

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)

ПОЯСНОВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

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

Виконав: студент IV курсу, групи КІ-406

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

_____ Володимир КУРИЛО

(ім'я та прізвище)

Керівник _____ Андрій ЮЗЬКІВ

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

АНОТАЦІЯ

Курило В.О. Проектування комп'ютерної мережі компанії «WebTop»: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра за спеціальністю 123 «Комп'ютерна інженерія». – Тернопіль: ВСП «ТФК ТНТУ», 2026. – 87 с.

Основним завданням даної кваліфікаційної роботи є створення проекту корпоративної мережевої інфраструктури для підприємства, яка повинна забезпечувати високу продуктивність, надійність та захист даних, а також сприяти ефективній роботі користувачів і безперебійному функціонуванню внутрішніх сервісів.

У ході виконання роботи проведено аналіз вимог до майбутньої мережі, здійснено вибір відповідного комутаційного обладнання та програмних рішень, розглянуто питання інформаційної безпеки та методи захисту від зовнішніх загроз. Побудовано логічну модель та фізичну топологію мережі, що дозволяє реалізувати масштабовану та гнучку систему. Також підготовлено практичні інструкції з інсталяції та налаштування серверів, мережевих пристроїв і робочих станцій.

Окремо виконано економічний аналіз запропонованих рішень: визначено витрати на обладнання та програмне забезпечення, а також оцінено очікуваний ефект від реалізації проекту у вигляді зростання продуктивності та зменшення експлуатаційних витрат. У роботі враховано вимоги охорони праці та техніки безпеки, що є важливим аспектом при створенні сучасної інформаційної інфраструктури.

Кваліфікаційна робота складається з пояснювальної записки обсягом (82 сторінок, 14 таблиць, 15 рисунків та 5 креслень на аркушах формату А1).

Ключові слова: персональний комп'ютер, корпоративна мережа, комутаційне обладнання, програмні рішення, захист інформації, економічна ефективність, охорона праці, техніка безпеки.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		4

ANNOTATION

Kurylo V.O. Design of a Computer Network for the Company “WebTop”: Qualification Work for the Educational and Professional Degree of Junior Bachelor in Specialty 123 “Computer Engineering.” – Ternopil: VSP “TFK TNTU,” 2026. – 87 p.

The main objective of this qualification work is to develop a corporate network infrastructure for the enterprise that ensures high performance, reliability, and data protection, while supporting efficient user operations and uninterrupted functioning of internal services. The work includes analysis of network requirements, selection of appropriate switching equipment and software solutions, consideration of information security issues, and methods of protection against external threats. A logical model and physical topology of the network were designed to enable scalability and flexibility. Practical instructions for installation and configuration of servers, network devices, and workstations were also prepared.

An economic analysis of the proposed solutions was carried out: costs for equipment and software were calculated, and the expected benefits of implementation were evaluated in terms of increased productivity and reduced operating expenses. Occupational safety and labor protection requirements were taken into account as an essential aspect of modern information infrastructure design.

The qualification work consists of an explanatory note (82 pages, 14 tables, 15 figures) and a graphical section with 5 drawings on A1 sheets.

Keywords: personal computer, corporate network, switching equipment, software solutions, information security, economic efficiency, occupational safety, labor protection.

					<i>2026.KBP.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

Перелік термінів і скорочень

Вступ

1 Загальний розділ

1.1 Технічне завдання:

1.1.1 Найменування та область застосування

1.1.2 Призначення розробки

1.1.3 Вимоги до апаратного та програмного забезпечення

1.1.4 Вимоги до документації

1.1.5 Техніко-економічні показники

1.1.6 Стадії та етапи розробки

1.1.7 Порядок контролю та прийому

1.2 Опис задачі та характеристика підприємства (організації, установи)

2 Розробка технічного та робочого проекту

2.1 Опис та обґрунтування вибору логічного типу мережі

2.2 Розробка схеми фізичного розташування кабелів та вузлів:

2.2.1 Типи кабельних з'єднань та їх прокладка

2.2.2 Будова вузлів та необхідність їх застосування

2.3 Обґрунтування вибору комунікаційного обладнання

2.4 Особливості монтажу мережі

2.5 Обґрунтування вибору програмного забезпечення

2.6 Обґрунтування вибору засобів захисту мережі

2.7 Тестування мережі

3 Спеціальний розділ

3.1 Інструкції з налаштування програмного забезпечення серверів

2026.КВР.123.406.12.00.00 ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		В. КУРИЛО			<i>Розробка проекту комп'ютерної мережі компанії "WebTop" Пояснювальна записка</i>	Літ.	Арк.	Аркушів
Перевір.		А. ЮЗЬКІВ						
Реценз.								
Н. Контр.		В. ПРИЙМАК						
Затверд.								
						ВСП «ТФК ТНТУ ім. Ів. Пулюя» гр. КІ-406 м. Тернопіль		

- 3.1.1 Інструкція з налаштування сервера HPE ProLiant DL380 Gen11
- 3.1.2 Інструкція з налаштування NAS-сервера Synology DS923+
- 3.2 Інструкції з налаштування активного комутаційного обладнання
 - 3.2.1 Інструкція з налаштування головного комутатора MikroTik CRS326-24G-2S+RM
 - 3.2.2 Інструкція з налаштування комутаторів робочих груп MikroTik CSS318-16G-2S+IN
 - 3.2.3 Інструкція з налаштування безпроводного маршрутизатора MikroTik sAP ax
- 3.3 Інструкція з використання тестових наборів та програм
- 3.4 Інструкція з експлуатації та моніторингу в мережі
- 4 Економічний розділ
 - 4.1 Визначення стадій техн.. процесу та загальної тривалості проведення НДР
 - 4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи
 - 4.3 Розрахунок матеріальних витрат
 - 4.4 Розрахунок витрат на електроенергію
 - 4.5 Визначення транспортних затрат
 - 4.6 Розрахунок суми амортизаційних відрахувань
 - 4.7 Обчислення накладних витрат
 - 4.8 Складання кошторису витрат та визначення собівартості НДР
 - 4.9 Розрахунок ціни НДР
 - 4.10 Визначення економ. ефективності і терміну окупності кап. вкладень
- 5 Охорона праці, техніка безпеки та екологічні вимоги
 - 5.1 Розслідування та облік аварій на виробництві
 - 5.2 Інженерні заходи щодо зниження рівня акустичного шуму на робочих місцях персоналу компанії «WebTop»

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

5.3 Організація системи управління охороною праці та проведення інструктажів для інженерів мережі в компанії «WebTop»

Висновки

Перелік посилань

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

NAT (Network Address Translation) – мережева трансляція адрес;

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол;

WINS (Windows Internet Name Service) – сервіс імен Windows;

ПК - персональний комп'ютер;

СКС – структурно кабельні системи;

CRM-система (Customer Relationship Management) - програмне забезпечення для автоматизації взаємодії з клієнтами, що зберігає історію спілкування, керує продажами та маркетингом.

Mesh-системи - це комплект із кількох Wi-Fi пристроїв (вузлів/модулів), що створюють єдину безшовну мережу, усуваючи «мертві зони» у великих квартирах чи будинках.

ОС - операційна система.

ПЗ- програмне забезпечення

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		9

ВСТУП

Будь-яка компанія сьогодні не може обходитися без правильно спроектованої комп'ютерної мережі. Вона необхідна для доступу до корпоративних ресурсів, захист даних від зовнішнього впливу та взаємодією між працівниками. Комп'ютерні мережі є 2 типів: провідні та безпроводні.

Основна мета кваліфікаційної роботи це розробка проекту комп'ютерної мережі компанії "WebTop". Провівши аналіз технічного завдання та аналітичний аналіз існуючих рішень, потрібно спроектувати логічну та фізичну топологію мережі, обрати необхідне обладнання, розробити інструкції з інсталяції та налаштування програмного забезпечення.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Тема кваліфікаційної роботи - розробка проекту комп'ютерної мережі компанії "WebTop".

Компанія має багато різноманітних вимог, серед яких можна зазначити:

- Потребу в об'єднанні ПК, що належать різним відділам.
- Забезпечення високошвидкісного підключення до мережі Інтернету для всіх співробітників.
- Введення дешевих та ефективних засобів комунікації між співробітниками.
- Можливість роботи в мережі як з ПК, так і з допомогою ноутбуків або мобільних пристроїв.

1.1.2 Призначення розробки

Практична реалізація кваліфікаційної роботи має на меті реалізувати наступні можливості:

- Можливість об'єднання усіх ПК в єдину мережу з поділом на підмережі.
- Надання можливості доступу до мережі Інтернет робочим станціям, а також іншим пристроям через технологію NAT.
- Розміщення безпроводної точки доступу для приєднання інших пристроїв(ноутбуки, смартфони або планшети).

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

1.1.3 Вимоги до апаратного і програмного забезпечення

Для проєкту локальної мережі потрібно таке обладнання:

- Головний комутатор стандарту Gigabit Ethernet з функціями 3-го рівня моделі OSI.
- Комутатори робочих груп стандарту Gigabit Ethernet.
- Маршрутизатор-шлюз.
- Маршрутизатор з безпроводним інтерфейсом стандарту IEEE 802.11ах.
- Комутаційна шафа.

Локальна мережа буде побудована на основі стеку протоколів TCP/IP версії 4.

1.1.4 Вимоги до документації

Для швидкого і ефективного виконання обслуговування локальної мережі необхідно мати належним чином оформлену технічну документацію. Технічна документація для мережі компанії «WebTop»:

- План приміщення.
- Логічна топологія.
- Схема зв'язків між вузлами перенесена на план приміщення (фізична топологія).
- Таблиця IP-адрес.

1.1.5 Техніко-економічні показники

Основні техніко-економічні показники локальної мережі компанії «WebTop»:

- Тип мережі - Гібридна.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

- Стандарт мережі - Gigabit Ethernet та Wi-Fi6.
- Кількість робочих станцій - 38.
- Середовище передачі - вита пара категорії 5e.
- Вартість мережі – 1180524,55 грн.

1.1.6 Стадії та етапи розробки

Проектування локальної комп'ютерної мережі поділяється на наступні етапи:

- Планування розробки локальної мережі.
- Розробка логічної топології комп'ютерної мережі.
- Розробка фізичної топології комп'ютерної мережі.
- Вибір необхідного обладнання.
- Встановлення комутаційної шафи та підключення комутаційного обладнання.
- Конфігурування головного комутатора.
- Конфігурування комутаторів робочих груп.
- Налаштування маршрутизаторів.
- Тестування та налагодження мережі.
- Написання технічної документації.

1.1.7 Порядок контролю та прийому

Щоб зробити висновок про якість мережі будуть перевірятися такі технічні параметри локальної мережі:

- Параметри тестування фізичного середовища кабельним тестером.
- Перевірка пропускної здатності - максимальна швидкість передачі даних у мережі.
- Визначення відсотка втрати пакетів.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Визначення затримки - час відправлення пакета до отримання відповіді.

1.2 Опис задачі та характеристики підприємства (організації, установи)

Основними напрямками діяльності компанії «WebTop» є:

- проектування та розробка програмного забезпечення (Full-stack development).
- UI/UX дизайн та графічне оформлення цифрових продуктів.
- надання консалтингових послуг у сфері ІТ-інфраструктури.
- підтримка та адміністрування високонавантажених серверних систем.

Офіс компанії розташований на 1 поверсі будівлі та об'єднує в собі відкриті простори для роботи (open space), а також окремі кабінети для адміністрації, серверну та конференц зал. Загальна площа становить близько 210 м².

Функціональна структура компанії складається з 10 відділів, кожен з яких має специфічні вимоги до мережевих ресурсів:

- Відділ розробки і тестування працює з програмами, їм потрібен швидкий доступ до локальних серверів.
- Відділ дизайну займається роботою з великою кількістю медіа файлів, це створює навантаження на швидкість передачі даних.
- Відділ бізнес-аналізу, відділ кадрів та маркетингу використовує хмарні сервіси та CRM системи, тому їм потрібен стабільний доступ до інтернету.
- Відділи фінансів та Адміністрація працюють з конфіденційними даними, тим самим потребують вищий рівень інформаційної безпеки та ізоляції трафіку.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

- Системні адміністратори керують усією інфраструктурою, їм потрібні інструменти для моніторингу та управління.

