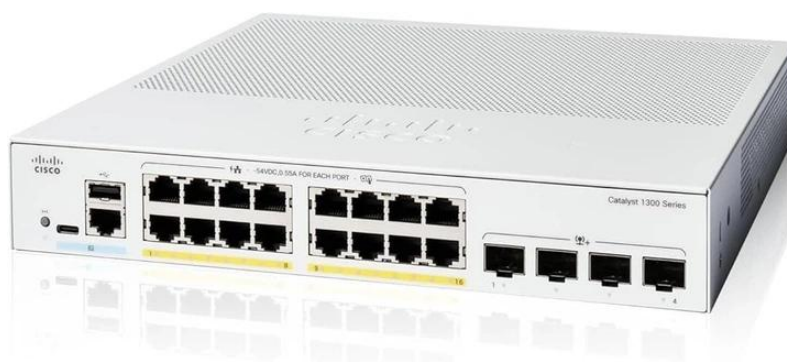


Рисунок 2.5 – Комутатор Cisco Catalyst C1300-16P-4X

Основні характеристики та функціональні можливості [10]:

Продуктивність:

- Двоядерний процесор ARM з тактовою частотою 1.4 GHz;
- 1 GB системної пам'яті покоління DDR4;
- 1.5 MB динамічного кешу для обробки черг трафіку;
- приблизний час робот на відмову понад 2 165 105 годин.

Живлення:

- вбудований блок живлення з підтримкою вхідної напруги 100-240V;
- підтримка стандарту IEEE 802.3az, що знижує енергоспоживання портів у моменти простою.

Функціональні можливості:

- 512 MB постійної пам'яті для надійного збереження файлів конфігурації та образів ОС;

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		31

- підтримка близько 990 статичних маршрутів та 128 IP-інтерфейсів, робота з динамічним протоколом RIP v2;
- пасивне охолодження, що забезпечує безшумну роботу;
- підтримка повного стеку протоколів Spanning Tree та агрегація ліній LACP(до 8 динамічних груп).

Безпека:

- підтримка протоколу IEEE 802.1X та RADIUS-серверів для контролю доступу пристроїв до мережі;
- функції Private VLAN Edge (PVE) та Guest VLAN для створення захищених зон та ізоляції гостьового трафіку;
- вбудований механізм фільтрації завдяки списків контролю доступу (ACL) та захисту від мережевих петель.

Керування трафіком:

- маркування та розподіл мережевих пакетів за номерами VLAN;
- апаратна підтримка черг для обробки чутливого до затримок трафіку;
- функція встановлення лімітів на вхідний та вихідний трафік для кожного фізичного інтерфейсу.

Для реалізації зовнішнього підключення до мережі, організації захищеного міжмережевого екрана, здійснення VPN-з'єднань для того, щоб співробітники могли працювати дистанційно також маршрутизації між віртуальними мережами був проведений аналіз трьох маршрутизаторів для вибору моделі, яка буде впроваджена в мережу.

Маршрутизатор є ключовим пристроєм мережевої інфраструктури, бо саме він відповідає за передачу трафіку між різними сегментами мережі, реалізацій політик безпеки та підключення до зовнішніх мереж.

Саме тому, висунуто наступні вимоги для вибору необхідного маршрутизатора.

Основні вимоги до маршрутизатора:

- швидкість маршрутизації неменше 1 Гбіт/с;
- швидкість шифрування тунелів – не менше 300 Мбіт/с;

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		32

- наявність порту 10G SFP+.

Порівняльна характеристика вибору маршрутизатора наведена в таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика маршрутизаторів

Моделі	Ubiquiti EdgeRouter 4	MikroTik RB5009UG+S+IN	Cisco RV160
1	2	3	4
Процесор	4 ядра, 1.0 ГГц	4 ядра, 1.4 ГГц (ARM 64)	2 ядра, 1.0 ГГц
Оперативна пам'ять	1 ГБ DDR3	1 ГБ DDR4	1 ГБ DDR3
Мережеві інтерфейси	3 x 1 Гбіт/с RJ-45, 1 x 1 Гбіт/с SFP	1 x 10 Гбіт/с SFP+, 1 x 2.5 Гбіт/с, 7 x 1 Гбіт/с	1 x 1 Гбіт/с WAN, 4 x 1 Гбіт/с LAN
Пропускна здатність NAT	До 3.4 Гбіт/с	До 9.85 Гбіт/с	До 600 Мбіт/с
Швидкість VPN	До 500 Мбіт/с	До 1.41 Гбіт/с	До 50 Мбіт/с
Надійність	-	200 000 годин	-
Ціна, грн	10 000	11 300	11 000

Для проектування мережі обрано модель MikroTik RB5009UG+S+IN. В таблиці показано, що конкуренти мають приблизно однакову вартість, але при тому обрана модель забезпечує максимальну швидкість маршрутизації та шифрування VPN. Наявність вбудованого 10G SFP+ дозволяє підключити пристрій до головного комутатора без втрат швидкості на магістралі, це повністю задовольняє вимоги проекту.

Щоб забезпечити повноцінну роботу проекрованої ІТ-компанії, впроваджено локальну серверну інфраструктуру. Оскільки, компанія налічує 37 робочих станцій, які постійно працюють з локальними репозиторіями, їм необхідна швидка автентифікація, тому мережевий сегмент розгорнуто на базі двох окремих серверів.

Головний сервер автоматизує щоденні офіційні служби такі як DNS, AD та зберігає файли користувачів. Під внутрішні завдання штучного інтелекту та обробки Big Data виділено окремий сервер. Для вибору моделі було проведено

порівняння з іншими пристроями, щоб сформувавши оптимальну архітектуру сервера штучного інтелекту та файлового.

Критерії вибору сервера для розгортання ШІ:

- достатній обсяг оперативної пам'яті та її тип для розгортання ШІ-моделей;
- тип дискової підсистеми та швидкість передачі даних;
- підтримка апаратних інструкцій прискорення обчислень (AMX, AVX-512);
- кількість ядер процесора;
- пропускну здатність мережевого інтерфейсу.

У таблиці 2.6 наведено порівняльну характеристику для сервера штучного інтелекту.

Таблиця 2.6 – Порівняльна характеристика серверів для розгортання ШІ

Модель	Dell PowerEdge R660	Lenovo ThinkSystem SR630 V3	HPE ProLiant DL360 Gen11
1	2	3	4
Тип корпусу	1U	1U	1U
Процесор	Intel Xeon Silver 4416+	Intel Xeon Silver 4410Y	Intel Xeon Silver 4510
Кількість ядер/потоків	20 ядер / 40 потоків	12 ядер / 24 потоки	12 ядер / 24 потоки
Оперативна пам'ять	128 ГБ	64 ГБ	64 ГБ
Стандарт та захист пам'яті	DDR5 RDIMM ECC	DDR5 RDIMM ECC	DDR5 RDIMM ECC
Дискова підсистема	2 x 1.92 ТБ NVMe SSD	-	2 x 960 ГБ SATA SSD
Керування дисками (RAID)	PERC H755, RAID 0/1/5/10	ThinkSystem RAID, SMART	HPE Smart Array, RAID 0/1/5
Вбудовані мережеві порти	2 x 1 Гбіт/с RJ-45	2 x 1 Гбіт/с RJ-45	4 x 1 Гбіт/с RJ-45

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

34

Продовження таблиці 2.6

1	2	3	4
Слоти PCIe для розширення	3 x PCIe Gen5	3 x PCIe Gen5	2 x PCIe Gen5 + 2 x OCP 3.0
Операційна система	Ubuntu Server	Windows Server	Red Hat Enterprise Linux
Протоколи адміністрування	SSH, HTTPS, SNMP v3	SSH, HTTPS, SNMP v3	SSH, HTTPS, SNMP v3
Система апаратного моніторингу	iDRAC9 Enterprise	Lenovo XClarity	HPE iLo 6 Standard
Блоки живлення	2 x 800 Вт	1 x 1100 Вт	2 x 1000 Вт
Вартість, грн	286 000	215 000	280 000

За результатами порівняльної таблиці 2.6 серверів для розгортання моделей штучного інтелекту обрано модель Dell PowerEdge R660. Дана модель гарантує оптимальне поєднання обчислюваної потужності та пропускну здатності, що потрібно для локального розгортання моделей штучного інтелекту. Процесор Intel Xeon Silver 4416+ з 20 ядрами та 128 ГБ оперативної пам'яті DDR5 забезпечують ресурси для виконання об'ємних задач обробки запитів до моделей ШІ, а також дискова підсистема на базі двох NVMe SSD загальним об'ємом 3.84 ТБ забезпечує високу швидкість зчитування та запису даних. Додатково у сервер встановлено мережевий адаптер Intel X520-DA1 з інтерфейсом 10 Гбіт/с SFP+, щоб забезпечити високошвидкісне підключення до комутатора та мінімізувати затримки під час передачі великих масивів даних у мережі.

На рисунку 2.6 зображено сервер Dell PowerEdge R660.



Рисунок 2.6 – Сервер Dell PowerEdge R660

Змн.	Арк.	№ док.м.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

35

Для того, щоб організувати файлове сховище, розгортання доменних служб та забезпечити автономну роботу мережевих сервісів необхідно обрати відповідну модель сервера.

Критерії для порівняння:

- обсяг оперативної пам'яті не менше 64 ГБ;
- підтримка мережевих протоколів доступу SMB,NFS та iSCSI;
- можливість розгортання служб Active Directory, DNS;
- надійність файлової системи та керування дисковим масивом;
- масштабованість дискового масиву.

В таблиці 2.7 наведено порівняльну характеристику моделей для вибору файлового сервера.

Таблиця 2.7 – Порівняльна характеристика моделей для файлового сервера

Моделі	PowerUp Rack 4U	Dual ALFA Rack 923	Lenovo ThinkSystem ST50 V2
1	2	3	4
Архітектурний тип системи	Повноцінний сервер	Повноцінний сервер	Повноцінний сервер
Центральний процесор (ЦП)	2 x Intel Xeon E5-2673 v4	2 x Intel Xeon E5-2690 v3	1 x Intel Xeon E-2324G
Обчислювані ресурси ЦП	40 ядер / 80 потоків	24 ядра / 48 потоків	4 ядра / 4 потоки
Обсяг оперативної пам'яті	64 ГБ	64 ГБ	8 ГБ (макс. 128 ГБ)
Стандарт та захист пам'яті	DDR4 Registered ECC	DDR4 Registered ECC	DDR4 ECC Unbuffered
Відсіки для накопичувачів	8 відсіків із гарячою заміною	4 відсіки для дисків	3 відсіки SATA
Дискова підсистема	2 x 1 ТБ SSD (RAID 1)	2 x 256 ГБ SSD + 2 ТБ HDD	2048 ГБ SSD
RAID-контролер	Апаратний LSI / Broadcom	Інтегрований (Soft-RAID)	Апаратний ThinkSystem 5350-8i

Змн.	Арк.	№ докum.	Підпис	Дата

2026.KBP.123.406.11.00.00 ПЗ

Арк.

36

Продовження таблиці 2.7

1	2	3	4
Вбудовані мережеві порти	2 x 1 Гбіт/с RJ-45	2 x 1 Гбіт/с RJ-45 + 1 Mgmt	1 x 1 Гбіт/с RJ-45
Базова операційна система	Windows Server 2022	Windows Server 2022	Windows Server 2022
Мережеві протоколи доступу	SMB, NFS, iSCSI, FTP, WebDAV	SMB, NFS, iSCSI, FTP	SMB, NFS, iSCSI, FTP
Доменні служби (AD, DNS)	Повноцінне розгортання ролей	Повноцінне розгортання ролей	Повноцінне розгортання ролей
Керування дисковим масивом	За допомогою MegaRAID + IPMI	Базовий вбудований веб-інтерфейс	Lenovo XClarity
Система апаратного моніторингу	IPMI 2.0 / iKVM	ASMB8-iKVM / Mgmt	Intel AMT / XClarity
Блоки живлення	2 x 750 Вт	1 x 600 Вт	1 x 500 Вт
Вартість, грн	58 700	47 400	38 200

В результаті аналізу на основі таблиці 2.7 для інтеграції в інфраструктуру компанії було обрано сервер моделі PowerUp Rack 4U. Це рішення є найбільш раціональним, оскільки його двохпроцесорна архітектура на базі Intel Xeon E5-2673 v4 забезпечує сумарну потужність у 40 фізичних ядер та 80 обчислюваних потоків. Цього ресурсу буде повністю достатньо для обслуговування всіх робочих станцій компанії без затримок та одночасного функціонування локальних доменних служб Active Directory, DNS під час високого навантаження.

Ще одною перевагою обраної моделі є організація відмовостійкості дискової підсистеми у режимі RAID 1 із двох SSD розміром по 1 ТБ кожен, що забезпечує повне дзеркалювання корпоративних даних та автоматичне відновлення працездатності у разі відмови одного з накопичувачів. Цей режим є оптимальним для сервера корпоративних служб, коли пріоритетом є збереження даних, а не

Змн.	Арк.	№ док.м.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

37

швидкість операцій читання-запису.

Інші варіанти були відхилені, оскільки за приблизно одну цінову категорію вони пропонують критично обмежені обчислювальні ресурси, недостатній обсяг оперативної пам'яті в базовій комплектації або ж апаратно лімітовані виробником для обслуговування не більше 20 робочих станцій.

Отже, PowerUp Rack 4U є найбільш ефективним інженерним та фінансовим рішенням із високим потенціалом для подальшого масштабування ІТ-інфраструктури компанії.

Для реалізації бездротового сегмента мережі компанії та забезпечення надійного покриття для робочих станцій необхідно здійснити вибір моделі точок доступу (AP_1, AP_2).

Критерії для вибору моделі точки доступу:

- наявність продуктивного багатоядерного процесора та достатнього обсягу оперативної пам'яті;
- підтримка сучасного стандарту Wi-Fi 6;
- підтримка високошвидкісного мережевого інтерфейсу 2.5 Гбіт/с;
- можливість живлення пристрою через Ethernet-кабель за технологією PoE.

В таблиці 2.8 наведено порівняльний аналіз характеристик моделей точок доступу.

Таблиця 2.8 – Порівняльна характеристика точок доступу

Моделі	Mikrotik hAP ax3	Ubiquiti UniFi U6+	TP-LINK EAP653 UR Wi-Fi 6
1	2	3	4
Стандарт Wi-Fi	802.11ax (Wi-Fi 6)	802.11ax (Wi-Fi 6)	802.11ax (Wi-Fi 6)
Робота в двох діапазонах	+	+	+
Максимальна швидкість, Мбіт/с	574 + 1200	573.5 + 2402	574 + 2402

Продовження таблиці 2.8

1	2	3	4
Конфігурація порти LAN	1 x 2.5 GbE, 4 x 1 GbE	1 x 1 GbE	1 x 1 GbE
Коефіцієнт підсилення антен	3.3 dBi / 5.5 dBi	3 dBi / 5.4 dBi	4 dBi / 5 dBi
Підтримка MU-MIMO / OFDMA	+	+	+
Безшовний роумінг (802.1k/v/r)	+ (безкоштовний CAPsMAN)	+ (потребує контролер)	+ (потребує контролер)
Максимальна кількість клієнтів	150+	300+	250+
Живлення через PoE	+ (PoE-in / PoE-out)	+ (тільки PoE-in)	+ (тільки PoE-in)
Обсяг оперативної пам'яті	1 ГБ (1024 МБ)	512 МБ	512 МБ
Вартість, грн	5 800	5 800	6 800

На основі таблиці 2.8 проведено порівняльний аналіз технічних характеристик та економічної доцільності обладнання. Для бездротового сегмента мережі було обрано точку доступу моделі Mikrotik hAP ax3. Ця модель повністю задовольняє всі вимоги проекту, забезпечуючи роботу у двох частотних діапазонах за сучасними стандартами та високий коефіцієнт підсилення антен для стабільного покриття офісного простору.

Основною перевагою обраної моделі є подвійний обсяг оперативної пам'яті (1ГБ порівняно з 512 МБ у інших моделей) та потужна апаратна платформа, що гарантує безперебійну обробку пакетів для робочих станцій при пікових навантаженнях. Наявність високошвидкісного порту 2.5 GbE запобігає виникненню перевантажень під час з'єднання пристрою з головним комутатором, вбудована безкоштовна технологія CAPsMAN дозволяє централізовано організувати безшовний роумінг в офісі без залучення

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

39

додаткових платних контролерів. Комплектація пристрою блоком живлення та PoE-інжектором, а також додаткових LAN-портів забезпечує економічне та зручне встановлення пристрою.

Також планується встановлення одного мережевого принтера у бухгалтерії (PR_1). Таке рішення було прийняте через те, що у цьому відділі найбільший обсяг документообігу. Крім того, це гарантує фізичний захист і конфіденційність фінансових звітів та персональних даних від сторонніх осіб. Водночас завдяки підключенню до ЛОМ пристрій забезпечує повноцінний віддалений доступ для друку всім іншим співробітникам, що дозволяє раціонально й економічно закривати потреби всього офісу одним потужним принтером.

В таблиці 2.9 наведено порівняльний аналіз характеристик моделей лазерних принтерів.

Таблиця 2.9 – Порівняльна характеристика моделей принтерів

Моделі	HP LaserJet Enterprise M507dn	Canon i-SENSYS MF553DW	Xerox C315
1	2	3	4
Швидкість друку	43 стор./хв	43 стор./хв	35 стор./хв
Продуктивність процесора	1200 МГц	2 x 800 МГц	1200 МГц
Максимальне місячне навантаження	До 150 000 сторінок	До 150 000 сторінок	До 80 000 сторінок
Місткість лотка видачі	250 аркушів	150 аркушів	150 аркушів
Енергоспоживання	7.6 Вт	13.6 Вт	26.2 Вт
Ресурс картриджа	До 20 000 сторінок (Серія 89Y)	До 21 000 сторінок (Серія 056H)	До 8 000 сторінок (Серія XL)
Безпека	Апаратна (HP Sure Start + захист ОЗП)	Базова програмна	Стандартна мережева
Вага, кг	11.48	19.8	27.1
Вартість, грн	41 400	46 600	40 400

Змн.	Арк.	№ док.м.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

40

На основі проведеного аналізу технічних характеристик в таблиці 2.8, для інтеграції в мережі було обрано пристрій HP LaserJet Enterprise M507dn. Ця модель повністю задовольняє вимоги проєкту. Вона пропонує поєднання продуктивності завдяки двоядерному процесору з частотою 1200 МГц, значного місячного навантаження до 150 000 сторінок та передового апаратного захисту. Серед ключових елементів захисту є технологія HP Sure Start, яка забезпечує перевірку цілісності ядра прошивки, а також надійний захист оперативної пам'яті.

Мінімальне енергоспоживання в режимі очікування, місткий лоток на 250 аркушів та високий ресурс картриджа дозволяють суттєво знизити сукупну вартість володіння пристроєм. Завдяки цьому, принтер гарантує високу автономність роботи, економічність та стабільність.

В таблиці 2.10 наведено перелік пасивного та активного обладнання для побудови ЛОМ.

Таблиця 2.10 – Перелік обладнання для побудови мережі

№ п/п	Назва елемента	Позначення	Модель	Ціна, грн	Одиниці виміру	К-ть
1	2	3	4	5	6	7
1	Кабель	-	UTP Cat 6	23	М.	228
2	Короб	-	60*40 (2м)	53,50	Шт.	10
3	Короб	-	25*16 (2м)	14,90	Шт.	26
4	Короб	-	16*16 (2м)	11,25	Шт.	20
5	Роз'єм	-	RJ45 Cat 6	5,79	Шт.	100
6	Мережева розетка	-	RJ45	94	Шт.	20
7	Патч-корд (мідний)	-	CAT6 UTP 0.5 м	75	Шт.	29
8	Патч-корд (мідний)	-	CAT6 UTP 2 м	85	Шт.	20
9	Патч-панель	-	Cat 6 24 портів	2 145	Шт.	3

Змн.	Арк.	№ док.м.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

41

Продовження таблиці 2.10

1	2	3	4	5	6	7
10	Серверна шафа	-	12U 19" 600x600	3680	Шт.	2
11	Серверна стійка	-	CMS 24U	7 295	Шт.	1
12	Оптичний трансивер	-	MikroTik S+85DLC03D	1 575	Шт.	8
13	Патч-корд (оптичний)	-	LC-LC Duplex MultiMode OM3 2м	240	Шт.	2
14	Патч-корд (оптичний)	-	LC-LC Duplex MultiMode OM4 15м	480	Шт.	1
15	Патч-корд (оптичний)	-	LC-LC Duplex MultiMode OM3 30м	734	Шт.	1
16	Мережевий адаптер 10G	-	Dell Intel X520-DA2 10Gb Dual Port SFP+ PCIe	6 314	Шт.	1
17	Комутатор	SW_2	Cisco Catalyst 1200 24xGE, PoE, 4x10G SFP+	35 000	Шт.	1
18	Комутатор	SW_1, SW_3	Cisco Catalyst 1300 (C1300-16P-4X)	34 700	Шт.	2
19	Маршрутизатор	R_1	MikroTik RB5009UG+S+IN	11 300	Шт.	1
20	Сервер	S_1	Dell PowerEdge R660	286 000	Шт.	1
21	Сервер	S_2	PowerUp Rack 4U	58 700	Шт.	1
22	Точка доступу	AP_1, AP_2	Mikrotik hAP ax3	5 800	Шт.	2
23	Принтер	PR_1	HP LaserJet Enterprise M507dn	41 400	Шт.	1

Загальна вартість обладнання, розрахунок якої виконано в економічній частині кваліфікаційної роботи, становить 567 823,40 гривень, що не перевищує встановлений ліміт та підтверджує техніко-економічну доцільність реалізації цієї мережі.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

2.4 Особливості монтажу мережі

Монтаж структурованої кабельної системи здійснюється відповідно до вимог міжнародних стандартів ISO/IEC 11801 і ANSI/TIA/EIA-568-C. Схема фізичної топології мережі, де показано розташування усіх вузлів, трас та кінцевого обладнання наведена в додатку Б. Кабельна система реалізована на основі неекранованого кабелю витвої пари категорії 6, прокладання головних кабельних потоків здійснюється у коробах 60x40 мм. Відгалуження до робочих зон виконуються у розподільчих коробах 25x16 мм, а спуск до розетки в коробах розміром 16x16 мм.

Біля робочих станцій, де з'єднання реалізовано кабельним шляхом повинна бути змонтована зовнішня мережева розетка. У кабельних каналах необхідні цілісні відрізки витвої пари від кожної розетки безпосередньо до відповідного комутатора. З'єднання робочих станцій до мережевих розеток здійснюється за допомогою патч-кордів.

У кабінетах 110 та 114 на висоті 1,8-2 метри будуть встановлені серверні шафи 12U 19". Така висота монтажу забезпечує зручний доступ до обладнання під час технічного обслуговування. Внутрішній простір шаф розподілено таким чином, що перший юніт займає патч-панель, ззаду підключаються кабелі від мережевих розеток. На другому юніті знаходиться комутатор доступу (SW_1 або SW_3). Для з'єднання патч-панелі з комутатором використовуються короткі мідні патч-корди CAT6 довжиною 0,5 метра. Вільний простір залишається для проведення ліній живлення та укладання технологічного запасу кабелю.

Головний вузол мережі розташований в серверній кімнаті 103. Там встановлено відкриту підлогову стійку висотою 24U. Сервери (S_1, S_2) монтується у нижній частині стійки, а патч-панель, головний комутатор (SW_2) та маршрутизатор (R_1) розміщуються зверху. Відкрита конструкція стійки дозволяє обладнанню природно охолоджуватись та має зручний доступ для обслуговування.

Кінцеві пристрої, в яких реалізоване дротове з'єднання підключаються через

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		43

настінні розетки RJ-45 CAT6. Від розетки до самого пристрою йде патч-корд довжиною 2 метри. При обтисканні кабеля на патч-панелі або розетці, потрібно стежити, щоб ділянка розкручених пар була не довшою 13 мм.

Дві точки доступу (AP_1, AP_2) підключаються без проміжних розеток за технологією MPTL. Тобто кабель CAT6 обтискається конектором RJ-45 і вставляється в точку доступу. Оскільки живлення точки доступу передається через той самий кабель (PoE), всі комутаційні кабелі повинні бути з чистої міді. Кабель з обмідненого алюмінію гріється під навантаженням і має більший опір, тому його небажано використовувати.

В кінці потрібно промаркувати всі лінії та перевірити кабельним аналізатором, щоб вони відповідали категорії 6.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

Вибір операційних систем для робочих та серверного обладнання визначається функціональним призначенням у структурі мережі, вимогами до продуктивності та відмовостійкості. Для того, щоб оптимізувати процеси адміністрування та досягнути максимальної ефективності апаратних засобів, реалізовано гібридну структуру системного ПЗ. Завдяки такому підходу, кожен клас пристроїв експлуатується під керуванням операційної системи, яка максимально відповідає вимогам покладених на нього та сприяє раціональному поділу обчислювальних ресурсів.

Для робочих станцій обрано операційну систему Windows 11 Pro. Це рішення обґрунтоване стабільним функціонуванням всього необхідного програмного забезпечення, офісних пакетів та інтегрованих середовищ розробки. Також обрана операційна система містить вбудовану підсистему безпеки, зокрема технологію апаратного шифрування дисків BitLocker, яка зменшує ризики несанкціонованого доступу до даних на рівні робочих станцій. Ще одною додатковою функцією є наявність розширених мережевих протоколів, що

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		44

спрощують процеси централізованого адміністрування, моніторингу та технічної підтримки робочих станцій.

Для того, щоб забезпечити високопродуктивну обчислювану платформу сервера III (S_1) вибрано дистрибутив Ubuntu Server. Ця операційна система чудово підходить для розгортання обчислюваних платформ завдяки вбудованій підтримці Python та бібліотек для роботи з III-моделями. Відсутність графічного інтерфейсу зменшує нецільове використання ресурсів, напрявляючи цю потужність процесора та оперативної пам'яті на виконання обчислюваних задач. Ядро Linux забезпечує стабільну роботу під час високих навантажень та повну сумісність із сучасними середовищами контейнеризації, зокрема Docker.

Функціонування сховища даних на базі сервера зберігання (S_2) організовано на базі операційної системи Windows Server 2022, що дозволяє реалізувати політику розмежування прав доступу користувачів до ресурсів та каталогів за допомогою сервісів Microsoft та протоколу SMB. Інтегрована технологія керування дисковими просторами (Storage Spaces) шляхом організації надійного дзеркалювання даних гарантує стійкість масиву до фізичних збоїв накопичувачів та високу надійність підсистеми збереження.

2.6 Тестування та налагодження мережі

Тестування інфраструктури мережі здійснюється для підтвердження працездатності мережі, конфігурування, виявлення помилок монтажу та відповідності технічному завданню. Процес діагностики розділено на чотири етапи [4]:

1. Діагностика кабельної системи

Здійснюється інструментальна перевірка кабельним аналізатором на відповідність стандарту ISO/IEC 11801. Прилад вимірює три основні параметри: загасання, перехресні наводки та хвильовий опір. Це дозволяє відразу знайти обриви провідників, короткі замикання чи помилки розводки пар.

2. Перевірка мережевого рівня та сегментації

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		45

Перевіряється правильність призначених IP-адрес пристроям у кожному сегменті та доступність шлюзів маршрутизатора. Далі перевіряється налаштування віртуальних мереж VLAN для логічної ізоляції трафіку. На завершення тестується правильність статичних маршрутів, внутрішній зв'язок та вихід в Інтернет перевіряються утилітами ping та traceroute прямо з маршрутизатора.

3. Перевірка серверів та сервісів

На сервері штучного інтелекту S_1 перевіряється стабільність віддаленого доступу SSH та правильність запуску сервісів Ollama і Open WebUI. На сервері зберігання даних S_2 перевіряється надійність дискового масиву і правильність налаштування прав доступу користувачів до спільних папок за протоколом SMB.

4. Вимірювання швидкості каналів

Пропускна здатність перевіряється утилітою iperf3, що запускається в режимі клієнт-сервер і генерує інтенсивний TCP/UDP трафік для того, щоб оцінити пропускну здатність. Швидкість з'єднання на робочих місцях має становити 1 Гбіт/с, а на магістральних каналах – 10 Гбіт/с. Ці показники підтверджують, що мережа готова до навантажень та до її впровадження.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		46

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з налаштування програмного забезпечення серверів

3.2.1 Інструкція з налаштування сервера штучного інтелекту

Ubuntu Server вибрано як операційну систему для сервера S_1 через його підтримку Docker, інструментів розгортання і підтримки ШІ-моделей та безкоштовну ліцензію. Реалізація ШІ здійснюється локально на базі Ollama та Open WebUI.

Налаштування сервера охоплює конфігурування безпеки ОС, захисту віддаленого доступу SSH, захисту від брутфорс-атак та правил міжмережевого екрана.

Налаштування здійснюється за наступними кроками [1]:

1. Першим етапом є первинна актуалізація та підготовка середовища ОС:

```
# Оновлюємо локальний індекс пакетів із офіційних репозиторіїв
```

```
sudo apt update
```

```
# Проводимо модернізацію всіх встановлених пакетів
```

```
sudo apt upgrade -y
```

```
# Встановлюємо додаткові утиліти моніторингу, системних ресурсів та компіляції
```

```
sudo apt install curl wget git build-essential net-tools htop software-properties-common -y
```

```
# Налаштовуємо системний часовий пояс
```

```
sudo timedatectl set-timezone Europe/Kyiv
```

2. Налаштування безпеки віддаленого доступу SSH:

```
# Створюємо резервну копію конфігураційного файлу
```

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

```
# Відкриваємо конфігураційний файл для внесенні змін безпеки
```

```
sudo nano /etc/ssh/sshd_config
```

					2026.КВР.123.406.11.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

```
# Змінює всередині файлу sshd_config 2222
```

```
PermitRootLogin no
```

```
MaxAuthTries 3
```

```
X11Forwarding no
```

```
# Тестуємо коректність синтаксису конфігураційного файлу
```

```
sudo sshd -t
```

```
# Перезапускаємо системну службу для застосування нових правил безпеки
```

```
sudo systemctl restart sshd
```

3. Налаштування захисту від брутфорс-атак:

```
# Встановлюємо службу захисту від автоматизованого підбору паролів
```

```
sudo apt install fail2ban -y
```

```
# Запускаємо та додаємо сервіс в автозавантаження ОС
```

```
sudo systemctl start fail2ban
```

```
sudo systemctl enable fail2ban
```

4. Конфігурування міжмережевого екрана:

```
# Налаштовуємо міжмережевий екран, блокуємо вхідний трафік за замовчуванням
```

```
sudo ufw default deny incoming
```

```
# Дозволяємо весь вихідний трафік із сервера в локальну та глобальну мережу
```

```
sudo ufw default allow outgoing
```

```
# Відкриваємо новий змінений порт 2222 для підключення адміністраторів по SSH
```

```
sudo ufw allow 2222/tcp
```

```
#Активуємо брандмауер
```

```
sudo ufw enable
```

```
# Перевіряємо поточний статус та відкриті порти у міжмережевому екрані
```

```
sudo ufw status verbose
```

5. Розгортання оточення Ollama та запуск локальної ШІ-моделі:

```
# Завантажуємо офіційний інсталяційний скрипт та запускаємо його
```

```
curl -fsSL https://ollama.com/install.sh | sh
```

									Арк.
									48
Змн.	Арк.	№ док.м.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ				

Додаємо службу Ollama у менеджер сервісів для автоматичного старту

```
sudo systemctl enable ollama
```

Запускаємо службу Ollama

```
sudo systemctl start ollama
```

Перевіряємо статус роботи

```
sudo systemctl status ollama
```

Перевіряємо, чи сервер успішно прослуховує свій порт 11434

```
netstat -tuln | grep 11434
```

Запускаємо локальну мовну модель в режимі діалогу

```
ollama run mistral
```

6. Налаштування Open WebUI та інтеграція з Ollama:

Запускаємо Open WebUI з підключенням до локальної Ollama

```
docker run -d \
```

```
--name open-webui \
```

```
--restart always \
```

```
-p 3000:8080 \
```

```
-e OLLAMA_BASE_URL=http://host.docker.internal:11434 \
```

```
--add-host=host.docker.internal:host-gateway \
```

```
ghcr.io/open-webui/open-webui:main
```

Перевіряємо чи запущено контейнер

```
docker ps
```

Веб-інтерфейс доступний за адресою 192.168.50.10 : 3000

На сервері S_1 успішно розгорнуто локальну ШІ-модель на базі Ollama Open та WebUI, що забезпечує компанії “MidHub” доступ до інструментів штучного інтелекту в межах внутрішньої мережі. Впроваджені заходи безпеки забезпечують захист від несанкціонованого доступу та гарантують конфіденційність корпоративних даних.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		49

3.2.2 Інструкція з налаштування файлового сервера

Сервер S_2 призначений для централізованого зберігання даних, організації розмежованого доступу користувачів до файлових ресурсів та динамічного керування адресацією. Розгортання здійснюється на операційній системі Windows Server 2022.

Налаштування здійснюються за наступними етапами [24]:

Після першого запуску сервера відкривається консоль Server Manager. Початкова сторінка консолі зображена на рисунку 3.1.

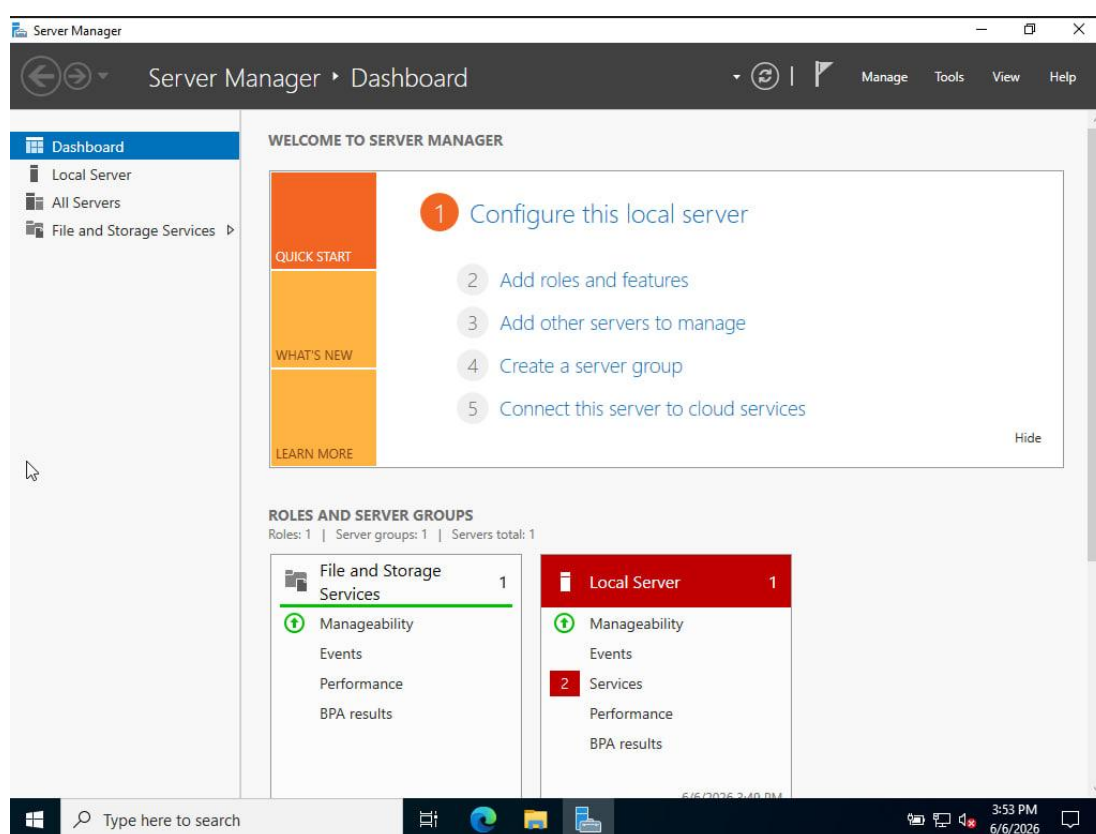


Рисунок 3.1 – Початковий екран Server Manager

Для розгортання доменної структури через майстер Add Roles and Features обирається роль Active Directory Domain Services разом із компонентами Group Policy Management, AD DS Tools та Active Directory Administrative Center (див. рис. 3.2).