- Рецепція приймає клієнтів, для цього їм є необхідним стабільний та швидкий Wi-Fi.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

На даний час існує безліч технологій побудови локальної мережі, до них відносяться: Ethernet, FDDI, ATM, Token Ring і ARCNET. Проте найбільш поширеною є Ethernet та її удосконалені версії (Fast Ethernet та Gigabit Ethernet), які кращі за своїх конкурентів для побудови локальних мереж. Якщо порівнювати Gigabit Ethernet з усіма вище перерахованими технологіями менш затратний на обладнання та обслуговуванні, забезпечує вразі більшу пропускну здатність. Можна виділити ще технологію FDDI (Fiber Distributed Data Interface), яка також забезпечує непогану пропускну здатність (100 Мбіт/с), проте для її роботи необхідні дорогі волоконно-оптичні лінії зв'язку, а також вона складніша у монтажі.

Для побудови фізичного рівня мережі використано стандарт Gigabit Ethernet. Він на сьогоднішній день є досить поширеним, пропускну здатність велика. Також стандарт підтримує старі версії Ethernet та Fast Ethernet, що дозволяє йому працювати із старим мережевим обладнанням.

Існують і стандарти з більшою пропускну здатністю, наприклад: 10 Gigabit Ethernet, але на цей момент впровадження їх в експлуатацію для звичайних користувачів не є раціональним, оскільки:

- Висока вартість обладнання - більшість домашніх моделей маршрутизаторів має лише порти на 1 Гбіт/с;
- Потреба у кабелях класу 6 якщо відстань передачі до 55 м або класу 6а/7 якщо передача даних до 100 м, які товстіші, жорсткіші за рахунок чого важчі в монтажі;
- Немає необхідності у такій великій пропускну здатності: для домашнього користування 1 Гбіт/с - це величезний запас, наприклад для стрімінгу 4К-відео використовується лише приблизно 25 Мбіт/с;

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Тепловиділення і шум - чіпи, які мають можливість обробляти 10Гбіт/с, сильно нагріваються. Також комутатори які підтримують таку пропускну здатність оснащенні активним охолодженням, яке створює досить високий рівень шуму, що є неприйнятним для розташування наприклад в квартирах.

За рахунок того, що технологія добре знайома користувачам і забезпечує сумісність з Ethernet, Gigabit Ethernet не потребує перенавчання мережевих адміністраторів та користувачів, зміни обладнання. Також немає необхідності забезпечувати підтримку додаткових протоколів та інтерфейсів.

Оскільки в проектуванні передбачено бездротовий сегмент мережі, розглянемо стандарти побудови WLAN, та їх переваги і недоліки. За висновком з цього порівняння можливо буде вибрати найкращий варіант для поставлених задач.

Безпроводні мережі Wi-Fi вже стали частиною нашого життя, витіснивши провідні мережі по ряду причин:

- Мобільність - користувач з його робочою машиною не прив'язаний до якогось конкретного місця в мережі;

- Масштабованість - до одного роутера можливо підключити десятки пристроїв, тоді як у провідному варіанті потрібно поставити окремий комутатор для підключення всіх пристроїв.

- Економічна вигода - якщо мережа встановлюється в офісі в перспективі це економить багато коштів, а саме на фізичному пошкодженні кабелів(перегини, пошкодження конекторів), робота майстрів та вартість кабелю.

- Гнучкість покриття - mesh-системи дозволяють легко розширювати покриття, просто встановивши додатковий модуль у мертвій зоні.

Різновид устаткування постійно розширюється, поліпшення захисту та вдосконалення стандартів робить можливим застосування корпоративних бездротових локальних мереж.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		17

На даний момент існує 5 основних стандартів Wi-Fi - це 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax.[6].

Стандарт 802.11b також відомий як Wi-Fi. Це самий перший масовий стандарт бездротової мережі, розроблений у 1999 році. Пропускна здатність досить невелика, а безпека знаходиться на низькому рівні. Для захисту використовують протокол WEP, який зарекомендував себе не з кращого боку. Не рекомендується для домашнього користування, а тим більше для корпоративного використання.

- Швидкість - 11 Мбіт/с.
- Протокол забезпечення безпеки - WEP.
- Рівень захисту - низький.

Стандарт 802.11g загальновідомий як Wi-Fi3. Це поєднання 2 старших стандартів 802.11a та 802.11b, прийнятий в 2003 році. Пропускна здатність уже на рівні стандарту 802.11a, але використовується канал зв'язку 2.4 ГГц. Рівень безпеки також став кращим через введення нового протоколу безпеки, названого WPA. Він використовував протокол TKIP (Temporal Key Integrity Protocol - протокол тимчасової цілісності ключів), який ефективно бореться з проблемою, що лежить в основі вразливості WEP, повторного використання ключів шифрування. Але на даний час вважається не надійним.[12]

- Швидкість - 54 Мбіт/с.
- Протокол забезпечення безпеки - WPA.
- Рівень захисту - середній.

Стандарт 802.11n відомий як Wi-Fi4. Стандарт схвалено у 2009 році, швидкість передачі даних знову ж таки зросла. Використовує обидва канали зв'язку 2.4 та 5 ГГц. А висока швидкість досягається завдяки новій технології MIMO(multiple-input multiple-output), яка дає змогу використовувати одразу декілька антен для одночасного прийому і передачі даних. Також використовує новішу версію протоколу WPA, а саме WPA2. Цей протокол безпеки уже використовує протокол CCMP(Counter Mode with Cipher Block

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

Chaining Message Authentication Code Protocol), який базується на алгоритмі шифрування AES(Advanced Encryption Standard)[3].

- Швидкість - 600 Мбіт/с.
- Протокол забезпечення безпеки - WPA2.
- Рівень захисту - великий.

Стандарт 802.11ac відомий як Wi-Fi5. Стандарт прийнято в 2013 році. Використовує лише канал зв'язку 5 ГГц. Проте пропускна здатність зросла до 1 Гбіт/с. Протокол безпеки залишився такий же, WPA2.

- Швидкість - до 1 Гбіт/с.
- Протокол забезпечення безпеки - WPA2.
- Рівень захисту - великий.

Стандарт 802.11ax загальновідомий як Wi-Fi6. Розроблений в 2019 році. Працює на обох каналах зв'язку 2.4 і 5 ГГц. А також пропускна здатність зросла понад 1 Гбіт/с. Рівень безпеки також вдосконалили. Тепер використовується протокол безпеки під назвою WPA3, який захищає від атак шляхом підбору паролів і захищає минулий трафік в разі, якщо пароль все ж зламали.

- Швидкість - понад 1 Гбіт/с.
- Протокол забезпечення безпеки - WPA3.
- Рівень безпеки - максимально можливий станом на зараз.

Провівши аналіз стандартів бездротового зв'язку найбільш доцільним є використання стандарту IEEE 802.11ax (Wi-Fi6). Основна задача цього покоління - підвищення пропускної здатності в людних місцях, наприклад офіси або торгові центри, а швидкість порівняно з старшим стандартом зросла вразі. Стандарт також підтримує сумісність з старішими версіями. Оскільки офіс компанії «WebTop» передбачає використання мобільних пристроїв та використання хмарних сервісів, вибір є обґрунтованим з технічної, так і з перспективної точки зору.[7]

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

Для сегментування мережі на підмережі використовуватиметься технологія VLAN відповідно до стандарту IEEE 802.1Q. Це буде здійснено засобами комутатора 3 рівня OSI.

VLAN (Virtual Local Area Network — віртуальна локальна комп'ютерна мережа) є групою хостів із загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, що й фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі, а реконфігурація мережі може бути зроблена за допомогою програмного забезпечення замість фізичного переміщення пристроїв [13].

В таблиці 2.1 наведено дані про логічну адресацію в локальній мережі.

Таблиця 2.1 - Логічна адресація в ЛОМ

№ п/п	Діапазон позначен ня вузлів	Робоча група/ К-сть вузлів		Примі щення	Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
		3	4		5	6		
1	WS_1- WS_8, SW_1	-	9	1	Відділ розробки	-	51	192.168.51.0/24
2	WS_9- WS_14	-	6	2	Відділ дизайну	-	52	192.168.52.0/24
3	WS_15- WS_18	-	4	3	Відділ бізнес аналізу	-	53	192.168.53.0/24
4	WS_19- WS_22, SW_2	-	5	4	Відділ кадрів	-	54	192.168.54.0/24

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		20

Продовження таблиці 2.1

1	2	3	4	5	6	7	8	9
5	WS_23- WS_26	-	4	5	Відділ фінансів	-	55	192.168.55.0/24
6	WS_27- WS_30	-	4	6	Відділ маркетингу	-	56	192.168.56.0/24
7	WS_31- WS_34, SW_3	-	6	7	Відділ тестування	-	57	192.168.57.0/24
8	AP_1	-	1	10	Кімната засідань	-	58	192.168.58.0/24
9	WS_35	-	1	8	Адміністрація	-	59	192.168.59.0/24
10	WS_36, SW_4, S_1-S_2	-	4	9	Серверна	-	60	192.168.60.0/24
11	WS_37- WS_38,	-	2	12	Рецепція	-	61	192.168.61.0/24

В таблиці 2.2 наведено дані, які необхідні перед початком конфігурування VLAN.

Таблиця 2.2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мер. пристар.	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS_8	Eth0	-	SW_1	1-8	Access	51

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21

Продовження таблиці 2.2

1	2	3	4	5	6	7	8
2	WS_9-WS_14	Eth0	-	SW_1	9-14	Access	52
3	WS_15-WS_18	Eth0	-	SW_2	1-4	Access	53
4	WS_19-WS_22	Eth0	-	SW_2	5-8	Access	54
5	WS_23-WS_26	Eth0	-	SW_2	9-12	Access	55
6	WS_27-WS_30	Eth0	-	SW_3	1-4	Access	56
7	WS_31-WS_34	Eth0	-	SW_3	5-8	Access	57
8	AP_1	Eth0	-	SW_4	20	Access	58
9	WS_35	Eth0	-	SW_3	9	Access	59
10	WS_36	Eth0	-	SW_4	10	Access	60
11	WS_37-WS_38	Eth0	-	SW_4	11-12	Access	61
12	SW_1	15	Trunk	SW_4	3	Trunk	-
13	SW_2	15	Trunk	SW_4	4	Trunk	-
14	SW_3	15	Trunk	SW_4	5	Trunk	-
15	S_1	1	-	SW_4	2	Access	60
16	S_2	2	-	SW_4	1	Access	50

					<i>2026.KBP.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

СКС локальної мережі компанії складається з таких підсистем:

- Підсистема робочого місця. Складається з робочої станції, мережевої розетки та патчкорду, який підключає станцію до мережевої розетки. Патчкорд і мережева розетка узгоджуються з вимогами категорії 5e. Мережева плата робочої станції підтримує стандарти Ethernet/Fast Ethernet/Gigabit Ethernet.

- Горизонтальна підсистема. Представляє кабельні сегменти, які з'єднують мережеві розетки з комутатором робочих груп.

- Вертикальна підсистема. Представляє кабельні сегменти, які з'єднують комутатори робочих груп з центральним комутатором. Ці сегменти заходять у патч-панель, яка розміщена у комутаційній шафі з іншим мережевим обладнанням.

- Підсистема технічного приміщення, в якому буде знаходитися комутаційна шафа.

Обладнання буде розміщено у спеціально обладнаному серверному приміщенні.

2.2.2 Будова вузлів та необхідність їх застосування

Топологія локальної мережі є одним із ключових елементів під час проектування мереж. Також вона визначає спосіб взаємодії між пристроями, рівень надійності, швидкість передачі даних та можливість подальшого розширення мережі. Для компанії «WebTop» була розроблена локальна мережа, яка має два сегменти: провідний та безпроводний. Такий підхід

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

забезпечує стабільну роботу стаціонарних пристроїв та дає можливість для мобільного підключення до мережі.