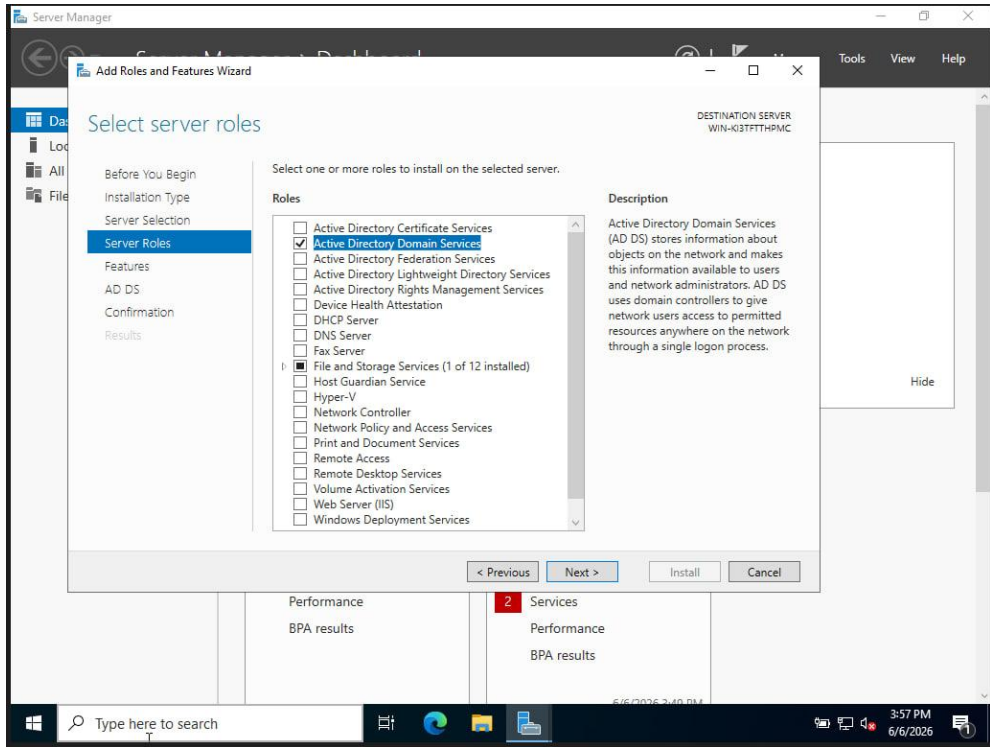


Рисунок 3.2 – Вікно вибору ролі

Після підтвердження вибору запускається процес встановлення. На рисунку 3.3 зображено вікно процесу встановлення.

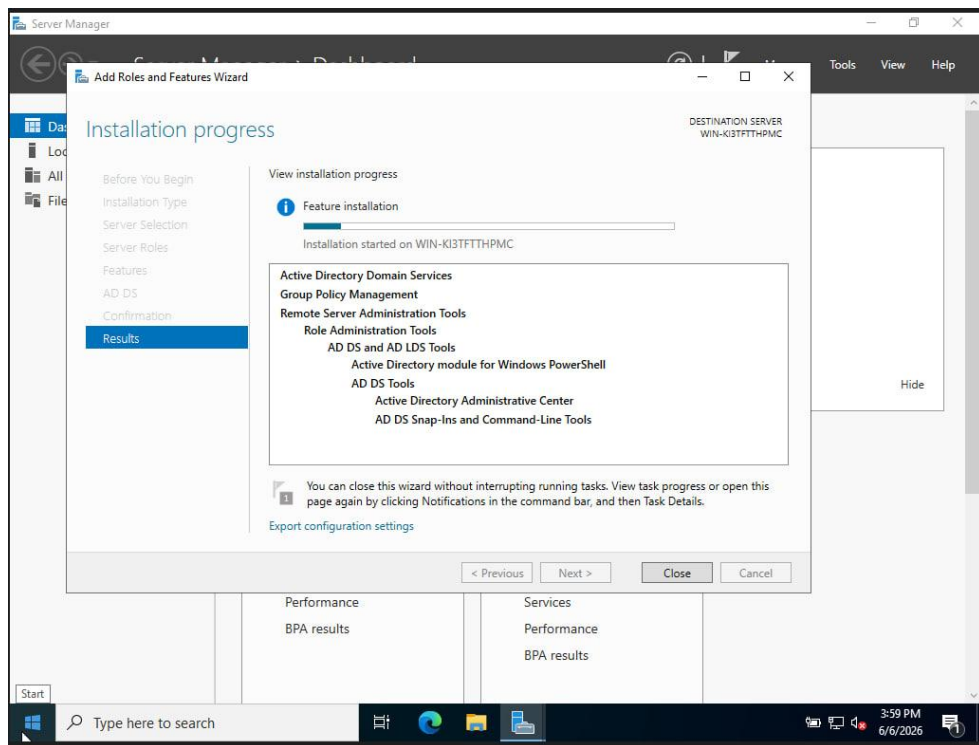


Рисунок 3.3 – Вікно встановлення

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Після успішного встановлення AD DS система сповіщає про необхідність розширеного налаштування (див. рис. 3.4).

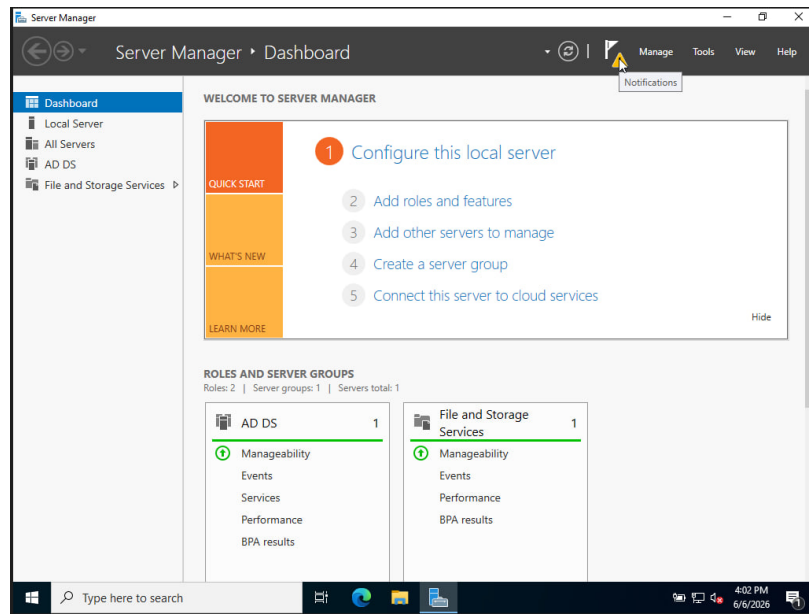


Рисунок 3.4 – Попередження системи

Далі запускається майстер конфігурації Active Directory Domain Services Configuration Wizard. Вибирається операція створення нового лісу з доменом midhub.local (див. рис. 3.5).

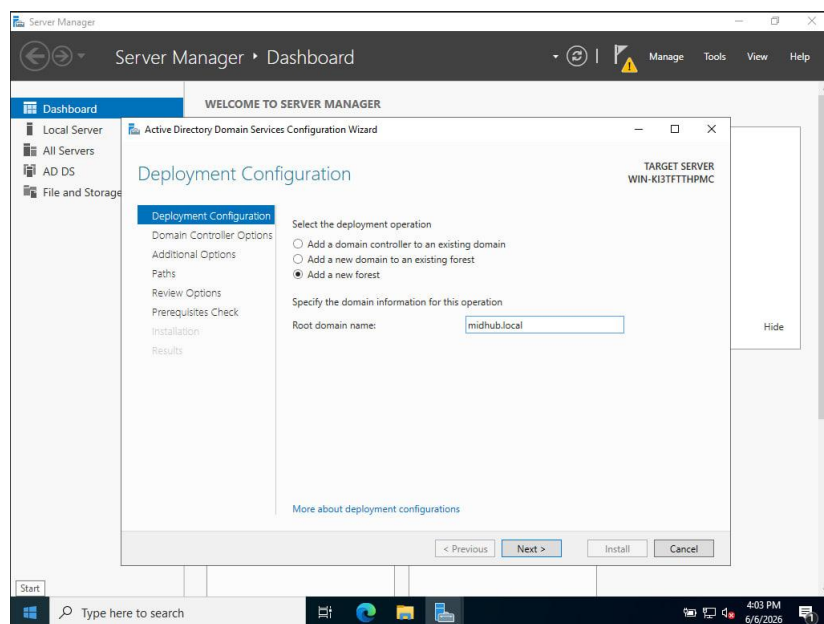


Рисунок 3.5 – Створення лісу з корневим доменом

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

На етапі налаштування контролера домену активуються наступні служби: DNS Server, Global Catalog, встановлюється пароль відновлення DSRM (див. рис. 3.6).

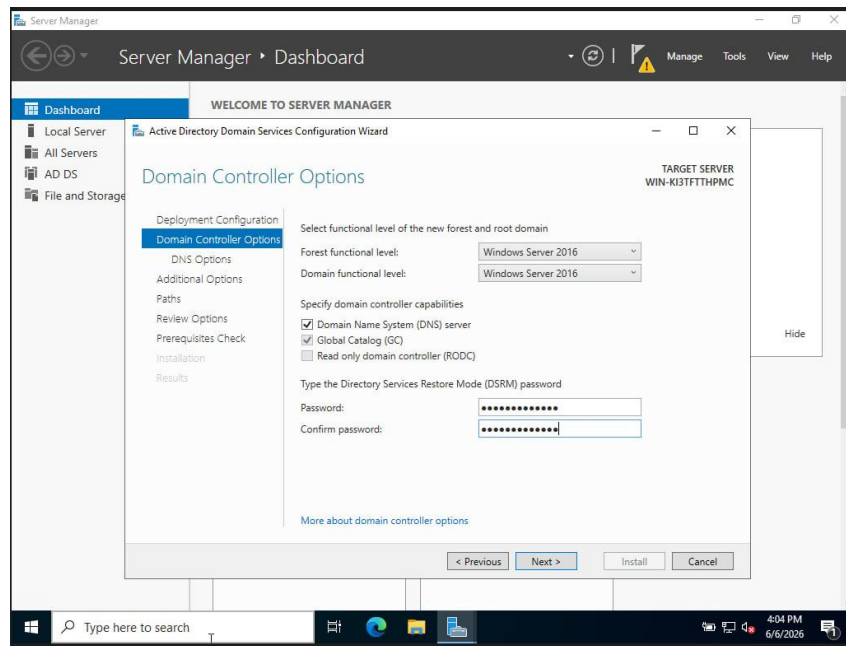


Рисунок 3.6 – Налаштування параметрів контролера домену

NetBIOS-ім'я домену автоматично визначається як MIDHUB (див. рис. 3.7).

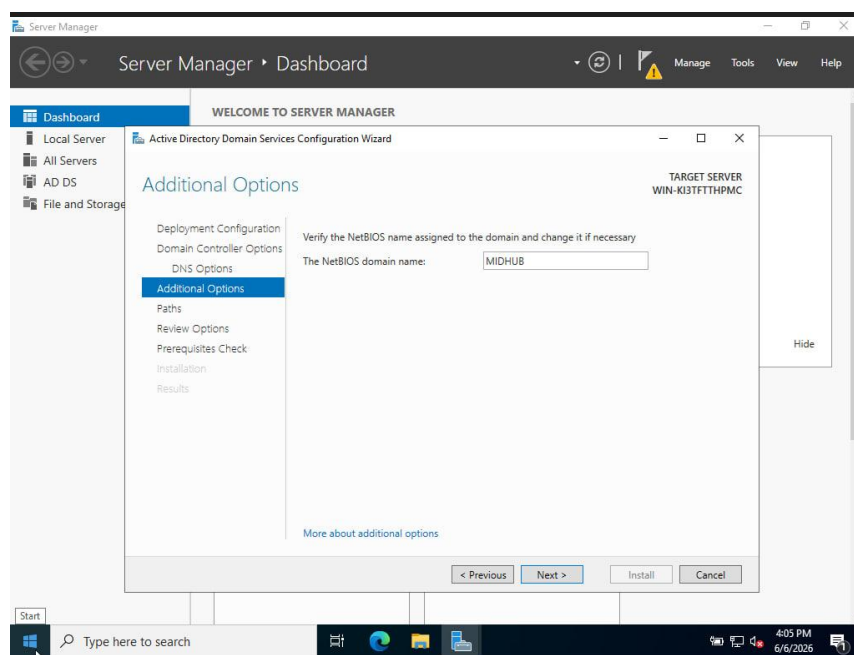


Рисунок 3.7 – Визначення NetBIOS-ім'я домену

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Шляхи розміщення бази даних AD, журналів та папки SYSVOL залишається за замовчуванням (див. рис. 3.8).

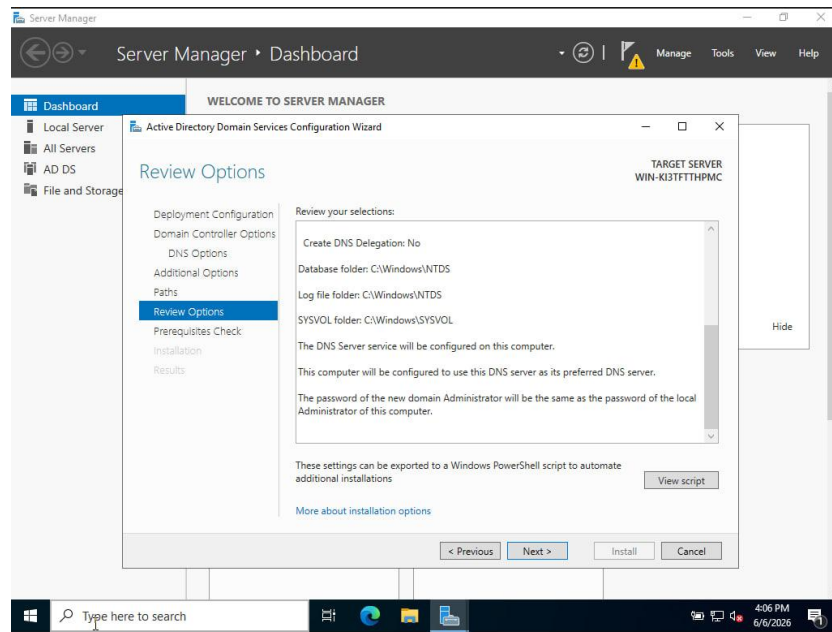


Рисунок 3.8 – Огляд параметрів перед встановленням

Після перевірки налаштувань виконується встановлення та автоматичне перезавантаження сервера. Тоді вхід виконується від імені адміністратора MIDHUB\Administrator, що підтверджує вдале розгортання домену (див. рис. 3.9).

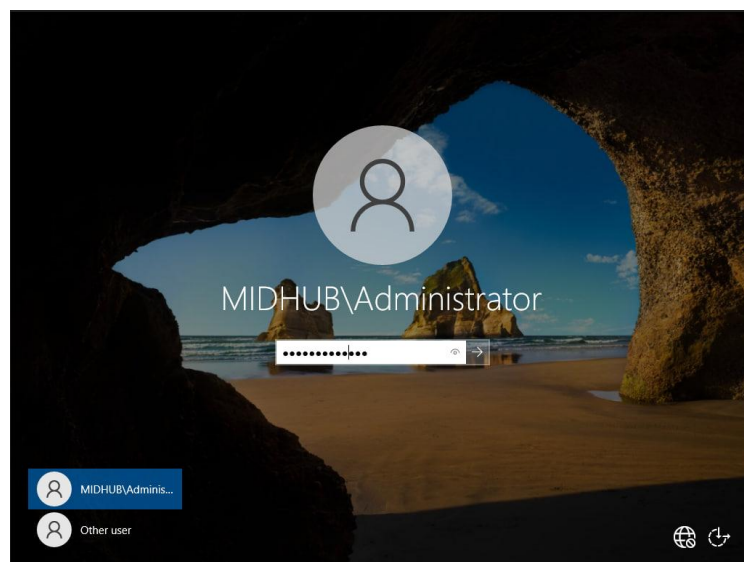


Рисунок 3.9 – Вхід в систему під доменним обліковим записом

									Арк.
									54
Змн.	Арк.	№ докum.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ				

Перезавантаживши систему в консолі Server Manager показуються всі налаштовані вище ролі: Active Directory Domain Services, DNS Server, File and Storage Services (див. рис. 3.10).

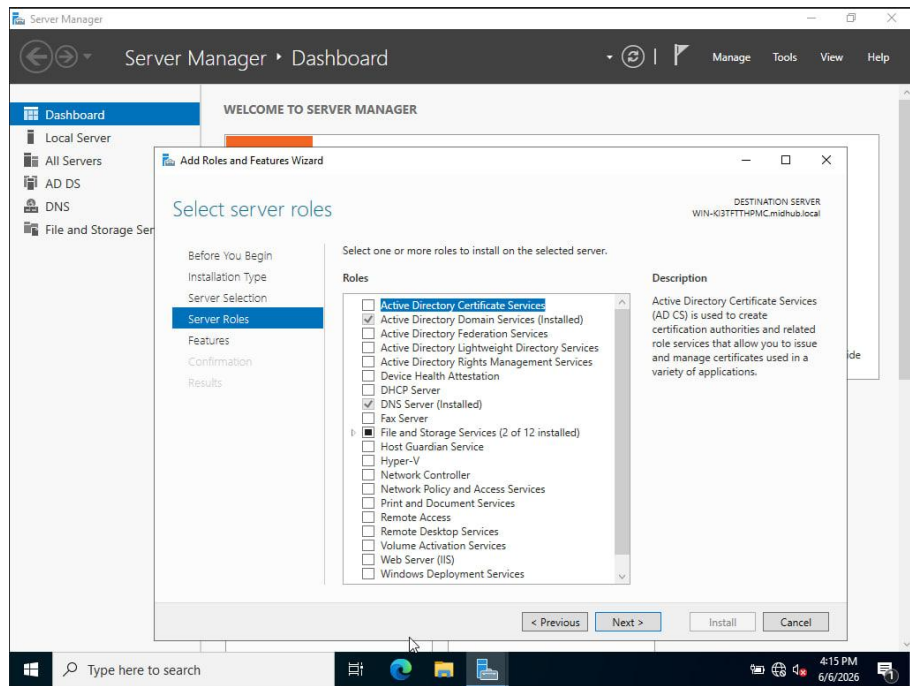


Рисунок 3.10 – Перелік встановлених ролей

Також виконується налаштування через PowerShell з правами адміністратора. Спочатку виконується сканування дискової системи та ініціалізація накопичувачів (див. рис. 3.11).

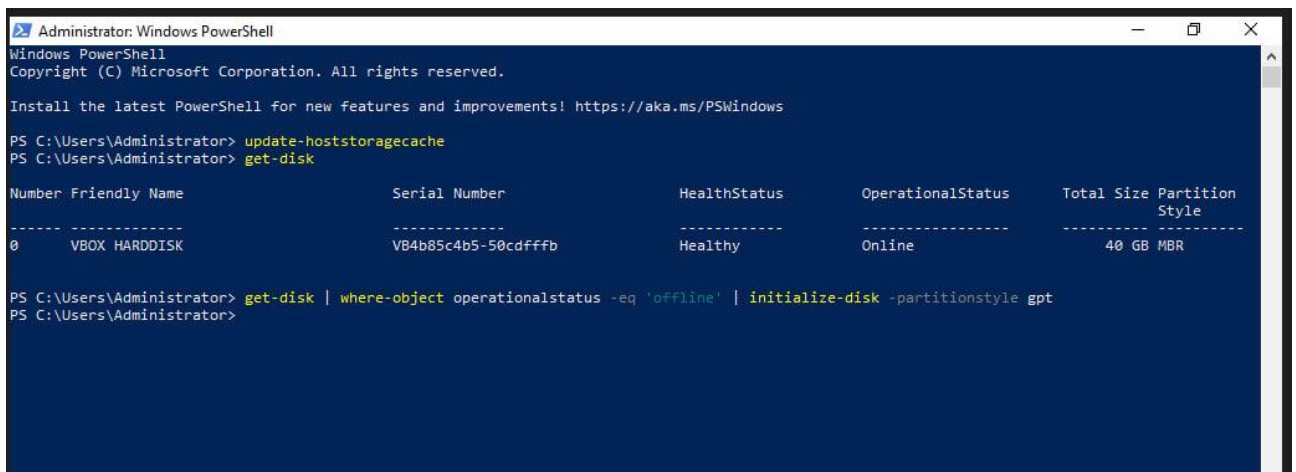


Рисунок 3.11 – Сканування дискової системи

Далі створюється спільна папка Company_Share та мережевий ресурс SMB з описом цієї папки (див. рис. 3.12) [21].

```
PS C:\Users\Administrator> new-item -itemtype directory -path "C:\Company_Share"

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----           6/6/2026   5:19 PM         Company_Share

PS C:\Users\Administrator> new-smbshare -name "Company_Share" -path "C:\Company_Share" -fullaccess everyone -description "Central Storage"

Name                ScopeName Path                Description
----                -
Company_Share *      C:\Company_Share    Central Storage

PS C:\Users\Administrator>
```

Рисунок 3.12 – Створення спільної папки

На останньому етапі конфігуруються списки контролю доступу ACL, де адміністратори отримують повний контроль, а звичайним користувачам надаються права читання та запису (див. рис. 3.13).

```
PS C:\Users\Administrator> $acl = get-acl "C:\Company_Share"
PS C:\Users\Administrator> $acl.setaccessruleprotection($True, $False)
PS C:\Users\Administrator> set-acl "C:\Company_Share" $acl
PS C:\Users\Administrator> $managerrule = new-object system.security.accesscontrol.filesystemaccessrule("administrators", "fullcontrol", "contai
nerinherit, objectinherit", "none", "allow")
PS C:\Users\Administrator> $userrule = new-object system.security.accesscontrol.filesystemaccessrule("users", "readandexecute, write", "contai
nerinherit, objectinherit", "none", "allow")
PS C:\Users\Administrator> $acl.addaccessrule($managerrule)
PS C:\Users\Administrator> $acl.addaccessrule($userrule)
PS C:\Users\Administrator> set-acl "C:\Company_Share" $acl
PS C:\Users\Administrator> get-acl "C:\Company_Share" | Format-List

Path      : Microsoft.PowerShell.Core\FileSystem::C:\Company_Share
Owner     : BUILTIN\Administrators
Group     : MIDHUB\Domain Users
Access    : BUILTIN\Administrators Allow FullControl
           BUILTIN\Users Allow Write, ReadAndExecute, Synchronize
Audit     :
Sddl     : O:BAG:DUD:PAI(A;OICI;FA;;;BA)(A;OICI;0x1201bf;;;BU)

PS C:\Users\Administrator>
```

Рисунок 3.13 – налаштування та перевірка списків контролю доступу

Отже, сервер налаштовано успішно як контролер домену midhub.local з працюючими службами Active Directory Domain Services, DNS Server, File and Storage Services. Також розгорнута структура забезпечує управління обліковими записами користувачів та обмежений доступ до спільних ресурсів компанії “MidHub”.

3.2 Інструкція з налаштування активного комутаційного обладнання

3.2.3 Інструкція з налаштування комутаторів робочих груп

На рівні доступу мережевої системи використовуються керовані комутатори Cisco Catalyst C1300-16P-4X [17]. Основне призначення яких – підключення кінцевих пристроїв (робочих станцій та принтера) до мережі, первинна інкапсуляція трафіку у відповідні VLAN та ізоляція широкомовних доменів. Також вони реалізують механізми безпеки на рівні портів а саме: обмеження кількості MAC-адрес та блокування несанкціонованих підключень за допомогою Port Security.

1. Налаштування комутатора SW_1

Комутатор фізично встановлено у серверній шафі кабінету 117. Обслуговує сегмент VLAN 10 (Dev_Wired) та забезпечує дротове з'єднання робочих станцій WS_1-WS_11. Це найбільш навантажений сегмент мережі з огляду вимог до пропускної здатності, оскільки розробники, які підключені до цього сегменту активно використовують мережеві ресурси для роботи з репозиторіями, хмарними сервісами та ІІТ-системою.

Для реалізації безпечного віддаленого адміністрування на комутаторі налаштовано інтерфейс управління у VLAN 50 з IP-адресою 192.168.50.3 та шлюзом 192.168.50.1. Доступ до пристрою захищено протоколом SSH версії 2 з використанням RSA-ключа довжиною 2048 біт, що унеможливує перехоплення облікових даних. Також встановлено паролі на привілейований режим та консольний порт.

Клієнтські порти GigabitEthernet1/0/2-12 налаштовано в режим access з прив'язкою до VLAN 10. На всіх портах підключено функцію Spanning Tree, вона дозволяє пристроям переходити в активний стан без затримок при початковому підключенні завдяки цьому скорочується час готовності робочих станцій до роботи після ввімкнення.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		57

На кожному порті реалізовано Port Security з обмеженням однієї MAC-адреси. Якщо буде спроба підключення стороннього пристрою, то режим реагування restrict фіксує порушення в журналі подій без блокування порту, відповідно ця функція дозволяє адміністратору відстежити несанкціоноване підключення без переривання роботи користувачів.

Зв'язок з SW_2 реалізовано через оптичний SFP+ порт TenGigabitEthernet1/0/1 з дозволим VLAN 10 і VLAN 50. Повна конфігурація комутатора SW_1 наведена в додатку В кваліфікаційної роботи.

2. Налаштування комутатора доступу SW_3

Комутатор розміщено у телекомунікаційній шафі кабінету 109. Він забезпечує підключення 8 робочих станцій керівництва та бухгалтерії, а також мережевого принтера у межах відокремленого фінансово-адміністративного сегмента VLAN 30. Пристрій обслуговує кінцеві точки, розташовані у приміщеннях кабінетів 109 та 110, а саме WS_25-WS_32. Цей сегмент є одним з найбільш захищених у мережі. Забезпечення безпеки реалізовується правилами брандмауера маршрутизатора R_1, забороняючи доступ з бездротових сегментів VLAN 20 та VLAN 40.

Аналогічно до SW_1, на комутаторі налаштовано інтерфейс управління у VLAN 50 з IP-адресою 192.168.50.4, захищений доступ по SSH з RSA-ключем 2048 біт та паролі на привілейований режим та консольний порт. Це створює єдину політику адміністрування для комутаторів в мережі.

Порти GigabitEthernet1/0/2-9 налаштовано в режимі access з прив'язкою до VLAN 30. Порт GigabitEthernet1/0/10 також налаштовано в режим access для підключення мережевого принтера, що дозволяє всім користувачам в межах VLAN 30 використовувати спільний друк. На клієнтських портах активовано PortFast та Port Security з обмеженням одного пристрою на порт і режимом restrict.

Підключення до SW_2 виконується реалізовано через оптичний SFP+ порт TenGigabitEthernet1/0/1 з дозволим VLAN 30 і VLAN 50. Невикористані порти

									Арк.
									58
Змн.	Арк.	№ док.м.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ				

інтерфейси 4-16 вимкнено з міркувань безпеки. Повна конфігурація центрального комутатора наведена у додатку Д кваліфікаційної роботи.

3.2.3 Інструкція з налаштування маршрутизатора

Маршрутизатор R_1 виступає як центральний пристрій управління трафіком мережі компанії “MidHub”. Цей пристрій реалізовує функції міжVLAN маршрутизації, вихід в глобальну мережу, політики безпеки за допомогою міжмережевого екрана та обмежує пропускну здатність для кожного сегмента.

На базі порту ether1, підключеного до комутатора SW_2 через SFP+ канал, реалізуються п’ять віртуальних інтерфейсів для кожного VLAN [23]. Кожному віртуальному інтерфейсу призначається своя IP-адреса, що являється шлюзом за замовчуванням для пристроїв: 192.168.10.1 для VLAN 10, 192.168.20.1 для VLAN 20, 192.168.30.1 для VLAN 30, 192.168.40.1 для VLAN 40 та 192.168.50.1 для VLAN 50.

Для реалізації доступу до глобальної мережі прописується статичний маршрут за замовчуванням у бік провайдера через порт ether2. DNS-сервери налаштовано на загальнодоступні адреси 8.8.8.8. та 8.8.4.4 з дозволом обробки зовнішніх запитів.

Для обміну інформацією про підмережі конфігурується протокол динамічної маршрутизації OSPF v2 [20]. Створюється OSPF_Core з ідентифікатором маршрутизатора 192.168.50.1 та магістральна область Backbone Area 0.0.0.0, яка об’єднує всі п’ять підмереж.

Щоб забезпечити доступ користувачів до мережі Інтернет реалізовується трансляція мережевих адрес на інтерфейсі ether2 у режимі masquerade, що дозволяє пристроям безпечно виходити в Інтернет, використовуючи одну спільну публічну IP-адресу.

Захист та розмежування доступу реалізовано за допомогою правил фільтрації брандмауера [18]. Правила застосовуються до ланцюжка forward і

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		60

обробляються послідовно зверху вниз. Призначення та обґрунтування для кожного правила безпеки наведено в таблиці 3.1.

Таблиця 3.1 – Обґрунтування правил фільтрації брандмауера

Ідентифікатор	Критерії фільтрації трафіку	Дія	Обґрунтування
1	2	3	4
ACL_1	connection-state=established, related	ACCEPT	Дозволяє проходження відповідей на вже відкриті запити, що зменшує навантаження на процесор маршрутизатора.
ACL_2	src-address=192.168.40.0/24 dst-address=192.168.30.0/24	DROP	Повністю ізолює бездротову мережу персоналу від комп'ютерів керівництва для захисту комерційних даних.
ACL_3	src-address=192.168.20.0/24 dst-address=192.168.30.0/24	DROP	Блокує можливість доступу з бездротової мережі тестувальників до адміністративного сегмента, що захищає робочі станції менеджменту.
ACL_4	src-address=192.168.40.0/24 dst-address=192.168.50.0/24	DROP	Обмежує доступ звичайних працівників офісу до серверів ІІІ та баз даних(доступ залишається лише для розробників).
ACL_5	connection-state=invalid	DROP	Забезпечує автоматичне видалення пошкоджених пакетів, захищаючи мережу від збоїв та базових атак.

Розподіл пропускної здатності між підмережами реалізовано за допомогою НТВ [19]. Завдяки цій функції закріплюється необхідна швидкість Інтернету за кожним відділом. Трафік кожного сегмента маркується засобами Mangle за IP-адресою, після цього створюється окрема черга з індивідуальним обмеженням для кожного VLAN: VLAN 10 (DevOps) – 300 Мбіт/с, VLAN 20 (QA WiFi) – 250 Мбіт/с, VLAN 30 (Management) – 150 Мбіт/с, VLAN 40 (Staff) – 100 Мбіт/с, VLAN 50 (Infrastructure) – 500 Мбіт/с. Завдяки такому розподілу розробникам та

серверна інфраструктура отримують пріоритет, забезпечуючи потреби основних робочих процесів.

Повний скрипт налаштування RouterOS маршрутизатора R_1 наведено у додатку Е.

3.2.4 Інструкція з налаштування точок доступу

Для реалізації бездротової інфраструктури використано точки доступу MikroTik hAP ax3 з підтримкою стандарту Wi-Fi 6 (802.11ax). Налаштування пристроїв виконується в межах архітектури Bridge VLAN Filtering під управлінням ОС RouterOS. Це дозволяє реалізувати апаратне тегування та комутацію трафіку на рівні комутаційного чіпа пристрою, знижуючи навантаження на центральний процесор.

Налаштовуючи бездротовий сегмент основним рішенням стало розділення середовищ передавання даних, за якого клієнтські радіоінтерфейси ізольовані та закріплені за відповідними віртуальними мережами.

Для бездротової мережі тестувальників виділено VLAN 20, а для загального персоналу VLAN 40. Задля безпеки інтерфейси керування точками доступу перенесені в мережу VLAN 50. У цьому сегменті точці AP_1 призначено IP-адресу 192.168.50.5, а точці AP_2 – 192.168.50.6. Захист обладнання реалізовано через брандмауер. У ланцюжку input прописані правила, які дозволяють підключення до налаштувань лише з адміністративного сегменту 192.168.50.0/24, спроби з боку клієнтів автоматично блокуються.

Додатково для захисту на пристроях вимкнено незахищені служби Telnet, FTP, HTTP та API. Замість них для адміністрування використовується протокол SSH та утиліта WinBox. Для оптимальної роботи в налаштуваннях радіомодулів вказано регіон country=Ukraine. Щоб системні журнали та логи відображали точний час, налаштовано клієнт NTP, що синхронізує пристрої через національний пул серверів ua.pool.ntp.org. Повні скрипти налаштування точок доступу для AP_1 наведені в додатку Є, а для AP_2 в додатку Ж.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		62

3.3 Інструкція з використання тестових наборів та тестових програм

У підрозділі описано порядок перевірки та тестування налаштованої мережі. Наведені кроки дозволяють переконатись у правильності взаємодії всіх пристроїв, належній роботі правил безпеки та точності обмеження пропускнуої здатності.

Процедуру контролю розділено на три етапи:

1. Перевірка кабельних ліній та комутації

В основному тестування починається з перевірки фізичних з'єднань. Щоб перевірити правильний обтиск кабелю та виявити можливі механічні пошкодження ліній необхідно використовувати кабельний тестер для витої пари. Стабільність роботи портів та з'єднань між всім активним обладнанням перевіряється за допомогою світлодіодних індикаторів на панелях пристроїв та шляхом перегляду системних логів ОС.

2. Перевірка маршрутизації та брандмауера

Для тестування доступності мережевих ресурсів та контролю описаних обмежень виконується надсилання тестових пакетів. Щоб перевірити зв'язок із сервером та вихід в Інтернет необхідно в консолі по черзі прописати наступні команди: ping 192.168.50.11 та ping 8.8.8.8.

Якщо обмін пакетів відбувався без втрат, то це підтверджує правильність налаштування статичних маршрутів. Також разом з цим здійснюється аналогічний запит із бездротової мережі VLAN 40 (Staff) до VLAN 30 (Management), це робиться для перевірки брандмауера і відсутність відповідей свідчить про правильну ізоляцію сегментів. Для додаткової перевірки проходження пакетів через усі транзитні вузли здійснюється команда traceroute 8.8.8.8. Перевірка стабільності каналів здійснюється за допомогою утиліти MTR, вона поєднує функції команд ping і traceroute, безперервно надсилаючи пакети до зазначеного вузла та відображає статистику по кожному проміжку вузла маршруту, враховуючи відсоток втрачених пакетів та показники затримки.

3. Тестування обмеження пропускнуої здатності

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		63

дозволяють проходження лише перевірених з'єднань зі статусами established та related, тоді як пошкоджені пакети зі статусом invalid автоматично видаляються. Ізоляція між сегментами забезпечується блокуванням трафіку з бездротового з'єднання VLAN 40 до підмережі керівництва VLAN 30 та серверного сегменту VLAN 50. Для забезпечення безпечного виходу в Інтернет та приховування внутрішньої адресації компанії від зовнішньої мережі застосовується реалізація динамічної трансляції мережевих адрес NAT на зовнішньому інтерфейсі маршрутизатора, що приховує внутрішню адресацію компанії за єдиною публічною IP-адресою провайдера.

- Для захисту облікових записів та розмежування доступу до корпоративних ресурсів на сервері S_2 організовано службу Active Directory Domain Services. Доступ до спільних папок за протоколом SMB надається авторизованим групам користувачів відповідно до підрозділу, тому несанкціонований доступ до чужих ресурсів неможливий на рівні файлової системи. Також додатковим рівнем захисту є парольна політика домену, що вимагає використання складних паролів та їх обов'язкову заміну кожні 90 днів.

3.5 Інструкція з експлуатації та моніторингу в мережі

Для забезпечення безперервної роботи мережі, продовження терміну служби обладнання та оперативного реагування на збої розроблено регламенти експлуатації і впроваджено систему моніторингу мережі. Повноцінна експлуатація локальної мережі передбачає наявність обов'язкового комплексу технічної документації, що складається з схем фізичної та логічної топології, таблиці розподілу IP-адрес та віртуальних мереж VLAN, а також специфікацію обладнання. На етапі проєктування архітектури було передбачено резервні порти підключення на комутаторах, що надає можливість масштабування мережі та підключення додаткових робочих станцій без внесення змін до логічної структури. Обов'язковою умовою стабільної експлуатації є дотримання

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		65

персоналом встановлених правил інформаційної безпеки. У межах корпоративної мережі користувачам суворо забороняється:

- самостійно змінювати параметри мережі робочих станцій;
- модифікувати або видаляти системні дані та налаштування прав доступу на сервері S_2;
- використовувати ПЗ без дозволу системного адміністратора;
- здійснювати дії, котрі можуть спричинити поширення шкідливого ПЗ або порушення цілісності даних.

Безперервний моніторинг стану мережі забезпечує вчасне виявлення збоїв у роботі. Основними напрямками контролю є: діагностика фізичного стану серверного обладнання, перевірка функціонування мережевих служб, контроль доступності інтернет-каналу, аналіз індикаторів апаратних засобів та перевірка доступності спільних мережевих ресурсів.