При проектуванні локальних мереж використовують різні типи топологій, у кожній з них є свої переваги та недоліки. Виділяють 3 основні види топологій, а саме “зірка”, “кільце” та “шина”. В таблиці 2.3 наведено порівняльну характеристику цих топологій.

Таблиця 2.3 – Порівняльна характеристика топологій локальних мереж

Характеристика	Зірка	Кільце	Шина
Надійність роботи	Висока	Середня	Низька
Простота адміністрування	Висока	Середня	Низька
Вартість реалізації	Середня	Середня	Низька
Можливість розширення	Висока	Обмежена	Обмежена
Швидкість передачі даних	Висока	Середня	Низька
Захист від збоїв	Високий	Середній	Низький
Витрати кабелю	Значні	Середні	Незначні
Виявлення несправностей	Просте	Ускладнене	Ускладнене
Продуктивність при високому навантаженні	Висока	Середня	Низька

Провівши порівняння для мережі компанії “WebTop” обрано за основу топологію “Гібридна”, яка включає в себе для провідного сегменту топологію

типу “розширена зірка”, а для безпроводного “Бездротова комірчаста”. “Розширена зірка” забезпечує високу пропускну здатність, простоту адміністрування та швидкість у пошуку несправностей. Усе мережеве обладнання підключається до центрального комутатора, який у свою чергу виконує роль головного вузла мережі.

Безпроводний сегмент мережі проваджений за допомогою точки доступу Wi-Fi, топологія “бездротова комірчаста”, яка дає можливість підключати ноутбуки, смартфони та інші мобільні пристрої без фізичного з’єднання за допомогою кабелю. Точка доступу також підключається до центрального комутатора, що забезпечує доступ до локальних ресурсів та значно збільшує рівень безпеки.

Також застосовано топологію типу “Ієрархічна”. Вона передбачає використання більше одного комутатора. Кожен із рівнів виконує свою функцію. Нижні рівні комутаторів обробляють запити на з’єднання між робочими станціями і серверами та функції доступу до локальної мережі. Вищі рівні такого типу топології агрегують нижчі рівні. Такий вид впорядкування добре підходить для малих та середніх за розміром локальних мереж. Також одна з переваг такої топології є можливість легкого подальшого розширення та нарощення пропускну здатності не лише у всій мережі, а й в окремих її сегментах.

2.3 Обґрунтування вибору комунікаційного обладнання

Для побудови мережі використовується пасивне та активне комутаційне обладнання.

До пасивного відноситься:

- Кабельна система локальної мережі (неекранована вита пара категорії 5е, фірма-виробник Одескабель)[[17](#)]
- Розетки RJ-45, які встановлено біля кожного комп’ютера.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		25

- Кабельні сегменти, які з'єднують розетки з портами комутаторів робочих груп.

- Патч-панель 24 порти, категорія 5e, висота 1U. Виробник DIGITUS.[19]

- Комутаційна шафа Digitus 12U Wall Mount Rack 600×450 мм.[4]

До активного комутаційного обладнання мережі відноситься:

- Центральний комутатор.
- Комутатори робочих груп.
- Маршрутизатор з безпроводним інтерфейсом.
- Мережеве сховище.
- Сервер.

Порівняльна характеристика центральних комутаторів наведена в таблиці 2.4.

Таблиця 2.4 – Технічні характеристики комутаторів

	MikroTik CRS326-24G- 2S+RM	Cisco CBS350- 24T-4G	TP-Link SG3428X	TL-
1	2	3	4	
Підтримка стандарту Gigabit Ethernet	+	+	+	
Рівень OSI	L3	L3	L3	
Пропускна здатність комутації	88 Гбіт/с	56 Гбіт/с	128 Гбіт/с	
VLAN 802.1Q	+	+	+	
Статична маршрутизація	+	+	+	
Динамічна маршрутизація	Частково (RouterOS)	RIP	RIP/OSPF	

Продовження таблиці 2.4

1	2	3	4
Керування	RouterOS / SwOS	Web / CLI	Web / CLI / Omada
Орієнтовна вартість	200–220\$	320–380\$	280–330\$

Для мережі обрано комутатор MikroTik CRS326-24G-2S+RM беручи до уваги співвідношення ціна/продуктивність. Зовнішній вигляд комутатора зображено на рисунку 2.1. [9]



Рисунок 2.1 – Комутатор MikroTik CRS326-24G-2S+RM

Наступним кроком необхідно порівняти і обрати комутатори робочих груп. В таблиці 2.5 наведено технічні характеристики комутаторів робочої групи.

Таблиця 2.5 – Технічні характеристики комутаторів

	MikroTik CSS318-16G- 2S+IN	TP-Link TL- SG2218	Cisco CBS250-16T-2G
1	2	3	4
Рівень OSI	L2	L2+	L2
Кількість Ethernet- портів	16 × 1G RJ-45	16 × 1G RJ-45	16 × 1G RJ-45
Пропускна здатність	72 Гбіт/с	36 Гбіт/с	36 Гбіт/с
VLAN 802.1Q	+	+	+

Продовження таблиці 2.5

1	2	3	4
Підтримка QoS та Link Aggregation	+	+	+
Керування	Web (SwOS)	Web / Omada	Web / CLI
Орієнтовна вартість	139\$	170\$	230\$

Для робочих груп використано 3 комутатора MikroTik CSS318-16G-2S+IN, враховуючи їх невелику вартість та конкуренту продуктивність. Зовнішній вигляд зображено на рисунку 2.2.[10]



Рисунок 2.2 – Комутатор MikroTik CSS318-16G-2S+IN

Для створення безпроводного сегменту мережі потрібно використовувати маршрутизатор з безпроводним інтерфейсом. Порівняння характеристик безпроводних маршрутизаторів наведено у таблиці 2.6.

Таблиця 2.6 – Порівняння маршрутизаторів з безпроводним інтерфейсом

	MikroTik cAP ax	TP-Link EAP650	Cisco Business CBW150AX
Підтримувані стандарти	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax (Wi-Fi 6)		
Робочі діапазони	2.4 ГГц / 5 ГГц		
Максимальна швидкість	1774 Мбіт/с	2976 Мбіт/с	1775 Мбіт/с
Віддалене керування	CAPsMAN	Omada SDN	Cisco Business Dashboard
Підсилення антени	5.5 dBi	4 dBi	5 dBi
Орієнтовна вартість	110–130\$	160–190\$	180–220\$

Для безпроводного сегменту вибрано MikroTik cAP ax для стабільної роботи в еко-системі MikroTik, а також він забезпечує більшу дальність зв'язку за рахунок вищого підсилення антени. Його зовнішній вигляд зображено на рисунку 2.3.[8]



Рисунок 2.3 – Безпроводний маршрутизатор MikroTik cAP ax

Наступним кроком необхідно обрати сервер мережевого сховища. Порівняння технічних характеристик наведено у таблиці 2.7.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		29

Таблиця 2.7 – Порівняння технічних характеристик NAS

	Synology DS923+	QNAP TS-464	TerraMaster F4-423
Тип пристрою	NAS 4-bay		
Процесор	AMD Ryzen R1600	Intel Celeron N5105	Intel Celeron N5095
Ядра / потоки	2 / 4	4 / 4	4 / 4
ОЗП	4 GB DDR4 ECC	4 GB DDR4	4 GB DDR4
Макс. ОЗП	32 GB	16 GB	32 GB
Ethernet порти	2 × 1GbE	2 × 2.5GbE	2 × 2.5GbE
RAID підтримка	RAID 0/1/5/6/10, SHR	RAID 0/1/5/6/10	RAID 0/1/5/6/10
Максимальна швидкість	~625 MB/s	~590 MB/s	~580 MB/s

Для використання в мережі обрано Synology DS923+, оскільки він використовує оперативну пам'ять типу ECC(Error-Correcting Code), яка самостійно виявляє та виправляє спотворення бітів, а також він забезпечує більше швидкість за своїх конкурентів. Зовнішній вигляд Synology DS923+ зображено на рисунку 2.4.[\[11\]](#)



Рисунок 2.4 – Сервер мережевого сховища Synology DS923+

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		30

Далі потрібно обрати сервер, який гарантує високий рівень продуктивності та відмовостійкості для побудови корпоративної ІТ-структури. Беручи до уваги потребу у підтримці віртуалізації, високонавантажених сервісів та мережних застосунків, від серверного обладнання вимагають високу обчислювальну потужність та надійність. В таблиці 2.8 зазначено порівняння технічних характеристик серверів.

Таблиця 2.8 – Порівняння характеристик серверів

	HPE ProLiant DL380 Gen11	Dell PowerEdge R760	Lenovo ThinkSystem SR650 V3
Форм-фактор	2U rack		
Процесор	Intel Xeon Scalable 4/5 Gen (до 60+ ядер/CPU)	Intel Xeon Scalable 4/5 Gen (до 56+ ядер/CPU)	Intel Xeon Scalable 4/5 Gen (до 60+ ядер/CPU)
Можливість використання 2 CPU	+	+	+
ОЗП	DDR5 ECC RDIMM	DDR5 ECC RDIMM	DDR5 ECC RDIMM
Макс. ОЗП	до 8 TB	до 8 TB	до 8 TB
Мережа	ОСР 3.0	ОСР / NIC модулі	ОСР / NIC модулі
PCIe	PCIe 5.0	PCIe 5.0	PCIe 5.0
Віртуалізація	VMware, Hyper-V, KVM	VMware, Hyper-V	VMware, Hyper-V
Надійність	Enterprise рівень	Enterprise рівень	Enterprise рівень
Безпека	Silicon Root of Trust	Secure Boot + TPM	TPM + Secure Boot

Для мережі обрано сервер HPE ProLiant DL380 Gen11, він є оптимальним вибором завдяки поєднанню високої потужності, підтримки пам'яті DDR5 ECC та PCIe 5.0. Також окремою перевагою відзначають систему віддаленого керування HPE iLO 6, яка дозволяє контролювати роботу серверу незалежно від стану операційної системи. Зовнішній вигляд серверу зображено на рисунку 2.5.[5]



Рисунок 2.5 – Сервер HPE ProLiant DL380 Gen11

Зведений перелік мережевого обладнання для побудови локальної мережі. наведено в таблиці 2.9.

Таблиця 2.9 - Мережеве обладнання для побудови ЛОМ

№ п/п	Найменування матеріальних ресурсів	Од. вим.	Факт. витрачено матеріалів	Ціна одиниці, грн
1	2	3	4	5
1.	Комутаційна шафа 12U	шт.	1	11000
2.	Патчпанель 24 порти, категорія 5e.	шт.	1	1500
3.	Розетка RJ-45 (категорія 5e)	шт.	38	130
4.	Кабель UTP(cat.5e)	м.	205	28

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		32

Продовження таблиці 2.9

1	2	3	4	5
5.	Патчкорди(cat.5e)	шт.	9	75
6.	Короб	м.	50	110
7.	MikroTik CRS326-24G-2S+RM	шт.	1	9000
8.	MikroTik CSS318-16G-2S+IN	шт.	3	6000
9.	MikroTik cAP ax	шт.	1	5500
10.	Synology DS923+	шт.	1	36000
11.	HPE ProLiant DL380 Gen11	шт.	1	520000
12.	Жорсткий диск 8TB 3.5" 5640 256MB SATA Red Plus NAS WD	шт.	4	17800

2.4 Особливості монтажу мережі

Основним критерієм локальної мережі є якість монтажу кабельної інфраструктури. При використанні сучасного обладнання та кабелю високої категорії, монтаж з порушенням технологій може призвести до значної втрати пропускної здатності, появи перешкод, втрати пакетів і загалом поганої роботи мережі. Через це монтаж кабельної системи повинен відбуватися згідно до вимог міжнародних стандартів ISO/IEC 11801 та ANSI/TIA/EIA-568.

У мережі використовується кабель типу UTP категорії 5e, який здатен забезпечувати швидкість передачі даних на швидкості 1 Гбіт/с. Кабельна система прокладається від центрального комутатора третього рівня до

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33

комутаторів робочих груп, серверного обладнання, точки доступу та інформаційних розеток користувачів.