Маршрутизатор керується за допомогою утиліти WinBox, вона надає в режимі реального часу повний графічний доступ до всіх параметрів. Наприклад:

1. Моніторинг інтерфейсів

Розділ Interfaces відображає перелік усіх фізичних та віртуальних інтерфейсів, їх поточний стан та швидкість передачі. Адміністратор може в реальному часі спостерігати завантаженість інтерфейсу та виявляти аномальну активність. На рисунку 3.14 зображено розділ Interfaces утиліти WinBox.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet	Rx Packet	FP Tx	FP Rx
<input type="checkbox"/>	R ether1	Ethernet	1500			36.5 kbps	4.8 kbps	5	7	0 bps
<input type="checkbox"/>	R vlan10-...	VLAN	1500			0 bps	0 bps	0	0	0 bps
<input type="checkbox"/>	R vlan20-...	VLAN	1500			0 bps	0 bps	0	0	0 bps
<input type="checkbox"/>	R vlan30-...	VLAN	1500			0 bps	0 bps	0	0	0 bps
<input type="checkbox"/>	R vlan40-...	VLAN	1500			0 bps	0 bps	0	0	0 bps
<input type="checkbox"/>	R vlan50-...	VLAN	1500			0 bps	0 bps	0	0	0 bps
<input type="checkbox"/>	R lo	Loopback	65536			0 bps	0 bps	0	0	0 bps

Рисунок 3.14 – Перелік мережевих інтерфейсів

Queues										
Simple Queues										
Interface Queues										
Queue Tree										
Queue Types										
New Enable Disable Remove										
		Name	Parent	Packet ...	Limit At	Max Limit	Avg. Rate	Queued Bytes	Bytes	Packets
<input type="checkbox"/>		VLAN10-Dev	global	vlan10		300M	0 bps	0 B	0 B	0
<input type="checkbox"/>		VLAN20-QA	global	vlan20		250M	0 bps	0 B	0 B	0
<input type="checkbox"/>		VLAN30-Mgmt	global	vlan30		150M	0 bps	0 B	0 B	0
<input type="checkbox"/>		VLAN40-Staff	global	vlan40		100M	0 bps	0 B	0 B	0
<input type="checkbox"/>		VLAN50-Infra	global	vlan50		500M	0 bps	0 B	0 B	0

Рисунок 3.17 – Розділ управління чергами трафіку

5. Перевірка доступності командою ping

На рисунку 3.18 зображено результат перевірки доступності вузла 8.8.8.8 засобами Tools – Ping.

The screenshot shows the Mikrotik WinBox interface for the Ping tool. The 'General' tab is active, showing 'Ping To' set to 8.8.8.8, 'Packet Count' at 8, and 'Interval' at 1000 ms. The results summary indicates '8 of 8 packets received', '0 % packet loss', 'Min: 25.721 ms', 'Avg: 27.402 ms', and 'Max: 31.215 ms'. A table below shows the individual ping results:

Seq #	Host	Time	Reply Size	TTL	Status
2	8.8.8.8	25.802	56	118	
3	8.8.8.8	27.069	56	118	
4	8.8.8.8	26.770	56	118	
5	8.8.8.8	26.969	56	118	
6	8.8.8.8	28.260	56	118	
7	8.8.8.8	27.417	56	118	

Рисунок 3.18 – Результат перевірки доступності вузла

6. Відстеження маршруту командою traceroute

На рисунку 3.19 зображено результат відстеження маршруту до вузла 8.8.8.8 засобами Tools – Traceroute. Маршрут пройшов через 9 проміжних вузлів з втратами 0%, що підтверджує стабільність каналу зв'язку з Інтернетом.

Hop	Host	Loss	Sent	Last	Avg.	Best	Worst	Std. Dev.	History	Status
1	192.168.0.1	0.0%	8	3.2ms	4.1	2.4	10.2	2.3		
2	5.58.128.1	0.0%	8	6.1ms	6.2	4.4	8.3	1.1		
3	185.53.79.74	0.0%	8	11.5ms	11.1	10.2	11.6	0.5		
4	192.178.243.65	0.0%	8	14.7ms	14.3	13.1	16.3	1.0		
5	74.125.245.64	0.0%	8	19.1ms	14.8	12.1	19.1	2.6		
6	142.251.242.41	0.0%	8	27.2ms	26.3	24.7	27.4	0.9		
7	192.178.99.169	0.0%	8	25.1ms	25.3	24.2	26.0	0.6		
8	142.250.238.1	0.0%	8	27.4ms	27.6	26.0	29.3	0.9		
9	8.8.8.8	0.0%	8	27.2ms	26.3	24.7	27.2	0.9		

Рисунок 3.19 – Результати відстеження маршруту до вузла

7. Журнал подій

На рисунку 3.20 зображено розділ Log, який фіксує системні події маршрутизатора

#	Time	Buffer	Topics	Message
0	2026-06-08 02:0...	memory	system, info	router rebooted
1	2026-06-08 02:0...	memory	interface, info	lo link up
2	2026-06-08 02:0...	memory	interface, info	ether1 link up (speed 1G, full duplex)
3	2026-06-08 02:0...	memory	dhcp, info	dhcp-client on ether1 got IP address 192.168.0.105
4	2026-06-08 02:0...	memory	system, info, accou...	user admin logged in from 192.168.0.102 via winbox
5	2026-06-08 02:0...	memory	system, info	user admin password changed by admin

Рисунок 3.20 – Журнал системних подій маршрутизатора

Моніторинг комутаторів Cisco виконується по протоколу SSH за адресами управління у VLAN 50: SW_2 – 192.168.50.2, SW_1 – 192.168.50.3, SW_3 – 192.168.50.4.

1. Стан портів

На рисунку 3.21 зображено результат виконання команди `show interfaces status`, яка відображає поточний стан усіх портів комутатора – активні та відключені порти, швидкість та режим дуплексу. Адміністратор може швидко визначити які порти активні та виявити несподівані підключення до мережі.

```
SW_2#show interfaces status
Port      Name          Status      Vlan      Duplex  Speed Type
-----
Fa0/1     Fa0/1         notconnect  20        auto    auto  10/100BaseTX
Fa0/2     Fa0/2         notconnect  40        auto    auto  10/100BaseTX
Fa0/3     Fa0/3         notconnect  50        auto    auto  10/100BaseTX
Fa0/4     Fa0/4         notconnect  1         auto    auto  10/100BaseTX
Fa0/5     Fa0/5         notconnect  1         auto    auto  10/100BaseTX
Fa0/6     Fa0/6         notconnect  1         auto    auto  10/100BaseTX
Fa0/7     Fa0/7         notconnect  1         auto    auto  10/100BaseTX
Fa0/8     Fa0/8         notconnect  1         auto    auto  10/100BaseTX
Fa0/9     Fa0/9         notconnect  1         auto    auto  10/100BaseTX
Fa0/10    Fa0/10        notconnect  1         auto    auto  10/100BaseTX
Fa0/11    Fa0/11        notconnect  1         auto    auto  10/100BaseTX
Fa0/12    Fa0/12        notconnect  1         auto    auto  10/100BaseTX
Fa0/13    Fa0/13        notconnect  1         auto    auto  10/100BaseTX
Fa0/14    Fa0/14        notconnect  1         auto    auto  10/100BaseTX
Fa0/15    Fa0/15        notconnect  1         auto    auto  10/100BaseTX
Fa0/16    Fa0/16        notconnect  1         auto    auto  10/100BaseTX
Fa0/17    Fa0/17        notconnect  1         auto    auto  10/100BaseTX
Fa0/18    Fa0/18        notconnect  1         auto    auto  10/100BaseTX
Fa0/19    Fa0/19        notconnect  1         auto    auto  10/100BaseTX
Fa0/20    Fa0/20        notconnect  1         auto    auto  10/100BaseTX
Fa0/21    Fa0/21        notconnect  1         auto    auto  10/100BaseTX
Fa0/22    Fa0/22        notconnect  1         auto    auto  10/100BaseTX
Fa0/23    Fa0/23        notconnect  1         auto    auto  10/100BaseTX
Fa0/24    Fa0/24        notconnect  1         auto    auto  10/100BaseTX
Gig0/1    Gig0/1        notconnect  trunk    auto    auto  10/100BaseTX
Gig0/2    Gig0/2        notconnect  trunk    auto    auto  10/100BaseTX
```