Під час монтажу необхідно дотримуватися таких вимог:

- Максимальна довжина кабелю не повинна перевищувати 100 м враховуючи патч-корди.
- Уникати надмірного натягу кабелю, це збільшує ризики деформації провідників, що у свою чергу веде до погіршення електричних характеристик.
- Мінімальний радіус вигину кабелю під час монтажу не менше 8 діаметрів кабелю і 4 діаметри під час використання.
- Не прокладати поблизу джерел електромагнітних перешкод, наприклад силові кабелі, люмінесцентні лампи.
- Під час підключення до мережеских розеток мінімізувати відстань розкрученої пари, оскільки це впливає на параметр NEXT.

Для прокладання кабельних ліній використовуються пластикові коробки, які забезпечують захист кабелів від механічних пошкоджень та пилу. Вони встановлюються вздовж стін відповідно до плану прокладання мережі. Встановлюючи коробки потрібно забезпечити вільний внутрішній простір для кабелів, щоб уникнути надмірного згинання та стискання. Кабелі всередині вкладаються вільно, без натягу або перехрещення. Також уникати спільного прокладання у коробах мережеских кабелів з силовими без екранування або розділення.

Установку мережеских розеток та комутаційної панелі необхідно за схемою T568B, вона найпопулярніша для локальних мереж типу Ethernet. А для обтискання кабелів необхідно використовувати спеціалізовані інструменти.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

2.5 Обґрунтування вибору програмного забезпечення

Для робочих станцій обрано ОС Windows 11 Pro. Вона являється актуальною платформою для корпоративного використання, також забезпечує високий рівень продуктивності та безпеки.

Ключовими можливостями ОС є:

- Висока продуктивність системи: швидке завантаження ОС та оптимізована робота з багатозадачністю.
- Оновлений інтерфейс користувача, який забезпечує комфортну та інтуїтивну роботу з програмами та файлами.
- Механізми керування ресурсами системи, оптимізація навантаження на процесор та оперативну пам'ять, автоматична діагностика і виявлення помилок.
- Підтримка актуального обладнання та легке встановлення драйверів через центр оновлення Windows.
- Підтримка віддаленої роботи та використання хмарних сервісів.
- Розширені засоби безпеки: захист ядра системи, Secure Boot, шифрування даних через BitLocker, модуль TPM 2.0.
- Інструменти для IT-фахівців: PowerShell, командний рядок, засоби моніторингу стабільності та продуктивності системи.
- Вбудована підтримка віртуалізації через технологію Hyper-V.
- Регулярні оновлення системи безпеки і підтримка нових стандартів мережевого зв'язку.

Для сервера HPE ProLiant DL380 Gen11 обрано серверну операційну систему Ubuntu Server 24.04.4 LTS. Ця ОС є найпопулярнішим рішенням для серверного обладнання через високу стабільність, безпеку та широкі можливості адміністрування.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

Основними перевагами Ubuntu Server є:

- Висока надійність та стабільність роботи серверних служб.
- Низькі системні вимоги, водночас ефективне використання апаратних ресурсів.
- Високий рівень безпеки і регулярні оновлення ОС.
- Підтримка мережевих служб DHCP, DNS, FTP, SMB.
- Можливість керування сервером віддалено через SSH.
- Підтримка віртуалізації та контейнеризації.
- Сумісність з актуальним серверним обладнанням.
- Великий різновид безкоштовного серверного програмного забезпечення.
- Відсутність необхідності купівлі ліцензії.

Мережеве сховище Synology DS923+ використовує власну ОС DiskStation Manager (DSM). Вона розроблена спеціально під пристрої Synology і надає можливість зручного керувати файлами та резервним копіюванням.

Основними можливостями DMS є:

- Централізоване файлове сховище для користувачів мережі.
- Підтримка RAID-масивів для забезпечення відмовостійкості та збереження даних.
- Автоматичне резервне копіювання даних.
- Віддалений доступ до файлів через веб-інтерфейс.
- Вбудовані засоби моніторингу стану дисків та системи.
- Розмежування прав доступу користувачів.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		36

2.6 Обґрунтування вибору засобів захисту мережі

Для надійної та безпечної роботи мережі необхідно використовувати комплекс засобів захисту. Основне завдання захисту мережі є запобігання несанкціонованому доступу до ресурсів компанії, захист від шкідливого ПЗ та мережевих атак.

У цій мережі для захисту робочих станцій використовується вбудований в ОС міжмережевий екран Microsoft Defender Firewall, який контролює вхідний та вихідний мережевий трафік, блокує небажані підключення та обмежує доступ до ресурсів. Для захисту від зловмисного ПЗ використовується Microsoft Defender, який постійно виконує моніторинг системи та автоматично виявляє потенційно небезпечне програмне забезпечення.

Для серверу HPE ProLiant DL380 Gen11, який працює з ОС Ubuntu Server, використовується внутрішні засоби захисту Linux. Основний з них це UFW (Uncomplicated Firewall), за допомогою нього можна налаштувати правила фільтрації трафіку та обмежити доступ до серверних служб. Також для підвищення безпеки використовується регулярне оновлення ОС та ПЗ, розмежування прав доступу користувачів, резервне копіювання даних, контроль системних журналів та моніторинг активності сервера.

Для захисту NAS Synology DS923+ використовуються вбудовані механізми безпеки DSM. Серед них: система автентифікації користувачів, налаштування прав доступу до файлів, шифрування даних та моніторинг підключень до сховища.

Також не менш важливим елементом захисту являється використання VLAN на комутаторі 3 рівня. Розділення мережі на окремі сегменти підвищує рівень безпеки, зменшує навантаження на мережу та дає змогу обмежити доступ до мережевих ресурсів.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		37

2.7 Тестування мережі

Тестування комп'ютерної мережі включає в себе використання різних програм та апаратних засобів для контролю працездатності мережевої інфраструктури, правильності налаштування обладнання та ефективність передачі даних. Засоби, використані для тестування мережі, описані в розділі 3.3 «Інструкція з використання тестових наборів та програм».

Для перевірки кабельної інфраструктури мережі використовується тестер Fluke Networks MicroScanner MS2-100, який є актуальним пристроєм для діагностики та перевірки мідних кабельних мереж Ethernet(див. рис. 2.6).

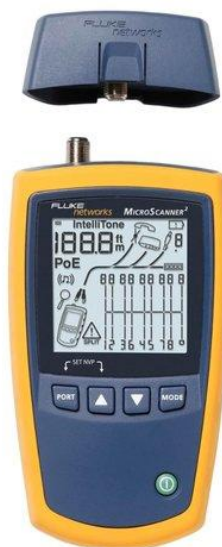


Рисунок 2.6 – Тестер Fluke Networks MicroScanner MS2-100

Функції які підтримує даний пристрій:

- Модульний порт: сумісність із роз'ємами RJ45 і RJ11, а також із коаксіальним F (тестування відео й звуку).
- Вбудований рефлектометр: визначення відстані до точки пошкодження / обриву / короткого замикання, довжини кабелю в діапазоні до 460 метрів.

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Функція PoE: виключає недостатній рівень напруги з переліку ймовірних проблем.
- Режим детального перегляду: додаткова інформація про стан перевірки.
- Схема розведення кабелів: відображає вид та місце несправності (некоректне розведення, полярність, розщеплені пари, короткі замикання, обриви).
- Ідентифікація Ethernet-портів та їхньої швидкості: 10/100/1000 Мбіт.
- Технологія IntelliTone: відстежує практично будь-який кабель або виту пару за допомогою цифрового та аналогового тонування. У режимі генерації аналогового сигналу пристрій сумісний з будь-яким аналоговим щупом.
- Калібрування: NVP з можливістю користувацьких налаштувань для витої пари чи коаксіального кабелю. Тестер дозволяє визначати фактичне значення NVP, якщо йдеться про кабель точно відомої довжини.
- Автовимкнення: так, через 10 хв неактивності.
- Великий РК-дисплей з підсвічуванням (монохром) та інтуїтивно зрозумілими позначеннями.[\[23\]](#)

Під час тестування мережевої інфраструктури буде здійснюватися перевірка правильності обтиску та відповідності розводки провідників стандарту T568B, що дозволяє виявити несправності ще на етапі інсталяції. Також тестером перевіряється цілісність кабельних ліній, наявність обривів, коротких замикань, переплутаних або розщеплених пар. Ще виконується вимірювання довжини кабельних сегментів для контролю відповідності встановленим нормативам СКС.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		39

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

3.1.1 Інструкція з налаштування сервера HPE ProLiant DL380 Gen11

Для працездатності серверу потрібно встановити на нього ОС. Для цього необхідно створити завантажувальний носій USB. Далі у Boot Manager обрати його та запустити інсталяцію.

Під час інсталяції ОС необхідно виконати декілька кроків:

- Налаштувати статичну IP-адресу сервера.
- Створити обліковий запис адміністратора.
- Встановити OpenSSH Server.

Розглянемо кожен з кроків, налаштувати статичну IP-адресу сервера можна одразу після вікна вибору мови системи та розкладки клавіатури. Це необхідно зробити для стабільного доступу до сервера з локальної мережі. На рисунку 3.1 зображено налаштування статичної IP-адреси.

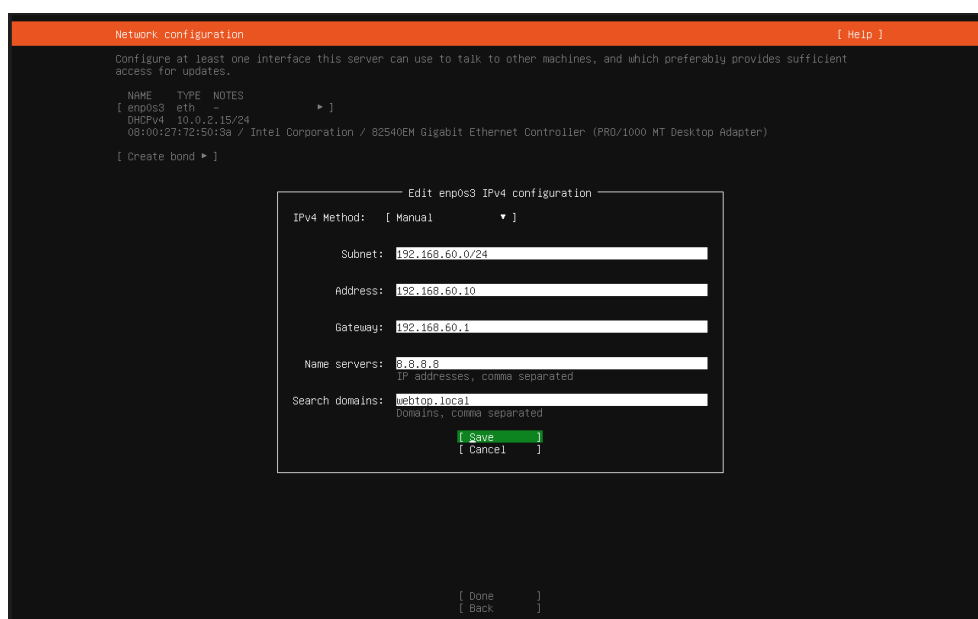


Рисунок 3.1 – налаштування статичної IP-адреси сервера.

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

Наступним кроком є створення облікового запису адміністратора. Надалі для доступу до сервера буде можливість використання SSH ключів, але цей обліковий запис потрібен для виконання таких команд, наприклад як sudo. На рисунку 3.2 зображено вікно створення облікового запису адміністратора.