Рисунок 3.21 – Стан портів комутатора

2. Стан VLAN

На рисунку 3.22 зображено результат виконання команди `show vlan brief`, яка відображає перелік створених VLAN та прив'язку портів до кожного сегмента. Це дозволяє перевірити коректність сегментації мережі та відповідність налаштувань.

```
SW_2#show vlan brief
VLAN Name                Status      Ports
-----
1    default                active     Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                           Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                           Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24, Gig0/1, Gig0/2
10   Dev_Wired              active
20   QA_Dev_WiFi           active     Fa0/1
30   Management             active
40   Staff_WiFi            active     Fa0/2
50   Infrastructure          active     Fa0/3
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

Рисунок 3.22 – Стан VLAN та прив'язка портів

Адміністрування та моніторинг серверів реалізовано на базі ОС Windows Server 2022 та Ubuntu Server. Це дозволяє контролювати роботу служб Active Directory, DNS, журнал подій, а також відстежувати стабільність процесів ІІІ в реальному часі.

- сервер S_2 (Windows Server 2022):

1. Журнал подій

На рисунку 2.23 зображено консоль Event Viewer, розділ Windows Logs – System, який показує системні події сервера. Регулярний перегляд дозволяє виявити проблема з роботою служб до того, як вони призведуть до збоїв.

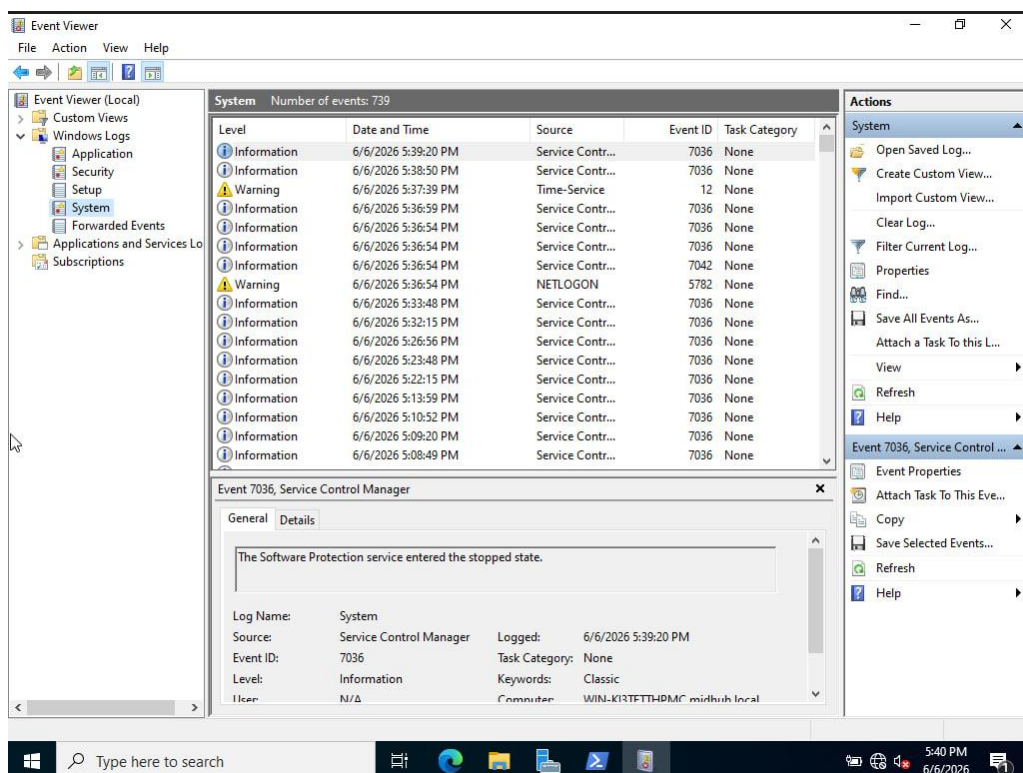


Рисунок 3.23 – Журнал системних подій сервера

2. Управління користувачами

На рисунку 3.24 зображено консоль Active Directory Users and Computers з структурою домену midhub.local. Адміністратор може керувати обліковими записами, налаштовувати групові політики та контролювати доступ до ресурсів мережі.

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

71

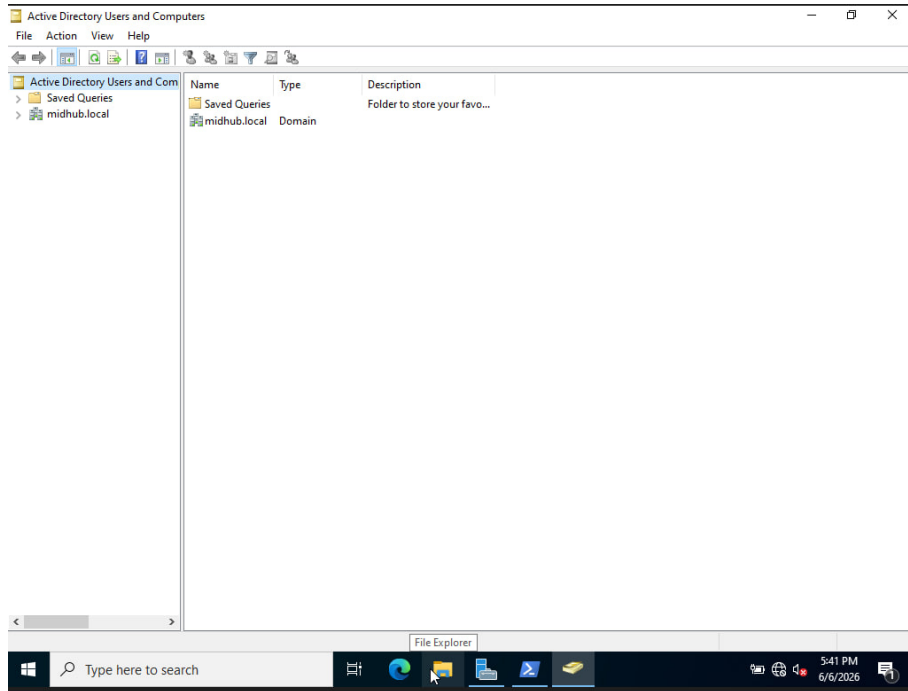


Рисунок 3.24 – Структура домену midhub.local

3. Моніторинг DNS

На рисунку 3.25 зображено DNS Manager з переліком DNS-зон домену midhub.local. Адміністратор може перевіряти правильність DNS-записів та діагностувати проблеми з розпізнаванням імен у мережі.

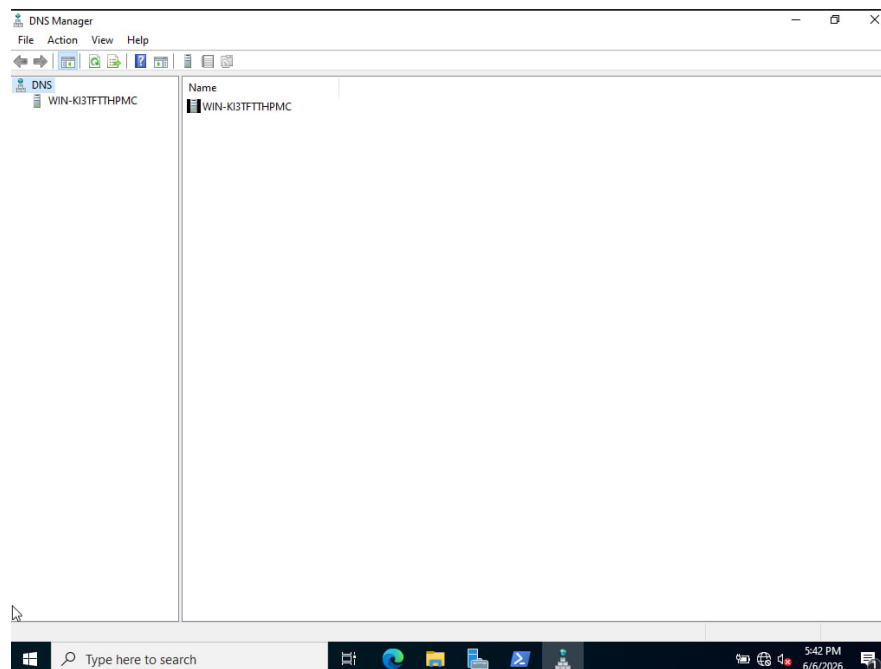


Рисунок 3.25 – Стан DNS-сервера

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

- сервер S_1 (Ubuntu Server):

Моніторинг ШІ-сервера реалізовується через SSH-підключення. Для здійснення перевірки стану сервісів адміністратор послідовно виконує наступні команди.

1. Перевірка стану сервісу Ollama – команда виводить стан служби, час запуску та останні записи журналу: `sudo systemctl status ollama`;

2. Перевірка стану контейнера Open WebUI – команда відображає список активних Docker-контейнерів та час їх роботи: `docker ps`;

3. Перегляд журналу контейнера Open WebUI – команда виводить останні події в журналі контейнера для діагностики можливих помилок: `docker logs open-webui`;

4. Моніторинг використання ресурсів процесора та оперативної пам'яті: `htop`;

5. Перевірка відкритих мережевих портів – команда відображає список активних з'єднань та портів що прослуховуються, зокрема 11434 для Ollama та порт 3000 для Open WebUI : `netstat -tuln`.

										Арк.
										73
Змн.	Арк.	№ док.м.	Підпис	Дата	<i>2026.КВР.123.406.11.00.00 ПЗ</i>					

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини роботи є техніко-економічне обґрунтування та розрахунок фінансової ефективності проекту локальної мережі ІТ-компанії “MidHub”. У межах розділу здійснено календарне планування етапів розробки та сформовано сумарний кошторис витрат. Він деталізує інвестиції в обладнання, витрати на оплату праці інженерів та амортизаційні відрахування. Отримані показники слугують фінансовим підґрунтям для оцінки доцільності впровадження та масштабування проекту.

Для розрахунку вартості НДР необхідно виконати наступні етапи:

- описати технологічний процес розробки із зазначенням трудомісткості кожної операції;
- визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;
- визначити суму матеріальних затрат;
- обчислити витрати на електроенергію для науково-виробничих цілей;
- розрахувати транспортні витрати;
- нарахувати суму амортизаційних відрахувань;
- визначити суму накладних витрат;
- скласти кошторис та визначити собівартість НДР;
- розрахувати ціну НДР;
- визначити економічну ефективність та термін окупності продукту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

З метою визначення сумарної тривалості проектування, дані про затрати часу на всі окремі етапи процесу зведено в таблицю 4.1.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		74

Таблиця 4.1 – Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Підготовка	Керівник	12
2	Розробка проєкту мережі	Інженер	35
3	Монтаж кабелів та розеток	Технік	25
4	Налаштування активного комутаційного обладнання	Інженер	20
5	Інсталяція та налаштування серверів	Інженер	11
6	Тестування мережі	Інженер	5
Разом			108

Згідно з проведеними розрахунками, сумарний час, необхідний для виконання всіх етапів розробки та впровадження комп'ютерної мережі, становить 108 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до нормативних положень Закону України «Про оплату праці», під заробітною платою розуміють винагороду (зазвичай у грошовому еквіваленті), яку роботодавець виплачує працівникові за виконаний обсяг робіт.

На її кінцевий розмір безпосередньо впливають складність і умови праці, професійні та ділові якості фахівця, а також загальні фінансово-господарські результати діяльності підприємства. Структурно заробітна плата складається з двох основних частин: основної та додаткової виплат. Нарахування основної

заробітної плати здійснюється за фактично виконані завдання згідно з посадовими окладами, тарифними ставками чи відрядними розцінками, і ця сума не пов'язана з поточним прибутком компанії.

Додаткова заробітна плата виступає елементом загального фонду оплати праці та охоплює виплати, які прямо не залежать від кількості відпрацьованого часу. Вона розраховується з урахуванням досягнутих результатів, умов на виробництві та кваліфікаційного рівня виконавців. Головним джерелом для фінансування додаткової оплати є фонд матеріального стимулювання, що утворюється за рахунок прибутку фірми.

Розрахунок основної заробітної плати здійснюється за формулою:

$$Z_{осн.} = T_c \cdot K_2, \quad (4.1)$$

де T_c – годинна тарифна ставка працівника, грн/год. (приймаємо для керівника проєкту – 175 грн/год, інженера – 180 грн/год, техніка – 140 грн/год). Вихідні дані стосовно вартості годинної оплати праці фахівців необхідної кваліфікації встановлено на основі моніторингу наявних вакансій і статистичних звітів про доходи в ІТ-сфері, оприлюднених на профільному ресурсі DOU [14].

K_2 – кількість відпрацьованих годин згідно з етапами розробки.

$$Z_{осн.} = 175 \cdot 12 + 180 \cdot 71 + 140 \cdot 25 = 18380 \text{ грн.}$$

Під додатковою заробітною платою розуміють грошову винагороду за працю понад установлені нормативи, за особливі умови праці, виробничі досягнення та професійну винахідливість. До цієї категорії належать різноманітні надбавки, доплати, гарантійні та компенсаційні виплати, регламентовані чинним законодавством, а також премії за якісне виконання виробничих завдань.

Величина додаткової оплати праці розраховується в межах від 10% до 15% від сформованого фонду основної заробітної плати:

$$Z_{дод.} = Z_{осн.} \cdot K_{опл.}, \quad (4.2)$$

де $K_{опл.}$ – коефіцієнт додаткових виплат працівникам.

$$Z_{дод.} = 18380 \cdot 0,15 = 2757 \text{ грн.}$$

Таким чином, загальний обсяг витрат на оплату праці ($B_{о.п.}$) обчислюється за формулою:

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		76

$$B_{o.n.} = Z_{ocn.} + Z_{dod.}, \quad (4.3)$$

$$B_{o.n.} = 18380 + 2757 = 21137 \text{ грн.}$$

Окрім прямих виплат персоналу, фінансовий план проєкту враховує обов'язкові нарахування на фонд оплати праці у вигляді єдиного соціального внеску (ЄСВ), ставка якого становить 22%. Підсумковий обсяг відрахувань на соціальні заходи визначається від отриманої суми витрат на оплату праці за формулою:

$$B_{c.z.} = \Phi O П \cdot 0,22, \quad (4.4)$$

де $\Phi O П$ – фонд оплати праці, грн.

$$B_{c.z.} = 21137 \cdot 0,22 = 4650,14 \text{ грн.}$$

Обчислені показники витрат на заробітну плату та соціальні відрахування структуровано й наведено в таблиці 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатко-ва заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тарифна ставка, грн.	К-сть від-працьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Керівник	175	12	2100	315	-	-
2	Інженер	180	71	12780	1917	-	-
3	Лаборант	140	25	3500	525	-	-
	Разом	-	-	18380	2757	4650,14	25787,14

4.3 Розрахунок матеріальних витрат

Розрахунок матеріальних витрат здійснюється на основі кількості використаних ресурсів та їхньої поточної вартості за такою формулою:

$$M_{Bi} = q_i \cdot p_i, \quad (4.5)$$

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		77

де q_i – кількість витраченого матеріалу i -го виду;

p_i – ціна матеріалу i -го виду.

Загальний обсяг матеріальних витрат ($Z_{м.в.}$) визначається як сума вартостей усіх елементів, залучених для побудови мережевої інфраструктури:

$$Z_{м.в.} = \sum M_{Bi} \quad (4.6)$$

$$Z_{м.в.} = 5244 + 535 + 387,40 + 225 + 579 + 1880 + 2175 + 1700 + 6435 + 7360 + 7295 + 12600 + 480 + 480 + 734 + 6314 + 35000 + 69400 + 11300 + 286000 + 58700 + 11600 + 41400 = 567823,40 \text{ грн.}$$

Усі техніко-економічні показники матеріальних витрат, що включають найменування ресурсів, одиниці виміру, обсяги та фінальну вартість, систематизовані й представлені у таблиці 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Кабель UTP Cat 6	м	228	23	5244
2	Короб 60*40 (2м)	шт.	10	53,50	535
3	Короб 25*16 (2м)	шт.	26	14,90	387,40
4	Короб 16*16 (2м)	шт.	20	11,25	225
5	Роз'єм RJ45 Cat 6	шт.	100	5,79	579
6	Мережева розетка	шт.	20	94	1880
7	Патч-корд (мідний) CAT6 UTP 0.5 м	шт.	29	75	2175
8	Патч-корд (мідний) CAT6 UTP 2 м	шт.	20	85	1700
9	Патч-панель Cat 6 24 портів	шт.	3	2145	6435
10	Серверна шафа 12U	шт.	2	3680	7360
11	Серверна стійка CMS 24U	шт.	1	7295	7295

Змн.	Арк.	№ док.м.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

78

Продовження таблиці 4.3

1	2	3	4	5	6
12	Оптичний трансивер MikroTik S+85DLC03D	шт.	8	1575	12600
13	Патч-корд (оптичний) LC- LC Duplex MM OM3 2м	шт.	2	240	480
14	Патч-корд (оптичний) LC- LC Duplex MM OM4 15м	шт.	1	480	480
15	Патч-корд (оптичний) LC- LC Duplex MM OM3 30м	шт.	1	734	734
16	Мережевий адаптер 10G Dell Intel X520-DA2	шт.	1	6314	6314
17	Комутатор Cisco Catalyst 1200 24xGE, PoE, 4x10G	шт.	1	35000	35000
18	Комутатор Cisco Catalyst 1300 C1300-16P-4X	шт.	2	34700	69400
19	Маршрутизатор MikroTik RB5009UG+S+IN	шт.	1	11300	11300
20	Сервер Dell PowerEdge R660	шт.	1	286000	286000
21	Сервер PowerUp Rack 4U	шт.	1	58700	58700
22	Точка доступу Mikrotik hAP ax3	шт.	2	5800	11600
23	Принтер HP LaserJet Enterprise M507dn	шт.	1	41400	41400
Разом					567823,40

4.4 Розрахунок витрат на електроенергію

Витрати на споживання електричної енергії, що необхідна для забезпечення роботи комп'ютерної техніки під час проектування, визначаються за такою формулою:

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		79

$$Z_e = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Весь цикл розробки та впровадження архітектури комп'ютерної мережі здійснювався за допомогою одного робочого ноутбука. Обчислення вартості використаної ним електричної енергії базується на сумарній тривалості робочого процесу (згідно з раніше затвердженою табл. 4.1), яка становить 35 годин, та середній потужності зарядного пристрою комп'ютера – 0,5 кВт. Комерційний тариф на електроенергію складає 15,94 грн за кВт-год.

$$Z_e = 0,5 \cdot 35 \cdot 15,94 = 278,95 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати, що враховують доставку активного й пасивного мережевого обладнання, серверів, кабельної продукції та монтажних компонентів до об'єкта впровадження, прогнозуються у розмірі 8–10% від загальної суми розрахованих матеріальних затрат.

Обчислення логістичних та транспортних витрат здійснюється за формулою:

$$T_B = Z_{м.в.} \cdot 0,08 \dots 0,1, \quad (4.8)$$

де T_B – транспортні витрати.

$$T_B = 567823,40 \cdot 0,08 = 45425,87 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Амортизація – це процес поступового перенесення вартості основних фондів на вартість створеного продукту з метою їх подальшого повного відновлення. Комп'ютерна техніка належить до четвертої групи основних фондів із мінімально допустимим строком корисного використання 2 роки (24 місяці). Відповідно, місячна норма амортизації становить близько 4%.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		80

Оскільки обладнання використовується лише протягом періоду проектування, розрахунок амортизаційних відрахувань проводиться пропорційно відпрацьованим годинам за формулою:

$$A = \frac{B_B \cdot H_A}{100\%}, \quad (4.9)$$

де A – амортизаційні відрахування за звітний період, грн.;

B_B – балансова вартість групи основних фондів на початок звітного періоду, грн.;

H_A – норма амортизації, %.

$$A = 30000 \cdot 0,04 \cdot 35 / 150 = 280 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати включають витрати на загальне управління проектом, господарське обслуговування робочих місць, апаратно-програмне забезпечення та організацію належних і безпечних умов праці.

Залежно від організаційно-правової форми діяльності підприємства та його структури, величина накладних витрат прогнозується в межах від 20% до 60% від сумарного фонду оплати праці розробників:

$$H_B = V_{o.n.} \cdot 0,2 \dots 0,6, \quad (4.10)$$

де H_B – накладні витрати.

$$H_B = 21137 \cdot 0,2 = 4227,40 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Фінальним етапом економічного обґрунтування є формування загального кошторису витрат, який відображає сукупні витрати на розробку та впровадження проекту комп'ютерної мережі. Узагальнені результати всіх попередніх техніко-економічних обчислень систематизовано й наведено у таблиці 4.4.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		81

Таблиця 4.4 – Кошторис витрат на розробку проекту

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основна і додаткова заробітна плата)	21137	3,28
Відрахування на соціальні заходи (ЄСВ 22%)	4650,14	0,72
Матеріальні витрати	567823,40	88,15
Витрати на електроенергію	278,95	0,04
Транспортні витрати	45425,87	7,05
Амортизаційні відрахування	280	0,13
Накладні витрати	4227,40	0,66
Собівартість	643822,76	100

Собівартість (C_B) НДР розрахуємо за формулою:

$$C_B = B_{o.n.} + B_{c.z.} + Z_{m.v.} + Z_e + T_B + A + H_B \quad (4.11)$$

$$C_B = 21137 + 4650,14 + 567823,40 + 278,95 + 45425,87 + 280 + 4227,40 = 643822,76 \text{ грн.}$$

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = C_B \cdot (1 + P_{рен.}) \cdot (1 + ПДВ), \quad (4.12)$$

де $P_{рен.}$ – рівень рентабельності, 25 %;

$ПДВ$ – ставка податку на додану вартість, (20 %).

$$Ц = 643822,76 \cdot (1 + 0,25) \cdot (1 + 0,20) = 965734,14 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність впровадження проекту оцінюється за допомогою розрахунку чистої теперішньої вартості (ЧТВ) та терміну окупності інвестицій ($T_{ок}$).

Чиста теперішня вартість для трирічного життєвого циклу мережі ($t = 3$) обчислюється за формулою:

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		82

$$ЧТВ = -K_B + \sum_{i=1}^t \frac{\Gamma_{II}}{(1+i)^t} \quad (4.13)$$

де K_B – затрати на проєкт;

Γ_{II} – грошовий потік за t – ий рік;

t – відповідний рік проєкту;

i - величина дисконтної ставки (10...15%).

Якщо $ЧТВ \geq 0$, то проєкт може бути рекомендований до впровадження.

$$ЧТВ = -643822,76 + 589095,88/(1+0,1)^1 + 589095,88/(1+0,1)^2 + 589095,88/(1+0,1)^3 = 313875,65 \text{ грн.}$$

Термін окупності визначається за формулою:

$$T_{ок} = T_{ПВ} + \frac{H_B}{\Gamma_{ПР}} \quad (4.14)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років;

H_B – невідшкодовані витрати на початок року, грн.;

$\Gamma_{ПР}$ – грошовий потік на початок року, грн.

$$T_{ок} = 1 + 131565,47 / 589095,88 = 1,2 \text{ роки}$$

Всі дані розрахунків винесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 – Техніко-економічні показники проєкту

№ п/п	Показник	Значення
1	Собівартість, грн	643822,76
2	Плановий прибуток, грн.	321911,38
3	Ціна, грн.	965734,14
4	Чиста теперішня вартість, грн.	313875,65
5	Термін окупності, рік	1,2

На основі отриманих економічних показників можна зробити висновок, що при терміні окупності 1,2 року проведення робіт із розгортання та впровадження проєктованої мережі є повністю доцільним, високоефективним та економічно вигідним.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Аналіз небезпеки та заходи захисту від ураження електричним струмом при обслуговуванні апаратного забезпечення компанії "MidHub"

Обслуговування серверів, комутаторів та точок доступу компанії "MidHub" безпосередньо пов'язане з роботою електроустановок під напругою 220/380 В із частотою 50 Гц. Така напруга є небезпечною для життя людини і може спричинити важкі електротравми або летальний наслідок у разі недотримання правил безпеки.

Основними джерелами небезпеки при обслуговуванні мережевого обладнання є прямий дотик до відкритих струмоведучих частин під час ремонту або діагностики зі знятими захисними кришками. Серйозну загрозу також становить поява електричного потенціалу на металевих корпусах пристроїв та монтажних стійках при пошкодженні або пробіі ізоляції силового кабелю. При короткому замиканні або роз'єднанні навантажених ліній може виникнути електрична дуга, яка становить термічну небезпеку для персоналу. Додатково постійна робота систем охолодження призводить до накопичення статичної електрики, яка може спровокувати мимовільні рухи працівника та призвести до травмування.

За ступенем небезпеки серверні приміщення відносяться до приміщень без підвищеної небезпеки завдяки постійному кондиціонуванню повітря та відсутності пилу і вологи. Проте висока щільність металевого обладнання вимагає обов'язкового впровадження технічних заходів захисту. Усі корпуси серверів, комутаторів та монтажні стійки підключаються до загального контуру захисного заземлення будівлі з опором не більше 4 Ом [6]. У мережах із глухозаземленою нейтраллю застосовується захисне занулення, яке забезпечує миттєве вимкнення автоматичного вимикача при виникненні короткого замикання. На лініях живлення встановлюються пристрої захисного відключення, які при виявленні струму витоку понад 30 мА автоматично

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		84

знеструмлюють лінію за частки секунди. Для додаткового захисту використовуються силові кабелі з подвійною ізоляцією, а внутрішні шини розподілу живлення в шафах закриваються захисними діелектричними панелями.

Організаційні заходи безпеки регламентують порядок виконання всіх робіт в інфраструктурі. До самостійного обслуговування обладнання допускається лише персонал із кваліфікаційною групою з електробезпеки не нижче третьої. Група з електробезпеки (“кваліфікаційна група“, “група допуску“) дає дозвіл персоналу компанії до виконання робіт в електроустановках, а також свідчить про рівень його підготовки. Некваліфікований працівник – це завжди ризик. Штрафи при перевірці, нещасні випадки, псування дорогого устаткування, збій роботи всього підприємства, неможливість впровадження нових технологій [8]. Роботи з заміни внутрішніх модулів, чистки або монтажу виконуються виключно на повністю знеструмленому обладнанні, а на відповідний автоматичний вимикач вивіщується заборонний плакат. Перед початком роботи обов'язково перевіряється відсутність напруги за допомогою мультиметра. У випадках коли діагностика виконується під напругою, використовуються діелектричні рукавички, гумові килимки та інструмент з ізольованими ручками. Для захисту чутливих мікросхем від статичного розряду інженер працює в антистатичному браслеті, підключеному до контуру заземлення стійки.

5.2 Організація ефективних систем вентиляції та кондиціонування в серверних приміщеннях

Серверне приміщення компанії "MidHub" є зосередженням активного мережевого обладнання – серверів, комутаторів та маршрутизатора, які в процесі роботи виділяють значну кількість теплової енергії. Перегрів обладнання є однією з найпоширеніших причин відмов і скорочення терміну служби електронних компонентів, тому організація ефективної системи вентиляції та кондиціонування є обов'язковою умовою надійної роботи інфраструктури.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докцм.	Підпис	Дата		85

Основною вимогою до мікроклімату серверного приміщення є підтримання стабільної температури в діапазоні від 18 до 27 градусів Цельсія та відносної вологості повітря від 40 до 60 відсотків [6]. Відхилення від цих параметрів негативно впливає на роботу обладнання – підвищена температура прискорює деградацію електронних компонентів, а надмірна вологість може спричинити конденсацію на платах і коротке замикання.

Для забезпечення належного температурного режиму в серверному приміщенні застосовується прецизійне кондиціонування, яке на відміну від побутових кондиціонерів підтримує задані параметри цілодобово та контролює не лише температуру, але й вологість повітря. Система вентиляції організовується за принципом холодного та гарячого коридорів – стійки з обладнанням розміщуються таким чином, щоб холодне повітря подавалося спереду стійок, а гаряче відводилося ззаду. Це унеможливорює змішування холодного та нагрітого повітря і суттєво підвищує ефективність охолодження.

Повітряні потоки в приміщенні організовуються з урахуванням розташування обладнання – припливні отвори розміщуються з боку холодного коридору, витяжні – з боку гарячого. Для рівномірного розподілу холодного повітря під стійками використовуються перфоровані підлогові плити. Кабельні прорізи та технологічні отвори в підлозі герметизуються для запобігання прориву холодного повітря в обхід обладнання.

Для своєчасного виявлення відхилень від допустимих параметрів у серверному приміщенні встановлюються датчики температури та вологості, показники яких відображаються в системі моніторингу. При перевищенні порогових значень система автоматично формує сповіщення для адміністратора. Резервування системи кондиціонування забезпечується встановленням додаткового резервного кондиціонера, який автоматично вмикається у разі відмови основного, що гарантує безперервну роботу обладнання навіть під час технічного обслуговування основної системи охолодження [6].

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ докum.</i>	<i>Підпис</i>	<i>Дата</i>		86

5.3 Нормативне забезпечення та планування профілактичних протипожежних заходів на в компанії "MidHub"

Забезпечення пожежної безпеки є невід'ємною складовою охорони праці та захисту майна компанії "MidHub". Основним нормативним документом у цій сфері є Закон України "Про пожежну безпеку", який встановлює правові та організаційні засади забезпечення пожежної безпеки на підприємствах. Відповідно до його вимог керівник підприємства несе повну відповідальність за стан пожежної безпеки на об'єкті та зобов'язаний забезпечити виконання всіх профілактичних заходів.

Серверне приміщення компанії відноситься до категорії приміщень з підвищеною пожежною небезпекою через значну концентрацію електронного обладнання, та кабельних трас [2]. Основними причинами виникнення пожеж в таких приміщеннях є коротке замикання в електричних мережах, перевантаження кабелів, несправність обладнання та займання ізоляції. Для мінімізації цих ризиків необхідно дотримуватись вимог НАПБ А.01.001-2014 "Правила пожежної безпеки в Україні".

Профілактичні протипожежні заходи у компанії "MidHub" поділяються на організаційні та технічні. До організаційних належать розробка та затвердження інструкцій з пожежної безпеки, проведення інструктажів з персоналом, визначення відповідальних осіб за пожежну безпеку в кожному приміщенні, розробка планів евакуації та регулярне проведення навчальних евакуацій [11]. Кожен працівник компанії повинен знати розташування первинних засобів пожежогасіння, шляхи евакуації та порядок дій у разі виникнення пожежі.

До технічних заходів відноситься оснащення серверного приміщення системою автоматичної пожежної сигналізації відповідно до вимог ДБН В.2.5-56, встановлення газових вогнегасників, які не пошкоджують електронне обладнання при гасінні. Використання водяних або порошкових вогнегасників у серверних приміщеннях забороняється. На всіх поверхах будівлі встановлюються порошкові або вуглекислотні вогнегасники з розрахунку

						2026.КВР.123.406.11.00.00 ПЗ	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата			87

відповідно до чинних норм. Електрична мережа захищається автоматичними вимикачами та пристроями захисного відключення для запобігання виникненню пожежі внаслідок перевантаження або короткого замикання.

Шляхи евакуації повинні бути вільними, позначеними відповідними знаками та обладнаними аварійним освітленням. Двері евакуаційних виходів мають відчинятися у напрямку виходу з будівлі та не замикатися на ключ під час перебування людей у приміщеннях. Ширина евакуаційних коридорів та дверей визначається відповідно до розрахункової кількості людей.

Планові перевірки стану пожежної безпеки проводяться не рідше одного разу на квартал відповідальною особою з пожежної безпеки з обов'язковим складанням акту перевірки. За результатами перевірок виявлені порушення усуваються у встановлені терміни. Первинні засоби пожежогасіння проходять технічне обслуговування відповідно до вимог виробника та замінюються після закінчення терміну придатності.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ докцм.</i>	<i>Підпис</i>	<i>Дата</i>		88

ВИСНОВКИ

У кваліфікаційній роботі розроблено проєктну документацію на впровадження комп'ютерної мережі ІТ-компанії "MidHub".

Перший розділ присвячено розробці технічного завдання, де проаналізовано організаційну структуру підприємства, схему розміщення техніки та ключові комунікаційні потреби персоналу.

У другому розділі обґрунтовано вибір комбінованої топології та логічну сегментацію інфраструктури за допомогою технології IEEE 802.1Q VLAN. Як середовище передачі даних специфіковано кабель UTP CAT6 із монтажем у настінних пластикових коробах. Технічне рішення базується на комутаторах доступу Cisco Catalyst C1300-16P-4X, комутаторі ядра Catalyst C1200-24P-4X та бездротових точках доступу MikroTik hAP ax3. Роль операційної системи для сервера S_1 виконує Ubuntu Server, а для сервера S_2 – Windows Server.

Третій розділ містить практичні інструкції з конфігурування комутаційного обладнання, налаштування профільних серверних служб, а також методику тестування та моніторингу працездатності мережі.

Графічна частина роботи представлена на окремих плакатах і включає план приміщень, логічну та фізичну топології, таблицю IP-адресації та схему техніко-економічних показників.

В економічному розділі проведено розрахунок собівартості робіт із проєктування, монтажу кабельної інфраструктури та запуску всієї мережі в експлуатацію, завдяки чому визначено термін окупності проєкту 1,2 року. Це підтверджує доцільність його реалізації та економічну ефективність.

П'ятий розділ повністю присвячено питанням охорони праці: забезпеченню електробезпеки при роботі з обладнанням, організації систем вентиляції та кондиціонування в серверних приміщеннях для підтримки мікроклімату, а також комплексним протипожежним заходах.

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ док.м.</i>	<i>Підпис</i>	<i>Дата</i>		89

ПЕРЕЛІК ПОСИЛАНЬ

1. Бочкарьов О. Ю. Системне програмування в ОС Linux : навч. посібник. Львів : Видавець ФОП Марченко Т.В., 2026. 229 с.
2. Грибан В. Г., Фоменко А. Є., Казначеев Д. Г. Безпека життєдіяльності та охорона праці : підручник. Дніпро : ДДУВС, 2022. 388 с.
3. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 1 : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 328 с.
4. Карпенко М. Ю., Макогон Н. В. Комп'ютерні мережі : конспект лекцій. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 100 с.
5. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок, А. О. Аносов, В. В. Семко та ін. Київ : Київський університет імені Бориса Грінченка, 2019. 218 с.
6. Вимоги до інженерної інфраструктури серверних : наказ ДСНС від 23.10.2019 № 608. URL: <https://dsns.gov.ua/upload/1/9/2/3/4/2019-10-25-3-vimogi.pdf> (дата звернення: 08.06.2026).
7. Все, що потрібно знати про виту пару. DEPS : веб-сайт. URL: <https://deps.ua/ua/knowegable-base/reference-information/9634.html> (дата звернення: 09.05.2026).
8. Допуски з електробезпеки. ЕУЦ Сфера : веб-сайт. URL: <https://evcsfera.com/dopuski-z-elektrobezpeki> (дата звернення: 08.06.2026).
9. Комп'ютерна мережа. Вікіпедія : вільна енциклопедія : веб-сайт. URL: https://uk.wikipedia.org/wiki/Комп'ютерна_мережа (дата звернення: 10.04.2026).
10. Комутатор Cisco Catalyst C1300-16P-4X. Cisco : веб-сайт. URL: <https://xn-h1aemkx.com.ua/switch/cisco-catalyst-1300-series/c1300-16p-4x> (дата звернення: 21.05.2026).
11. Пожежогасіння серверних і ЦОД. Brandmaster Systems : веб-сайт. URL: <https://brandmaster.systems/novyny/pozhezhohasinnia-servernykh-i-tsentriv-obrobky-danykh-tsodiv> (дата звернення: 08.06.2026).

										Арк.
										90
Змн.	Арк.	№ докum.	Підпис	Дата	2026.КВР.123.406.11.00.00 ПЗ					

12. Пояснення мережевої топології: типи, структури та як вибрати правильну. GlobalYo : веб-сайт. URL: <https://www.globalyo.com/uk/blog/exploring-the-different-types-of-network-topology-a-comprehensive-guide/> (дата звернення: 09.05.2026).

13. Різниця між апаратним та програмним забезпеченням. Guru99 : веб-сайт. URL: <https://www.guru99.com/uk/hardware-vs-software-difference.html> (дата звернення: 06.05.2026).

14. Робота в IT. DOU : веб-сайт. URL: <https://jobs.dou.ua/> (дата звернення: 08.06.2026).

15. Система створення комп'ютерних мереж: основні етапи і рекомендації. InfoPard : веб-сайт. URL: <https://infopard.com/systema-stvorennya-kompyuternyh-merezh-osnovni-etapy-i-rekomendacziyi/> (дата звернення: 09.05.2026).

16. Cisco Catalyst 1200 Series Switches Data Sheet. Cisco : веб-сайт. URL: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1200-series-switches/nb-06-cat1200-ser-data-sheet-cte-en.html> (дата звернення: 21.05.2026).

17. Cisco Catalyst 1300 Series Switches Support. Cisco : веб-сайт. URL: <https://www.cisco.com/c/en/us/support/switches/catalyst-1300-series-switches/series.html> (дата звернення: 02.06.2026).

18. Filter. MikroTik Documentation : веб-сайт. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/48660574/Filter> (дата звернення: 03.06.2026).

19. NTB - RouterOS. MikroTik Documentation : веб-сайт. URL: <https://help.mikrotik.com/docs/display/ROS/Queues> (дата звернення: 04.06.2026).

20. OSPF. MikroTik Documentation : веб-сайт. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/9863229/OSPF> (дата звернення: 03.06.2026).

21. SmbShare Module. Microsoft Learn : веб-сайт. URL: <https://learn.microsoft.com/en-us/powershell/module/smbshare/> (дата звернення: 02.06.2026).

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		91

22. TIA/EIA-568-B.1-2001. Commercial Building Telecommunications Cabling Standard. Part 1: General Requirements. Arlington : Telecommunications Industry Association, 2001. 94 с.

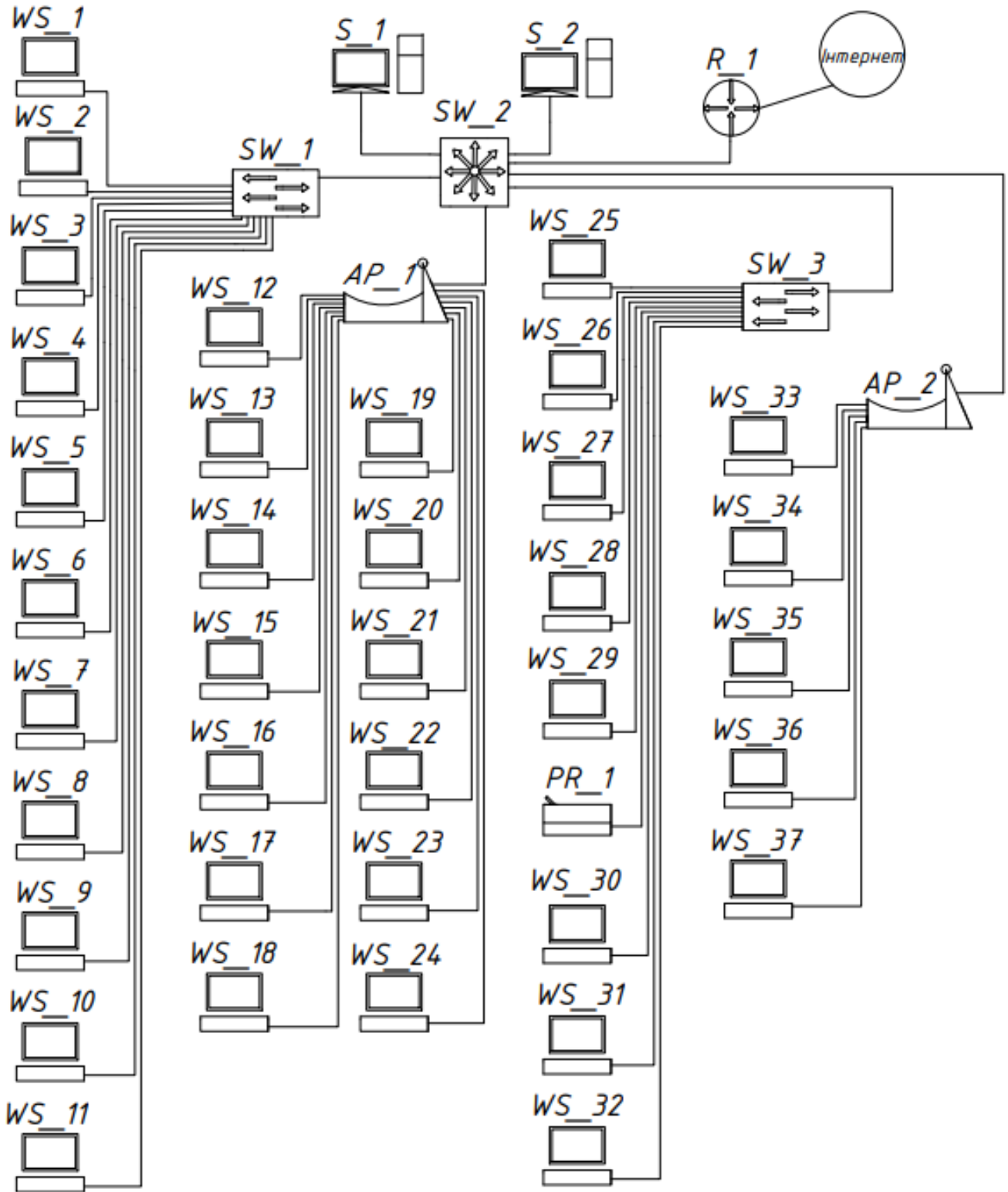
23. VLAN. MikroTik Documentation : веб-сайт. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/88014957/VLAN> (дата звернення: 03.06.2026).

24. Windows Server 2022 and Windows 11 PowerShell modules. Microsoft Learn : веб-сайт. URL: <https://learn.microsoft.com/en-us/powershell/windows/get-started> (дата звернення: 1.06.2026).

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		92

ДОДАТКИ

Додаток А. Схема логічної топології мережі компанії "MidHub"



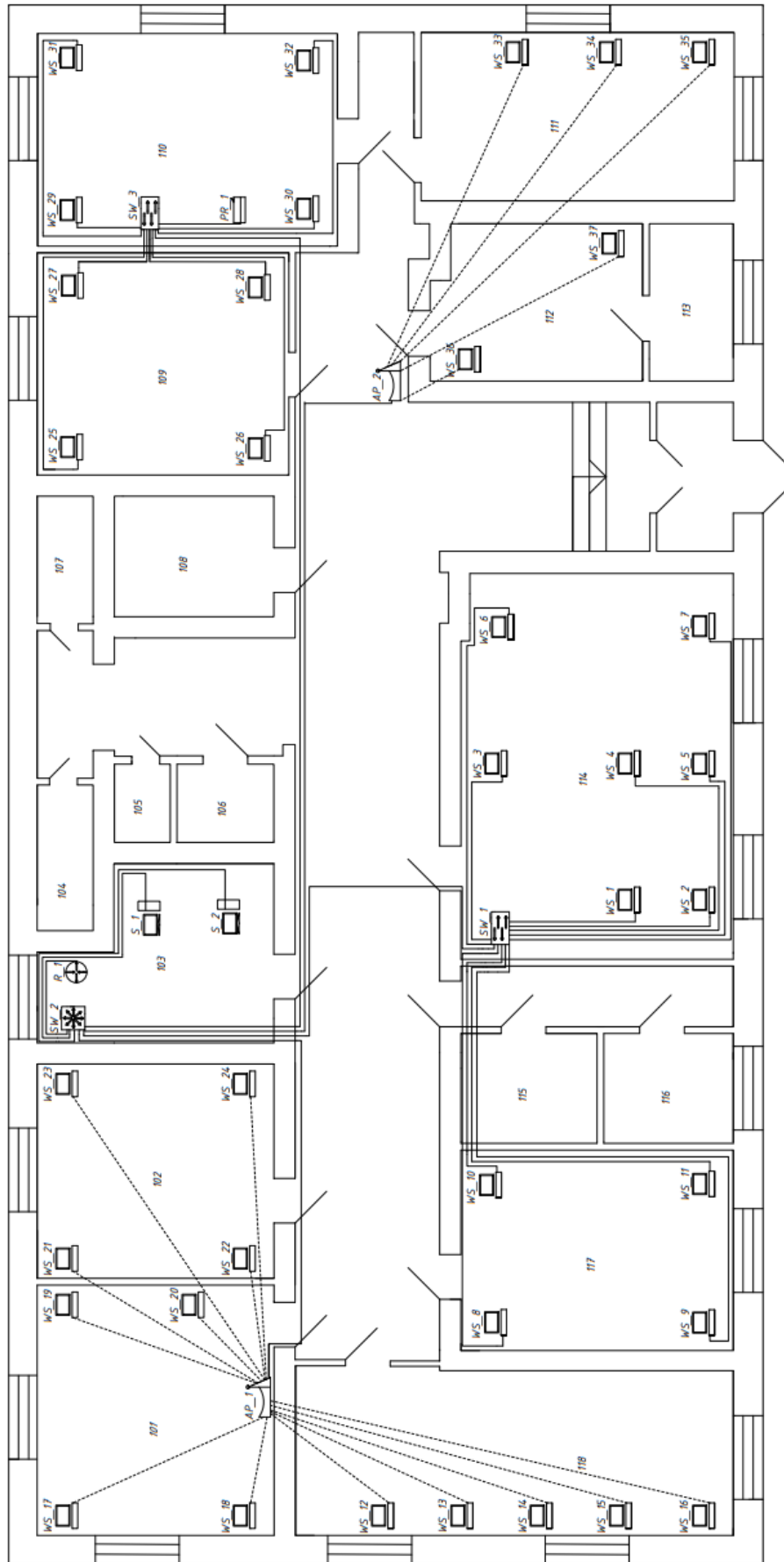
Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

93

Додаток Б. Схема фізичної топології мережі компанії "MidHub"



Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Додаток В. Лістинг конфігурації комутатора SW_1

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW_1
# Налаштування паролів доступу
SW_1(config)# enable secret StrongPass_Enable
SW_1(config)# line console 0
SW_1(config-line)# password StrongPass_Console
SW_1(config-line)# login
SW_1(config-line)# exit
# Створюємо необхідні віртуальні мережі
SW_1(config)# vlan 10
SW_1(config-vlan)# name Dev_Wired
SW_1(config-vlan)# exit
SW_1(config)# vlan 50
SW_1(config-vlan)# name Infrastructure
SW_1(config-vlan)# exit
# Інтерфейс керування у VLAN 50
SW_1(config)# interface vlan 50
SW_1(config-if)# ip address 192.168.50.3 255.255.255.0
SW_1(config-if)# no shutdown
SW_1(config-if)# exit
SW_1(config)# ip default-gateway 192.168.50.1
# Налаштування SSH
SW_1(config)# ip domain-name office.local
SW_1(config)# crypto key generate rsa modulus 2048
SW_1(config)# ip ssh version 2
SW_1(config)# line vty 0 4
SW_1(config-line)# transport input ssh
```