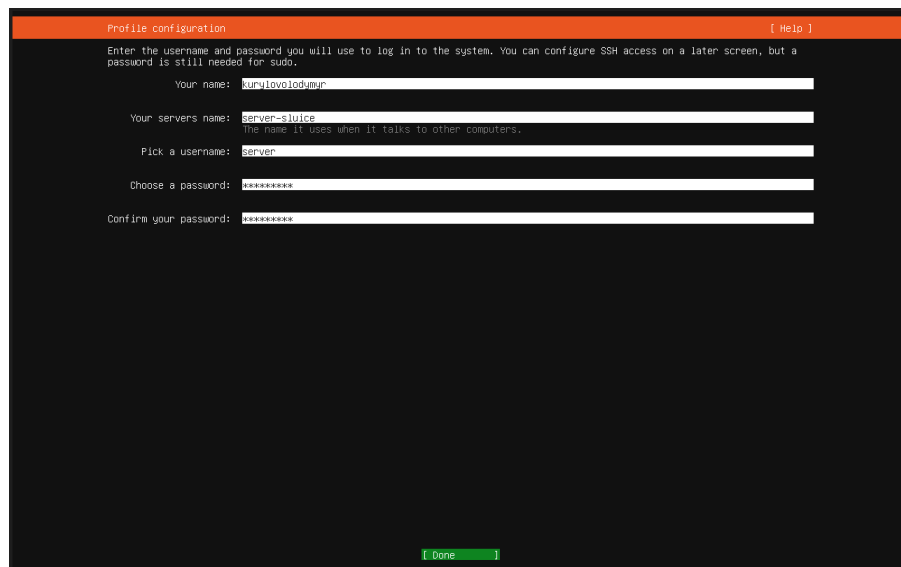


Рисунок 3.2 – Вікно створення облікового запису адміністратора.

Далі для можливості використання SSH ключів необхідно інсталиувати OpenSSH Server, поставивши відмітку у відповідному пункті(див. рис. 3.3).

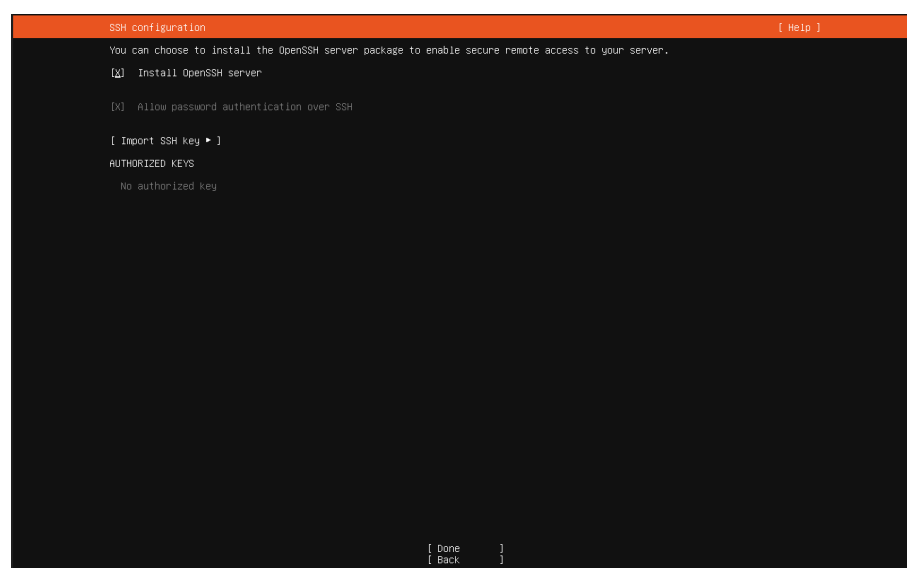


Рисунок 3.3 – Інсталяція OpenSSH Server

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		41

Після цього інсталяція ОС завершиться і сервер перезавантажиться. Після перезавантаження обов'язково потрібно перевірити систему на наявність оновлень та додатково встановити утиліти для моніторингу системи, роботи з мережею та адміністрування сервера. Це виконується за допомогою команд:

```
sudo apt upgrade -y
```

```
sudo apt install net-tools htop mc curl wget unzip software-properties-common -y
```

Наступний крок це налаштування мережевих інтерфейсів. В Ubuntu 24.04 Netplan використовує формат YAML.

Оскільки маршрутизація між користувацькими VLAN (51–61) здійснюється на комутаторі SW_4, у налаштуваннях Netplan прописано обов'язковий статичний маршрут (routes). Він вказує ядру Linux, що весь трафік, адресований у внутрішні підмережі класу 192.168.0.0/16, сервер повинен відправляти на IP-адресу комутатора 192.168.50.1.

Щоб відкрити конфігураційний файл потрібно виконати команду:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

Вміст файлу повністю замінити на наступний:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp1s0:
      dhcp4: true
    enp2s0:
      addresses: [192.168.50.2/30]
      dhcp4: false
      dhcp6: false
  routes:
```

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

- to: 192.168.0.0/16

via: 192.168.50.1

Для збереження змін у файлі потрібно натиснути комбінацію клавіш Ctrl+O, а щоб закрити редактор файлу комбінація Ctrl+X. Після закриття редактору файлу потрібно застосувати налаштування командою:

```
sudo netplan apply
```

Також необхідно перевести ядро системи у режим маршрутизації транзитного трафіку, оскільки потрібно забезпечити наскрізне проходження IP-пакетів між різними фізичними інтерфейсами пристрою. Це реалізовано наступною командою:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

Наступним кроком для забезпечення працездатності шлюзу та надання доступу користувачам локальної мережі до ресурсів Інтернет необхідно налаштувати трансляцію мережевих адрес NAT (Network Address Translation) та правильно налаштувати FireWall.

Як сучасний міжмережевий екран в ОС Ubuntu 24.04 LTS за замовчуванням використовується підсистема nftables. Конфігурування базового механізму маскуванню трафіку (NAT Masquerade) для зовнішнього інтерфейсу enp1s0 виконується так само, як і FireWall у системному файлі /etc/nftables.conf.

Реалізовані правила міжмережевого екрана базуються на таких архітектурних принципах:

- Реалізація концепції Zero Trust у межах ланцюжка input передбачає впровадження глобальної політики безпеки зі станом policy drop. Це забезпечує повне блокування сервером будь-яких вхідних запитів або спроб сканування, що надходять із зовнішньої мережі, гарантуючи надійний рівень захисту від несанкціонованого доступу.

- Забезпечення стабільності користувацьких сесій досягається завдяки правилу ct state established,related accept. Це правило в межах Firewall

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		43

автоматично дозволяє зворотній рух пакетів для з'єднань, які вже були ініційовані та перевірені. Такий підхід гарантує стабільне й безперешкодне отримання відповідей від веб-сайтів користувачами після надсилання ними запитів.

- Захист адміністративної консолі. Для мінімізації ризиків несанкціонованого віддаленого доступу, підключення до сервера через протокол SSH (TCP-порт 22) та до служби DNS (порт 53) дозволено виключно через внутрішній мережевий інтерфейс `enp2s0`. Усі спроби доступу до консолі керування з боку зовнішнього інтерфейсу інтернет-провайдера блокуються на рівні апаратного та програмного забезпечення.

- Маскування внутрішньої мережевої структури (NAT) здійснюється через таблицю `ip nat` з використанням директиви `masquerade` для зовнішнього інтерфейсу `enp1s0`. Цей механізм трансляції адрес автоматично змінює приватні IP-адреси пристроїв у мережі на одну публічну IP-адресу, яку надає провайдер. Таким чином приховується реальна кількість пристроїв у мережі, а також топологія внутрішніх VLAN від потенційних зовнішніх загроз або зловмисників.

Для відкриття вмісту файлу виконується команда:

```
sudo nano /etc/nftables.conf
```

Далі наведено конфігураційний лістинг правил nftables:

```
#!/usr/sbin/nft -f
```

```
flush ruleset
```

```
table ip filter {
```

```
  chain input {
```

```
    type filter hook input priority filter; policy drop;
```

```
    iifname "lo" accept
```

```
    ct state established,related accept
```

```
    iifname "enp2s0" tcp dport { 22, 53 } accept
```

```
    iifname "enp2s0" udp dport 53 accept
```

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

```

    ip protocol icmp accept
}
chain forward {
    type filter hook forward priority filter; policy accept;
}
chain output {
    type filter hook output priority filter; policy accept;
}
}
table ip nat {
    chain postrouting {
        type nat hook postrouting priority srcnat;
        oifname "enp1s0" masquerade comment "NAT в інтернет"
    }
}

```

Після написання зберегти зміни та перезапустити службу:

```
sudo systemctl restart nftables
```

```
sudo systemctl enable nftables
```

І останнім кроком є розгортання та конфігурування локального DNS-сервера. Він потрібен для прискорення завантаження веб-ресурсів та зручного доступу користувачів компанії до внутрішніх серверів за символічними іменами. Для цього буде використовуватися служба dnsmasq, налаштовану в режимі кешуючого DNS-сервера.

Архітектура DNS-сервера:

- Директива `interface=enp2s0` разом із `listen-address=192.168.50.2` налаштовує службу так, щоб вона працювала виключно у межах внутрішньої мережі. Це надзвичайно важливий захід захисту, який запобігає виникненню DDoS-атак типу DNS Amplification. У таких атаках зловмисники

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

експлуатують відкриті DNS-резолвери для створення перевантаження у зовнішніх каналах зв'язку.

- Опція `cache-size=1500` передбачає виділення оперативної пам'яті для зберігання до 1500 останніх запитів. Завдяки цьому, при повторному доступі до часто відвідуваних ресурсів, як-от пошукові системи, сервер швидко надає відповідну IP-адресу з локального кешу. Це дозволяє зменшити затримки, пов'язані з опитуванням віддалених серверів у мережі Інтернет.

- Блок локальних доменних імен (`address=...`) забезпечує внутрішню організацію зони `.webtop`. Завдяки цьому користувачі можуть підключатися до файлового сховища Synology NAS, використовуючи просту адресу `nas.webtop` замість складного набору цифрових IP-адрес. Це значно покращує зручність і комфорт при роботі в мережі.

Налаштування служби виконується в системному файлі `/etc/dnsmasq.conf` який можна відкрити за допомогою команди:

```
sudo nano /etc/dnsmasq.conf
```

Далі наведено конфігураційний лістинг служби `dnsmasq`:

```
interface=lo
```

```
interface=enp2s0
```

```
listen-address=127.0.0.1,192.168.50.2
```

```
server=217.196.160.44
```

```
server=185.53.79.89
```

```
strict-order
```

```
cache-size=1500
```

```
# Внутрішні локальні DNS-записи компанії WebTop
```

```
address=/nas.webtop/192.168.60.5
```

```
address=/gateway.webtop/192.168.50.2
```

Після налаштування також потрібно перезавантажити службу, щоб вона почала виконувати нові вказівки з конфігураційного файлу:

```
sudo systemctl restart dnsmasq
```

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46