					2026.КВР.123.406.11.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		95

```

SW_1(config-line)# password StrongPass_SW1
SW_1(config-line)# login
SW_1(config-line)# exit
# Оптичний SFP+ аплінк до SW_2
SW_1(config)# interface TenGigabitEthernet1/0/1
SW_1(config-if)# switchport mode trunk
SW_1(config-if)# switchport trunk allowed vlan 10,50
SW_1(config-if)# no shutdown
SW_1(config-if)# exit
# Access порти для робочих станцій WS_1-WS_11
SW_1(config)# interface range gigabitEthernet1/0/2-12
SW_1(config-if-range)# switchport mode access
SW_1(config-if-range)# switchport access vlan 10
SW_1(config-if-range)# spanning-tree portfast
SW_1(config-if-range)# switchport port-security
SW_1(config-if-range)# switchport port-security maximum 1
SW_1(config-if-range)# switchport port-security violation restrict
SW_1(config-if-range)# no shutdown
SW_1(config-if-range)# exit
# Вимкнення невикористаних портів
SW_1(config)# interface range gigabitEthernet1/0/1
SW_1(config-if)# shutdown
SW_1(config-if)# exit
SW_1(config)# interface range gigabitEthernet1/0/13-24
SW_1(config-if-range)# shutdown
SW_1(config-if-range)# exit
SW_1(config)# end
SW_1# write memory

```

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

96

Додаток Г. Лістинг конфігурації комутатора SW_3

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW_3
# Налаштування паролів доступу
SW_3(config)# enable secret StrongPass_Enable
SW_3(config)# line console 0
SW_3(config-line)# password StrongPass_Console
SW_3(config-line)# login
SW_3(config-line)# exit
# Створюємо необхідні віртуальні мережі
SW_3(config)# vlan 30
SW_3(config-vlan)# name Management
SW_3(config-vlan)# exit
SW_3(config)# vlan 50
SW_3(config-vlan)# name Infrastructure
SW_3(config-vlan)# exit
# Інтерфейс керування у VLAN 50
SW_3(config)# interface vlan 50
SW_3(config-if)# ip address 192.168.50.4 255.255.255.0
SW_3(config-if)# no shutdown
SW_3(config-if)# exit
SW_3(config)# ip default-gateway 192.168.50.1
# Налаштування SSH
SW_3(config)# ip domain-name office.local
SW_3(config)# crypto key generate rsa modulus 2048
SW_3(config)# ip ssh version 2
SW_3(config)# line vty 0 4
SW_3(config-line)# transport input ssh
```

					2026.КВР.123.406.11.00.00 ПЗ	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		97

```

SW_3(config-line)# password StrongPass_SW3
SW_3(config-line)# login
SW_3(config-line)# exit
# Оптичний SFP+ аплінк до SW_2
SW_3(config)# interface TenGigabitEthernet1/0/1
SW_3(config-if)# switchport mode trunk
SW_3(config-if)# switchport trunk allowed vlan 30,50
SW_3(config-if)# no shutdown
SW_3(config-if)# exit
# Access порти для робочих станцій WS_25-WS_32
SW_3(config)# interface range gigabitEthernet1/0/2-9
SW_3(config-if-range)# switchport mode access
SW_3(config-if-range)# switchport access vlan 30
SW_3(config-if-range)# spanning-tree portfast
SW_3(config-if-range)# switchport port-security
SW_3(config-if-range)# switchport port-security maximum 1
SW_3(config-if-range)# switchport port-security violation restrict
SW_3(config-if-range)# no shutdown
SW_3(config-if-range)# exit
# Порт для принтера PR_1
SW_3(config)# interface gigabitEthernet1/0/10
SW_3(config-if)# switchport mode access
SW_3(config-if)# switchport access vlan 30
SW_3(config-if)# spanning-tree portfast
SW_3(config-if)# switchport port-security
SW_3(config-if)# switchport port-security maximum 1
SW_3(config-if)# switchport port-security violation restrict
SW_3(config-if)# no shutdown
SW_3(config-if)# exit
# Вимкнення невикористаних портів

```

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		98

```
SW_3(config)# interface gigabitEthernet1/0/1
SW_3(config-if)# shutdown
SW_3(config-if)# exit
SW_3(config)# interface range gigabitEthernet1/0/11-24
SW_3(config-if-range)# shutdown
SW_3(config-if-range)# exit
SW_3(config)# end
SW_3# write memory
```

						Арк.
						99
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	<i>2026.КВР.123.406.11.00.00 ПЗ</i>	

Додаток Д. Лістинг конфігурації комутатора SW_2

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW_2
# Налаштування паролів доступу
SW_2(config)# enable secret StrongPass_Enable
SW_2(config)# line console 0
SW_2(config-line)# password StrongPass_Console
SW_2(config-line)# login
SW_2(config-line)# exit
# Створюємо базу даних віртуальних мереж
SW_2(config)# vlan 10
SW_2(config-vlan)# name Dev_Wired
SW_2(config-vlan)# exit
SW_2(config)# vlan 20
SW_2(config-vlan)# name QA_Dev_WiFi
SW_2(config-vlan)# exit
SW_2(config)# vlan 30
SW_2(config-vlan)# name Management
SW_2(config-vlan)# exit
SW_2(config)# vlan 40
SW_2(config-vlan)# name Staff_WiFi
SW_2(config-vlan)# exit
SW_2(config)# vlan 50
SW_2(config-vlan)# name Infrastructure
SW_2(config-vlan)# exit
# Інтерфейс керування у VLAN 50
SW_2(config)# interface vlan 50
SW_2(config-if)# ip address 192.168.50.2 255.255.255.0
SW_2(config-if)# no shutdown
```

					2026.КВР.123.406.11.00.00 ПЗ	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		100

```

SW_2(config-if)# exit
SW_2(config)# ip default-gateway 192.168.50.1
# Налаштування SSH
SW_2(config)# ip domain-name office.local
SW_2(config)# crypto key generate rsa modulus 2048
SW_2(config)# ip ssh version 2
SW_2(config)# line vty 0 4
SW_2(config-line)# transport input ssh
SW_2(config-line)# password StrongPass_SW2
SW_2(config-line)# login
SW_2(config-line)# exit
# SFP+ порт Te1/0/17 до SW_1
SW_2(config)# interface TenGigabitEthernet1/0/17
SW_2(config-if)# switchport mode trunk
SW_2(config-if)# switchport trunk allowed vlan 10,50
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# SFP+ порт Te1/0/18 до SW_3
SW_2(config)# interface TenGigabitEthernet1/0/18
SW_2(config-if)# switchport mode trunk
SW_2(config-if)# switchport trunk allowed vlan 30,50
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# SFP+ порт Te1/0/19 до сервера S_1
SW_2(config)# interface TenGigabitEthernet1/0/19
SW_2(config-if)# switchport mode access
SW_2(config-if)# switchport access vlan 50
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# SFP+ порт Te1/0/20 до маршрутизатора R_1

```

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		101

```

SW_2(config)# interface TenGigabitEthernet1/0/20
SW_2(config-if)# description TRUNK_TO_ROUTER_R1
SW_2(config-if)# switchport mode trunk
SW_2(config-if)# switchport trunk allowed vlan 10,20,30,40,50
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# Access порт для AP_1 VLAN 20 (PoE)
SW_2(config)# interface gigabitEthernet1/0/1
SW_2(config-if)# switchport mode access
SW_2(config-if)# switchport access vlan 20
SW_2(config-if)# spanning-tree portfast
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# Access порт для AP_2 VLAN 40 (PoE)
SW_2(config)# interface gigabitEthernet1/0/2
SW_2(config-if)# switchport mode access
SW_2(config-if)# switchport access vlan 40
SW_2(config-if)# spanning-tree portfast
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# Access порт для сервера S_2
SW_2(config)# interface gigabitEthernet1/0/3
SW_2(config-if)# switchport mode access
SW_2(config-if)# switchport access vlan 50
SW_2(config-if)# no shutdown
SW_2(config-if)# exit
# Вимкнення невикористаних мідних інтерфейсів
SW_2(config)# interface range gigabitEthernet1/0/4-16
SW_2(config-if-range)# shutdown
SW_2(config-if-range)# exit
SW_2(config)# end
SW_2# write memory

```

Змн.	Арк.	№ докум.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Додаток Е. Лістинг конфігурації маршрутизатора R_1

```
# Налаштування імені пристрою
/system identity set name=R_1

# Створення віртуальних VLAN-інтерфейсів на оптичному порту sfr-
sfpplus1

/interface vlan add name=vlan10-dev vlan-id=10 interface=sfr-sfpplus1
/interface vlan add name=vlan20-qa vlan-id=20 interface=sfr-sfpplus1
/interface vlan add name=vlan30-mgmt vlan-id=30 interface=sfr-sfpplus1
/interface vlan add name=vlan40-staff vlan-id=40 interface=sfr-sfpplus1
/interface vlan add name=vlan50-infra vlan-id=50 interface=sfr-sfpplus1

# Призначення IP-адрес шлюзів для кожного VLAN

/ip address add address=192.168.10.1/24 interface=vlan10-dev
comment="Gateway VLAN10 DevOps"

/ip address add address=192.168.20.1/24 interface=vlan20-qa
comment="Gateway VLAN20 QA"

/ip address add address=192.168.30.1/24 interface=vlan30-mgmt
comment="Gateway VLAN30 Management"

/ip address add address=192.168.40.1/24 interface=vlan40-staff
comment="Gateway VLAN40 Staff"

/ip address add address=192.168.50.1/24 interface=vlan50-infra
comment="Gateway VLAN50 Infrastructure"

# Статичний маршрут до Інтернету через провайдера

/ip route add dst-address=0.0.0.0/0 gateway=195.24.22.1 comment="Статичний
шлюз до Інтернету"

# Налаштування DNS-серверів

/ip dns set servers=8.8.8.8,8.8.4.4 allow-remote-requests=yes

# Налаштування протоколу динамічної маршрутизації OSPF v2
# (налаштовано на перспективу масштабування мережі)

/routing ospf instance add name=OSPF_Core router-id=192.168.50.1 version=2
```

Змн.	Арк.	№ докum.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

103

```

/routing ospf area add name=Backbone_Area instance=OSPF_Core area-
id=0.0.0.0

/routing ospf interface-template add area=Backbone_Area
networks=192.168.10.0/24,192.168.20.0/24,192.168.30.0/24,192.168.40.0/24,192.16
8.50.0/24 type=ptp

# Налаштування NAT на зовнішньому інтерфейсі
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
comment="NAT for Office"

# Правила фільтрації брандмауера
/ip firewall filter add chain=forward connection-state=established,related
action=accept comment="ACL_1: Дозвіл перевіреного трафіку"

/ip firewall filter add chain=forward src-address=192.168.40.0/24 dst-
address=192.168.30.0/24 action=drop comment="ACL_2: Ізоляція Staff_WiFi від
Management"

/ip firewall filter add chain=forward src-address=192.168.20.0/24 dst-
address=192.168.30.0/24 action=drop comment="ACL_3: Ізоляція QA_WiFi від
Management"

/ip firewall filter add chain=forward src-address=192.168.40.0/24 dst-
address=192.168.50.0/24 action=drop comment="ACL_4: Захист інфраструктури
серверів"

/ip firewall filter add chain=forward connection-state=invalid action=drop
comment="ACL_5: Блокування пошкоджених пакетів"

# Маркування трафіку для НТВ черг (Upload та Download)
/ip firewall mangle add chain=forward src-address=192.168.10.0/24
action=mark-packet new-packet-mark=vlan10 passthrough=no comment="VLAN10
Upload"

/ip firewall mangle add chain=forward dst-address=192.168.10.0/24
action=mark-packet new-packet-mark=vlan10 passthrough=no comment="VLAN10
Download"

```

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		104

```
/ip firewall mangle add chain=forward src-address=192.168.20.0/24
action=mark-packet new-packet-mark=vlan20 passthrough=no comment="VLAN20
Upload"
```

```
/ip firewall mangle add chain=forward dst-address=192.168.20.0/24
action=mark-packet new-packet-mark=vlan20 passthrough=no comment="VLAN20
Download"
```

```
/ip firewall mangle add chain=forward src-address=192.168.30.0/24
action=mark-packet new-packet-mark=vlan30 passthrough=no comment="VLAN30
Upload"
```

```
/ip firewall mangle add chain=forward dst-address=192.168.30.0/24
action=mark-packet new-packet-mark=vlan30 passthrough=no comment="VLAN30
Download"
```

```
/ip firewall mangle add chain=forward src-address=192.168.40.0/24
action=mark-packet new-packet-mark=vlan40 passthrough=no comment="VLAN40
Upload"
```

```
/ip firewall mangle add chain=forward dst-address=192.168.40.0/24
action=mark-packet new-packet-mark=vlan40 passthrough=no comment="VLAN40
Download"
```

```
/ip firewall mangle add chain=forward src-address=192.168.50.0/24
action=mark-packet new-packet-mark=vlan50 passthrough=no comment="VLAN50
Upload"
```

```
/ip firewall mangle add chain=forward dst-address=192.168.50.0/24
action=mark-packet new-packet-mark=vlan50 passthrough=no comment="VLAN50
Download"
```

НТВ черги управління пропускною здатністю

```
/queue tree add name=VLAN10-Dev parent=global packet-mark=vlan10 max-
limit=300M comment="DevOps"
```

```
/queue tree add name=VLAN20-QA parent=global packet-mark=vlan20 max-
limit=250M comment="QA WiFi"
```

					<i>2026.KBP.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ док.м.	Підпис	Дата		105

/queue tree add name=VLAN30-Mgmt parent=global packet-mark=vlan30 max-limit=150M comment="Management"

/queue tree add name=VLAN40-Staff parent=global packet-mark=vlan40 max-limit=100M comment="Staff"

/queue tree add name=VLAN50-Infra parent=global packet-mark=vlan50 max-limit=500M comment="Servers"

					<i>2026.KBP.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		106

Додаток Є. Лістинг конфігурації точки доступу AP_1

```
# Налаштування імені пристрою
/system identity set name=AP_1

# Регуляторні параметри радіочастот під стандарти України
/interface wifi channel
add name=ch-2.4g band=2.4ghz-ax width=20mhz skip-dfs-channels=all
add name=ch-5g band=5ghz-ax width=20/40/80mhz skip-dfs-channels=all

# Налаштування профілю безпеки з шифруванням WPA2/WPA3
/interface wifi security
add name=sec-qa passphrase="QA_SuperPassword2026" authentication-
types=wpa2-psk,wpa3-psk

# Створення конфігурації бездротової мережі (SSID)
/interface wifi configuration
add name=cfg-qa ssid="Company_QA_WiFi" security=sec-qa mode=ap
channel=ch-5g country=Ukraine

# Активація радіомодулів 5 ГГц та 2.4 ГГц з прив'язкою до VLAN 20
/interface wifi set [ find default-name=wifi1 ] configuration=cfg-qa disabled=no
channel=ch-5g

/interface wifi set [ find default-name=wifi2 ] configuration=cfg-qa disabled=no
channel=ch-2.4g datapath.vlan-id=20

# Активація мосту з функцією фільтрації VLAN-тегів
/interface bridge add name=bridge-lan vlan-filtering=yes

# Додавання фізичного порту ether1 та радіоінтерфейсів до мосту
/interface bridge port
add bridge=bridge-lan interface=ether1
add bridge=bridge-lan interface=wifi1 pvid=20
add bridge=bridge-lan interface=wifi2 pvid=20

# Конфігурування таблиці комутації VLAN всередині мосту
/interface bridge vlan
```

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		107

```
add bridge=bridge-lan tagged=ether1,bridge-lan vlan-ids=50
add bridge=bridge-lan tagged=ether1 untagged=wifi1,wifi2 vlan-ids=20
# Створення субінтерфейсу управління в інфраструктурній мережі
/interface vlan add name=vlan50-mgmt vlan-id=50 interface=bridge-lan
# Призначення IP-адреси та маршруту за замовчуванням
/ip address add address=192.168.50.5/24 interface=vlan50-mgmt
/ip route add dst-address=0.0.0.0/0 gateway=192.168.50.1
/ip dns set servers=192.168.50.1
# Закриття вразливих системних служб
/ip service set telnet disabled=yes
/ip service set ftp disabled=yes
/ip service set www disabled=yes
/ip service set api disabled=yes
/ip service set api-ssl disabled=yes
# Синхронізація системного часу
/system ntp client set enabled=yes
/system ntp client servers add address=ua.pool.ntp.org
# Брандмауер: обмеження доступу до керування пристроєм
/ip firewall filter
add chain=input connection-state=established,related action=accept
comment="Дозвіл встановлених сесій"
add chain=input src-address=192.168.50.0/24 action=accept comment="Дозвіл
адміністрування тільки з VLAN 50"
add chain=input action=drop comment="Блокування сторонніх запитів до
пристрою"
```

Змн.	Арк.	№ докum.	Підпис	Дата

2026.КВР.123.406.11.00.00 ПЗ

Арк.

108

Додаток Ж. Лістинг конфігурації точки доступу AP_2

```
# Налаштування імені пристрою
/system identity set name=AP_2

# Регуляторні параметри радіочастот під стандарти України
/interface wifi channel
add name=ch-2.4g band=2.4ghz-ax width=20mhz skip-dfs-channels=all
add name=ch-5g band=5ghz-ax width=20/40/80mhz skip-dfs-channels=all

# Налаштування профілю безпеки з шифруванням WPA2/WPA3
/interface wifi security
add name=sec-staff passphrase="Staff_Password2026" authentication-
types=wpa2-psk,wpa3-psk

# Створення конфігурації бездротової мережі (SSID)
/interface wifi configuration
add name=cfg-staff ssid="Company_Staff_WiFi" security=sec-staff mode=ap
channel=ch-5g country=Ukraine

# Активація радіомодулів 5 ГГц та 2.4 ГГц з прив'язкою до VLAN 40
/interface wifi set [ find default-name=wifi1 ] configuration=cfg-staff disabled=no
channel=ch-5g

/interface wifi set [ find default-name=wifi2 ] configuration=cfg-staff disabled=no
channel=ch-2.4g datapath.vlan-id=40

# Активація мосту з функцією фільтрації VLAN-тегів
/interface bridge add name=bridge-lan vlan-filtering=yes

# Додавання фізичного порту ether1 та радіоінтерфейсів до мосту
/interface bridge port
add bridge=bridge-lan interface=ether1
add bridge=bridge-lan interface=wifi1 pvid=40
add bridge=bridge-lan interface=wifi2 pvid=40

# Конфігурування таблиці комутації VLAN всередині мосту
/interface bridge vlan
```

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докum.	Підпис	Дата		109

```
add bridge=bridge-lan tagged=ether1,bridge-lan vlan-ids=50
add bridge=bridge-lan tagged=ether1 untagged=wifi1,wifi2 vlan-ids=4
# Створення віртуального інтерфейсу управління в інфраструктурній мережі
/interface vlan add name=vlan50-mgmt vlan-id=50 interface=bridge-lan
# Призначення IP-адреси та маршруту за замовчуванням
/ip address add address=192.168.50.6/24 interface=vlan50-mgmt
/ip route add dst-address=0.0.0.0/0 gateway=192.168.50.1
/ip dns set servers=192.168.50.1
# Закриття вразливих системних служб
/ip service set telnet disabled=yes
/ip service set ftp disabled=yes
/ip service set www disabled=yes
/ip service set api disabled=yes
/ip service set api-ssl disabled=yes
# Синхронізація системного часу
/system ntp client set enabled=yes
/system ntp client servers add address=ua.pool.ntp.org
# Брандмауер: обмеження доступу до керування пристроєм
/ip firewall filter
add chain=input connection-state=established,related action=accept
add chain=input src-address=192.168.50.0/24 action=accept
add chain=input action=drop
```

					<i>2026.КВР.123.406.11.00.00 ПЗ</i>	Арк.
<i>Змн.</i>	<i>Арк.</i>	<i>№ док.м.</i>	<i>Підпис</i>	<i>Дата</i>		110