```
sudo systemctl enable dnsmasq
```

3.1.2 Інструкція з налаштування NAS-сервера Synology DS923+

Оскільки Synology DS923+ використовує власну ОС, а саме DSM 7.3.2, налаштування файлового серверу відбувається через веб-інтерфейс. Для початку потрібно виконати статичне налаштування мережевих параметрів. Для цього потрібно перейти в Панель керування(Control Panel), далі Мережа(Network) та обрати вкладку Мережевий інтерфейс(Network Interface). Зовнішній вигляд вкладки зображено на рисунку 3.4.

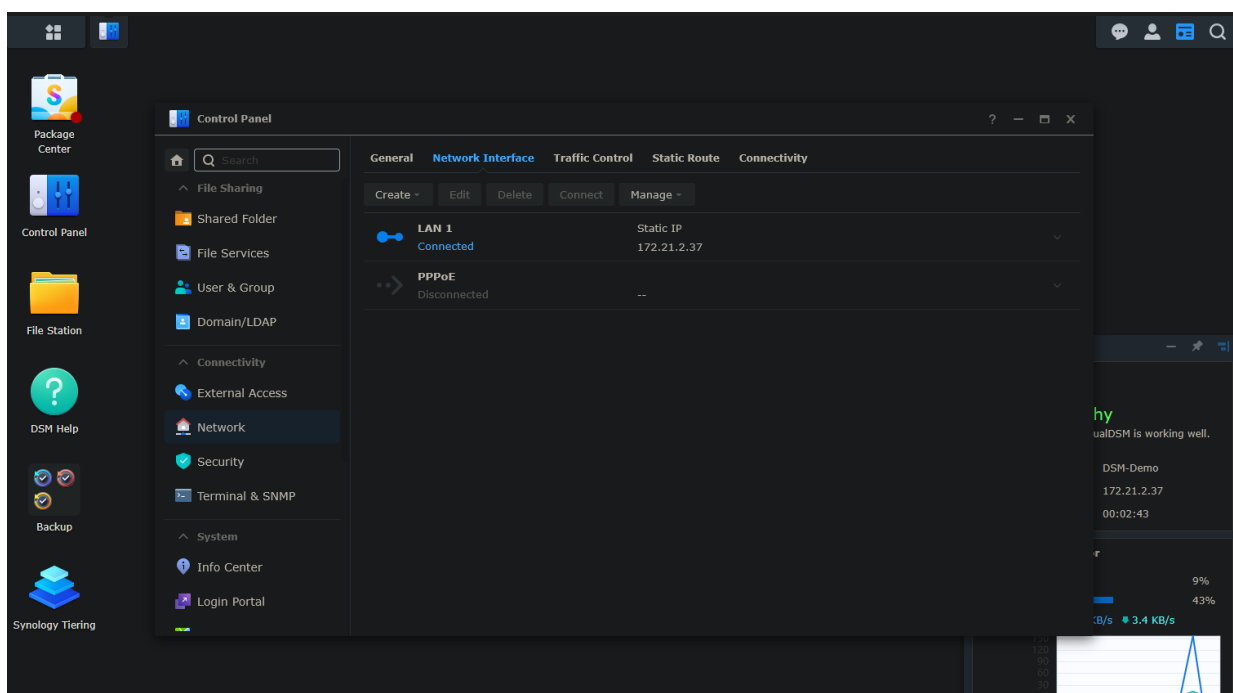


Рисунок 3.4 – Зовнішній вигляд вкладки Network Interface

Далі потрібно обрати фізичний інтерфейс LAN 1 та натиснути кнопку Редагувати(Edit).

У вікні налаштувань IPv4 активувати опцію “Use manual configuration” та внести наступні параметри як вказано на рисунку 3.5.

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

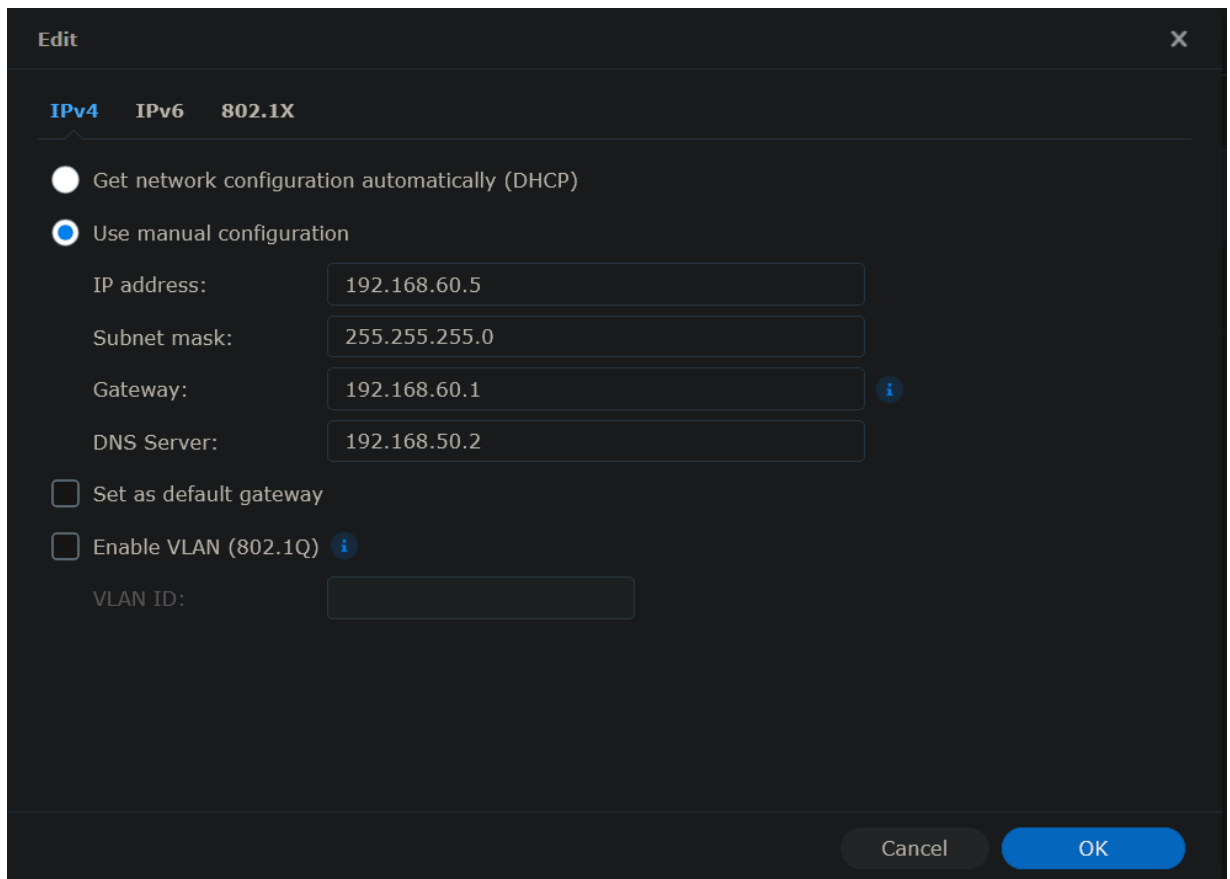


Рисунок 3.5 – Статичне налаштування мережевих параметрів

Після завершення обов'язково натиснути кнопку Зберегти(Apply) для застосування параметрів.

Наступним кроком є конфігурування дискового простору та файлової системи Btrfs.

Для захисту від фізичного виходу з ладу накопичувачів формується RAID-масив:

З головного меню DSM, яке знаходиться у верхньому лівому кутку екрану, відкрити утиліту Диспетчер зберігання (Storage Manager). Далі перейти у розділ Storage Pool, де натиснути Створити(Create). Обрати потрібні диски для об'єднання в RAID 5(мінімальна необхідна кількість дисків - 3). Після чого перейти в розділ Volume, де потрібно створити логічний том на базі файлової системи Btrfs.

Також щоб кінцеві користувачі мали змогу підключати директорії NAS як мережеві диски, потрібно запустити службу SMB.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		48

Для цього потрібно відкрити меню File Services у Панелі керування. Далі поставити галочку навпроти пункту Enable SMB service, у Workgroup ввести системний ідентифікатор компанії. Після чого натиснути кнопку Advanced Settings та виставити параметри зображені на рисунку 3.6.

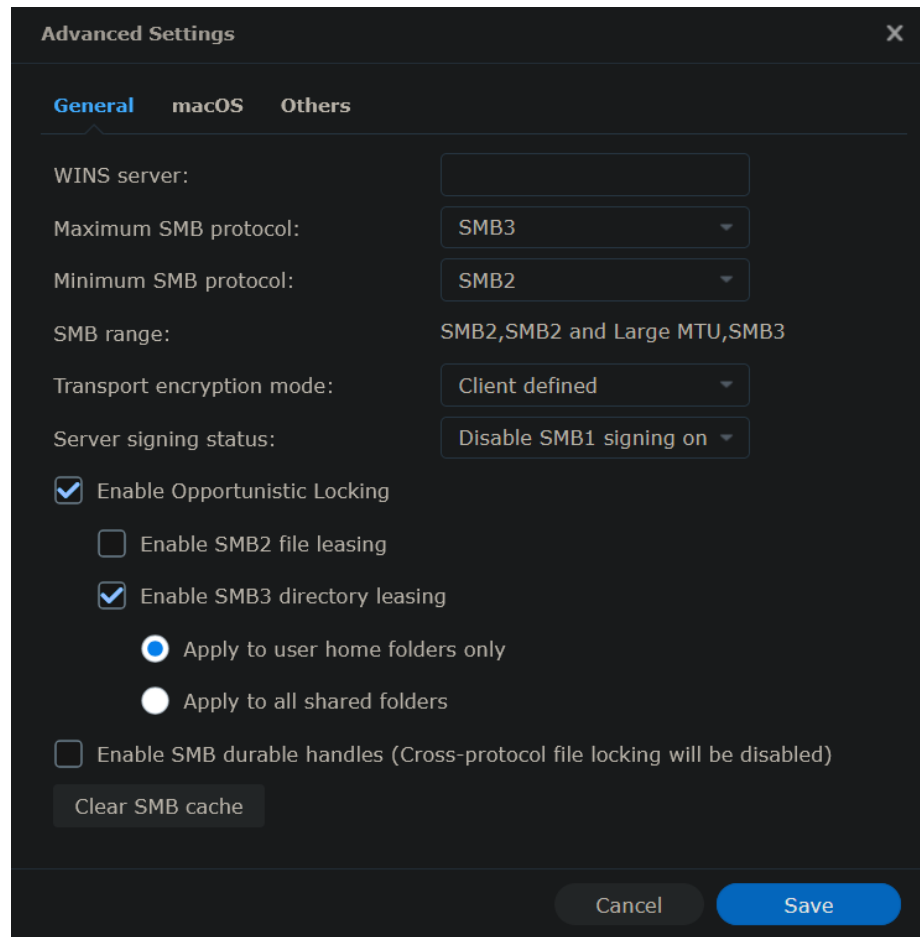


Рисунок 3.6 – Розширені налаштування сервісу SMB

І фінальним етапом є створення спільного каталогу та розмежування прав між відділами. Для цього відкриваємо Панель керування, далі розділ Shared Folder та натискаємо кнопку створити. У вікні потрібно задати назву каталогу та обрати раніше створений Vtrfs-том.(див. рис. 3.7)

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		49

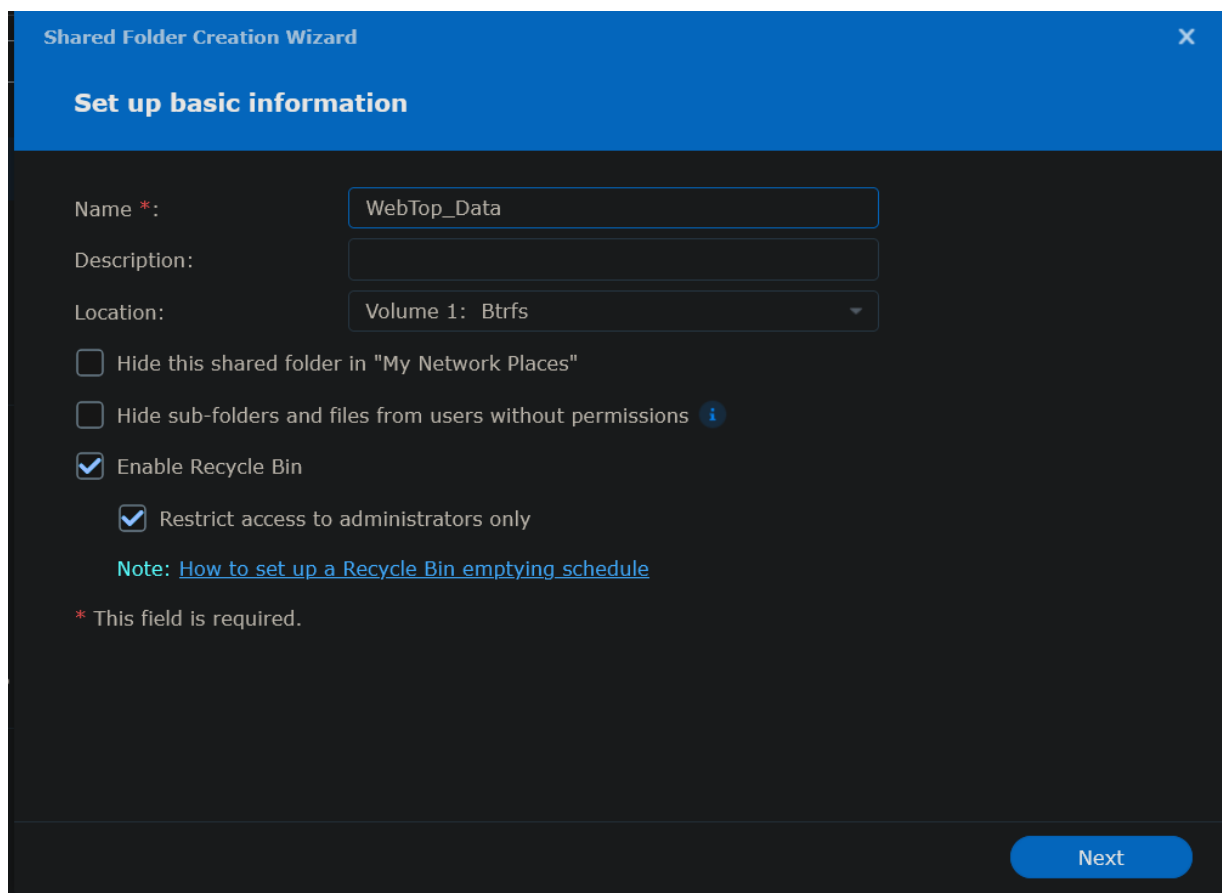


Рисунок 3.7 – Параметри спільного каталогу

Далі потрібно перейти у меню User & Group та створити облікові записи для співробітників та профільні групи, наприклад group_dev – відділ розробки, group_hr – відділ кадрів і тд.

Після чого потрібно повернутися назад до каталогу який був створений, натиснути кнопку Edit та перейти у вкладку Permissions. Тут потрібно налаштувати гнучкі права доступу локальним робочим станціям у підмережі 61, а саме Read/Write, а також для користувачів бездротових пристроїв – No Access.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		50

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкція з налаштування головного комутатора MikroTik CRS326-24G-2S+RM

Для налаштування VLAN у комутаторі MikroTik CRS326 є два шляхи, які залежать від обраної ОС. Для максимальної швидкості конфігурацію VLAN потрібно проводити через Bridge (в RouterOS) або через вкладку VLAN (в SwOS). Нижче розберемо налаштування через RouterOS.

Налаштування в RouterOS через Bridge являється сучасним та правильним, який задіє прискорення комутації (L2 HW offloading). Спочатку потрібно всі порти які задіяні у комутації об'єднати в один міст. Для цього виконуються команди:

```
/interface bridge
```

```
add name=bridge-main vlan-filtering=no
```

vlan-filtering=no вимикається тимчасово для збереження доступу до пристрою під час налаштування.

Наступним кроком є додавання портів до мосту. Нижче наведено команди для кожного із портів доступу:

```
/interface bridge port
```

```
add bridge=bridge-main interface=ether1 pvid=50 comment="Access to Gateway Server S_2"
```

```
add bridge=bridge-main interface=ether2 pvid=60 comment="Access for File Server S_1"
```

```
add bridge=bridge-main interface=ether10 pvid=60 comment="Access for WS_36"
```

```
add bridge=bridge-main interface=ether11 pvid=61 comment="Access for WS_37"
```

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		51

```
add bridge=bridge-main interface=ether12 pvid=61 comment="Access for WS_38"
```

```
add bridge=bridge-main interface=ether20 pvid=58 comment="Access for AP_1"
```

Також потрібно додати порти для комутаційного обладнання, які будуть працювати в режимі trunk:

```
add bridge=bridge-main interface=ether3 comment="Trunk to SW_1"
```

```
add bridge=bridge-main interface=ether4 comment="Trunk to SW_2"
```

```
add bridge=bridge-main interface=ether5 comment="Trunk to SW_3"
```

Наступним кроком потрібно створити VLAN таблицю. Необхідно вказати які порти є тегованими (tagged), а які нетегованими (untagged) для конкретного VLAN ID. Нижче наведено команди для створення цієї таблиці:

```
/interface bridge vlan
```

```
add bridge=bridge-main vlan-ids=50 tagged=bridge-main untagged=ether1
```

```
add bridge=bridge-main vlan-ids=51 tagged=bridge-main,ether3,ether4,ether5
```

```
add bridge=bridge-main vlan-ids=52 tagged=bridge-main,ether3,ether4,ether5
```

```
add bridge=bridge-main vlan-ids=53 tagged=bridge-main,ether4
```

```
add bridge=bridge-main vlan-ids=54 tagged=bridge-main,ether4
```

```
add bridge=bridge-main vlan-ids=55 tagged=bridge-main,ether4
```

```
add bridge=bridge-main vlan-ids=56 tagged=bridge-main,ether5
```

```
add bridge=bridge-main vlan-ids=57 tagged=bridge-main,ether5
```

```
add bridge=bridge-main vlan-ids=58 tagged=bridge-main,ether3,ether4,ether5 untagged=ether20
```

```
add bridge=bridge-main vlan-ids=59 tagged=bridge-main,ether5
```

```
add bridge=bridge-main vlan-ids=60 tagged=bridge-main,ether3,ether4,ether5 untagged=ether2,ether10
```

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

```
add bridge=bridge-main vlan-ids=61 tagged=bridge-  
main,ether3,ether4,ether5 untagged=ether11,ether12
```

Далі після перевірки налаштувань потрібно увімкнути фільтрацію VLAN для ізоляції трафіку. Це реалізується командою:

```
/interface bridge set bridge-main vlan-filtering=yes
```

Далі потрібно активувати інтерфейси маршрутизації L3-рівня та призначити ір-адреси внутрішніх шлюзів компанії. Першим кроком являється реєстрація віртуальних інтерфейсів маршрутизації для кожної із підмереж:

```
/interface vlan
```

```
add interface=bridge-main name=vlan50-transit vlan-id=50
```

```
add interface=bridge-main name=vlan51-int vlan-id=51
```

```
add interface=bridge-main name=vlan52-int vlan-id=52
```

```
add interface=bridge-main name=vlan53-int vlan-id=53
```

```
add interface=bridge-main name=vlan54-int vlan-id=54
```

```
add interface=bridge-main name=vlan55-int vlan-id=55
```

```
add interface=bridge-main name=vlan56-int vlan-id=56
```

```
add interface=bridge-main name=vlan57-int vlan-id=57
```

```
add interface=bridge-main name=vlan58-int vlan-id=58
```

```
add interface=bridge-main name=vlan59-int vlan-id=59
```

```
add interface=bridge-main name=vlan60-int vlan-id=60
```

```
add interface=bridge-main name=vlan61-int vlan-id=61
```

Після чого потрібно призначити IP-адреси шлюзів компанії:

```
/ip address
```

```
add address=192.168.50.1/30 interface=vlan50-transit  
comment="Транзитний IP для зв'язку з S_2"
```

```
add address=192.168.51.1/24 interface=vlan51-int comment="Шлюз  
Розробка"
```

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		53

```
add address=192.168.52.1/24 interface=vlan52-int comment="Шлюз  
Дизайн"
```

```
add address=192.168.53.1/24 interface=vlan53-int comment="Шлюз бізнес-  
аналіз"
```

```
add address=192.168.54.1/24 interface=vlan54-int comment="Шлюз Кадри"
```

```
add address=192.168.55.1/24 interface=vlan55-int comment="Шлюз  
Фінанси"
```

```
add address=192.168.56.1/24 interface=vlan56-int comment="Шлюз  
Маркетинг"
```

```
add address=192.168.57.1/24 interface=vlan57-int comment="Шлюз  
Тестування"
```

```
add address=192.168.58.1/24 interface=vlan58-int comment="Шлюз Wi-Fi  
Мережа"
```

```
add address=192.168.59.1/24 interface=vlan59-int comment="Шлюз  
Адміністрація"
```

```
add address=192.168.60.1/24 interface=vlan60-int comment="Шлюз  
Серверна та NAS S_1"
```

```
add address=192.168.61.1/24 interface=vlan61-int comment="Шлюз  
Рецепція"
```

Оскільки комутатор володіє повної інформацією про всі локальні підмережі, але не має доступу до зовнішнього світу, у його системну таблицю маршрутизації потрібно вказати маршрут за замовчуванням:

```
/ip route add gateway=192.168.50.2 comment="Default Route to S_2 Internet  
Gateway"
```

І останнім кроком є конфігурування DHCP-серверів для динамічних сегментів мережі. Комутатор для підвищення безпеки та оптимізації видає клієнтам параметри шлюзу самого на себе, а DNS-сервер примусово вказує адресу сервера S_2, на якому розгорнуто службу dnsmasq. Діапазон адрес

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		54

пулів розпочинаються з десятого хоста, залишаючи перші адреси зарезервовані під статичні потреби підприємства:

1. Визначення пулів адрес для динамічних підмереж

```
/ip pool
```

```
add name=pool-vlan58 ranges=192.168.58.10-192.168.58.254
```

```
add name=pool-vlan61 ranges=192.168.61.10-192.168.61.254
```

2. Конфігурування мережевих параметрів (Видача локального шлюзу та DNS-сервера S_2)

```
/ip dhcp-server network
```

```
add address=192.168.58.0/24 dns-server=192.168.50.2  
gateway=192.168.58.1 comment="Параметри мережі Wi-Fi"
```

```
add address=192.168.61.0/24 dns-server=192.168.50.2  
gateway=192.168.61.1 comment="Параметри мережі VLAN 61"
```

3. Активація служб DHCP-сервера на відповідних інтерфейсах

```
/ip dhcp-server
```

```
add address-pool=pool-vlan58 interface=vlan58-int name=server-vlan58  
disabled=no
```

```
add address-pool=pool-vlan61 interface=vlan61-int name=server-vlan61  
disabled=no
```

3.2.2 Інструкція з налаштування комутаторів робочих груп MikroTik CSS318-16G-2S+IN

Розглянемо приклад налаштування комутатора sw_1. Решта комутаторів налаштовуються аналогічно.

Комутатор MikroTik CSS318 працює під системою SwOS, тому для його налаштування потрібно перейти у браузері по його IP-адресі, після чого у вкладку VLAN. Далі для Port 1-8 встановити значення параметру VLAN Mode – strict, VLAN Receive – only untagged, а значення Default VLAN ID ввести

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		55

номер підмережі – 51. На рисунку 3.8 зображено зовнішній вигляд вкладки VLAN.

Port	VLAN Mode	VLAN Receive	Default VLAN ID	Force VLAN ID
Port1	strict	only untagged	51	<input type="checkbox"/>
Port2	strict	only untagged	51	<input type="checkbox"/>
Port3	strict	only untagged	51	<input type="checkbox"/>
Port4	strict	only untagged	51	<input type="checkbox"/>
Port5	strict	only untagged	51	<input type="checkbox"/>
Port6	strict	only untagged	51	<input type="checkbox"/>
Port7	strict	only untagged	51	<input type="checkbox"/>
Port8	strict	only untagged	51	<input type="checkbox"/>
Port9	strict	only untagged	52	<input type="checkbox"/>
Port10	strict	only untagged	52	<input type="checkbox"/>

Рисунок 3.8 – Зовнішній вигляд вкладки VLAN в SwOS

Для наступної підмережі всі параметри виставляються такі ж, окрім Default VLAN ID, у який потрібно ввести значення наступної підмережі – 52.

Також потрібно параметри порту для з’єднання з центральним комутатором, у нашому випадку це порт під номером 15. Потрібно виставити наступні параметри: VLAN Mode – enable, VLAN Receive – only tagged та Default VLAN ID – 1.

Наступним кроком є налаштування у вкладці VLANs. Потрібно натиснути кнопку “Append” 2 рази, щоб додати 2 рядки, тоді у 1 рядку в параметрах виставити наступні значення: VLAN ID – 51, Port Isolation та Learning – включити, а також у Members позначити галочками порти які використовуються саме для цієї підмережі. Для другого рядка параметри аналогічні, крім VLAN ID – 52 та Members наступні порти після обраних у 1 рядку. Зовнішній вигляд вкладки VLANs зображено на рисунку 3.9.

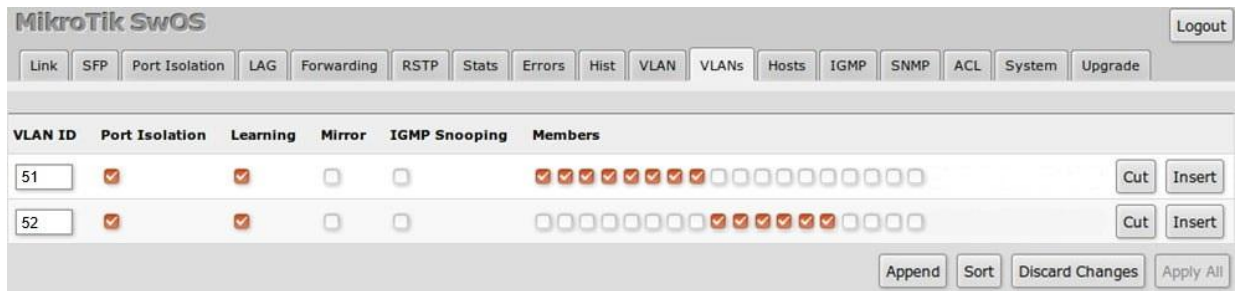


Рисунок 3.9 – Зовнішній вигляд вкладки VLANs в SwOS

Обов’язково після закінчення налаштування натиснути кнопку “Apply All” для збереження конфігурації.

3.2.3 Інструкція з налаштування безпроводного маршрутизатора MikroTik sAP ax

Цей маршрутизатор використовує операційну систему RouterOS, що дозволяє виконувати його налаштування за допомогою CLI.

Спочатку потрібно налаштувати профіль безпеки та пароль для бездротової мережі:

```
/interface wifi security
```

```
add name=sec-webtop passphrase="WebTop2026" authentication-
types=wpa2-psk,wpa3-psk
```

За необхідністю можливо замінити пароль для доступу змінивши значення параметру “passphrase”.

Далі необхідно створити загальну конфігурацію бездротової мережі (Ім’я мережі SSID):

```
/interface wifi configuration
```

```
add name=cfg-webtop ssid="WebTop_Wi-Fi" security=sec-webtop
```

Застосування конфігурації на фізичні радіоінтерфейси та їх увімкнення:

```
/interface wifi
```

```
set wifi1 configuration=cfg-webtop disabled=no comment="Радіомодуль 5 GHz"
```

```
set wifi2 configuration=cfg-webtop disabled=no comment="Радіомодуль 2.4 GHz"
```

Створення комутаційного мосту (Bridge) для об'єднання локальних інтерфейсів:

```
/interface bridge
```

```
add name=bridge-wifi vlan-filtering=no
```

Додавання фізичного порту та бездротових точок до єдиного мосту:

```
/interface bridge port
```

```
add bridge=bridge-wifi interface=ether1 comment="Вхідний кабель від SW_4"
```

```
add bridge=bridge-wifi interface=wifi1 comment="Клієнти 5 GHz"
```

```
add bridge=bridge-wifi interface=wifi2 comment="Клієнти 2.4 GHz"
```

Запуск DHCP-клієнта на мосту для отримання IP-адреси в підмережі VLAN 58:

```
/ip dhcp-client
```

```
add interface=bridge-wifi disabled=no comment="Отримання IP від комутатора SW_4"
```

3.3 Інструкція з використання тестових наборів та програм

Для перевірки та тестування мережі використовуються як апаратні, так і програмні засоби діагностики. Апаратні засоби застосовують для перевірки кабельного сегменту мережі, тоді як програмні – для аналізу параметрів мережевих з'єднань та доступу до вузлів мережі.

В ОС Windows до основних програмних засобів відносять наступні утиліти:

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

- ipconfig – використовується для відображення поточної конфігурації TCP/IP, а саме IP-адреса, маска підмережі та шлюз за замовчуванням.

- tracert – використовується для визначення шляху проходження пакету до віддаленого вузла мережі.

- ping – призначена для визначення часу передачі пакетів та доступності мережевих вузлів.

- netstat – надає можливість перегляду активних мережевих з'єднань та статистику протоколів TCP/IP.

- route – призначена для перегляду та редагування таблиці маршрутизації мережі.

- iPerf3 – утиліта для вимірювання пропускну здатності мережі. Дозволяє визначити максимальну швидкість передачі даних між двома вузлами мережі, а також перевірити стабільність каналу зв'язку.

Тестування мережі відбувається у 2 основні етапи. Першим етапом є перевірка кабельного зв'язку за допомогою тестера. Під час перевірки визначається правильність обтискання кабелю, відсутність коротких замикань та обривів.

Другим етапом є програмне тестування мережі за допомогою утиліт ОС Windows. Під час тестування потрібно перевірити правильність мережевих налаштувань, працездатність серверів, комутаторів та робочих станцій, а ще наявність мережевого з'єднання між вузлами мережі.

3.4 Інструкція з експлуатації та моніторингу в мережі

Експлуатація комп'ютерної мережі охоплює широкий спектр заходів, спрямованих на забезпечення її безперебійного функціонування та своєчасне виявлення можливих збоїв. Для підвищення надійності мережевої інфраструктури необхідно використовувати джерела безперебійного

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		59

живлення. Вони гарантують коректну роботу таких критичних компонентів, як комутатори, маршрутизатори й сервери, у випадку раптового відключення електроенергії. Це запобігає втраті даних та аварійному завершенню роботи систем, що є особливо важливим для ключових вузлів мережі. Крім того, доцільно застосовувати засоби захисту від перенапруги, які мінімізують ризик пошкодження обладнання через коливання електричної напруги.

У ході експлуатації мережі важливо регулярно здійснювати контроль її працездатності. Для цього використовуються кабельні тестери, що дають змогу перевіряти якість монтажу та цілісність ліній зв'язку, а також програмні утиліти для діагностики мережевих протоколів, вузлів і каналів передачі даних. Оперативне виявлення проблемних ділянок і їхнє усунення до того, як вони можуть спричинити серйозні порушення у роботі, стає можливим завдяки таким інструментам. Ще одним важливим елементом є впровадження систем моніторингу, які забезпечують централізований збір інформації про стан обладнання, ступінь завантаження каналів зв'язку та використання ресурсів. Такі системи дають адміністратору змогу отримувати всебічну картину мережевих процесів у реальному часі та оперативно реагувати на будь-які відхилення від нормальної роботи.

Технічне обслуговування мережі передбачає проведення регулярних оглядів обладнання, контроль температурного режиму та ефективності роботи систем охолодження, а також виконання профілактичного очищення від пилу. Особливу увагу слід приділяти оновленню програмного забезпечення мережевих пристроїв і серверів, адже це сприяє ліквідації можливих вразливостей та підтримці їх сумісності з актуальними стандартами. Налаштування маршрутизаторів і комутаторів повинні регулярно зберігатися у вигляді резервних копій. Це дозволяє швидко відновити їхню роботу у разі виходу з ладу. Також доцільним є ведення детального журналу подій та несправностей для аналізу причин збоїв і

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		60

планування превентивних заходів, спрямованих на оптимізацію роботи мережі.

Таким чином, правильно складені інструкції з експлуатації та моніторингу є невід'ємною частиною управління мережею. Використання джерел безперебійного живлення, кабельних тестерів, діагностичних програм та сучасних систем моніторингу дозволяє ефективно визначати й усувати проблеми на ранніх етапах. Це сприяє підтримці високого рівня надійності та безпеки корпоративної мережевої інфраструктури.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		61

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проєкту комп'ютерної мережі компанії "WebTop" і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно дані витрат часу по окремих операціях технологічного процесу звести у таблицю. Виконавцями стадій технологічного процесу будуть: керівник проєкту, інженер, технік. В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1	Узгодження з замовником місць підключення	Інженер	3
2	Розробка схеми локальної комп'ютерної мережі	Інженер	12

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		62

Продовження таблиці 4.1

1	2	3	4
3	Вибір мережевого обладнання та матеріалів	Інженер	6
4	Прокладання кабельних трас та монтаж коробів	Технік	16
5	Прокладання кабелю	Технік	17
6	Монтаж інформаційних розеток	Технік	8
7	Монтаж комутаційної панелі та організація кабелів у шафі	Технік	7
8	Встановлення та підключення комутаторів і маршрутизатора	Інженер	6
9	Обтискання та тестування кабельних ліній	Технік	8
10	Налаштування мережевого обладнання	Інженер	13
11	Перевірка працездатності мережі та усунення несправностей	Керівник	7
12	Оформлення технічної документації	Інженер	9
	Разом		112

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		63

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого власником підприємства працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів роботи підприємства, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою 4.1:

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

де, T_c – тарифна ставка, грн.; K_r – кількість відпрацьованих годин.

Основна заробітна плата становить:

1. Керівник проєкту: $Z_{осн1} = 259 \cdot 7 = 1813$ грн.;
2. Інженер: $Z_{осн2} = 208 \cdot 49 = 10192$ грн.;
3. Технік: $Z_{осн3} = 155 \cdot 56 = 8680$ грн.

Сумарна основна заробітна плата становить:

$$Z_{осн} = 1813 + 10192 + 8680 = 20685 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

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

де $K_{дод.}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проєкту: $Z_{дод1} = 1813 \cdot 0,11 = 199,43$ грн.;
2. Інженер: $Z_{дод2} = 10192 \cdot 0,11 = 1121,12$ грн.;
3. Технік: $Z_{дод3} = 8680 \cdot 0,11 = 954,8$ грн.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		64

Сумарна додаткова заробітна плата становить:

$$Z_{\text{дод}} = 199,43 + 1121,12 + 954,8 = 2275,35 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($V_{\text{о.п.}}$) визначаються за формулою:

$$V_{\text{о.п.}} = Z_{\text{осн.}} + Z_{\text{дод.}}, \quad (4.3)$$

$$V_{\text{о.п.}} = 20685 + 2275,35 = 22960,35 \text{ грн.}$$

Крім того, слід визначити суму нарахування на заробітну плату:

- єдиний соціальний внесок – 22 %;

Отже, сума нарахувань на заробітну плату буде становити:

$$V_{\text{с.з.}} = \text{ФОП} \cdot 0,22, \quad (4.4)$$

де, ФОП – фонд оплати праці, грн.

$$V_{\text{с.з.}} = 22960,35 \cdot 0,22 = 5051,27 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тарифна ставка, грн	К-сть відпра цьов. год.	Фактично нарах. з/пл., грн.			
1	2	3	4	5	6	7	8
1.	Інженер	208	49	10192	1121,12	-	-

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		65

Продовження таблиці 4.2

1	2	3	4	5	6	7	8
2.	Технік	155	56	8680	954,8	-	-
3.	Керівн ик	259	7	1813	199,43	-	-
Разом				20685	2275,35	5051,27	28011,62

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються за формулою 4.5 як добуток кількості витрачених матеріалів та їх ціни:

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

де q_i – кількість витраченого матеріалу i -го виду; p_i – ціна матеріалу i -го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

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

Проведені розрахунки занесемо у таблиці 4.3.

Таблиця 4.3 – Матеріальні витрати

№ п/п	Матеріальний ресурс	Од. виміру	Кількість	Ціна 1-ці, грн	Загальна сума, грн
1	2	3	4	5	6
1.	Комутаційна шафа 12U	шт.	1	11000	11000

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		66

Продовження таблиці 4.3

1	2	3	4	5	6
2.	Патчпанель 24 порти, категорія 5е.	шт.	1	1500	1500
3.	Розетка RJ-45 (категорія 5е)	шт.	38	130	4 940
4.	Кабель UTP(cat.5е)	м.	205	28	5 740
5.	Патчкорди(cat.5е)	шт.	9	75	675
6.	Короб	м.	50	110	5 500
7.	Жорсткий диск 8TB 3.5" 5640 256MB SATA RedPlus NAS WD	шт.	4	17 800	71 200
8.	MikroTik CRS326-24G-2S+RM	шт.	1	9 000	9 000
9.	Конектор Cablexpert RJ-45 Cat.5E 8P8C PLUG3UP6(50шт.)	шт.	2	165	330
10.	MikroTik CSS318-16G-2S+IN	шт.	3	6 000	18 000
11.	MikroTik cAPax	шт.	1	5 500	5 500

Арк.

2026.КВР.123.406.12.00.00 ПЗ

67

Змн.

Арк.

№ докум.

Підпис

Дата

Продовження таблиці 4.3

1	2	3	4	5	6
12.	Synology DS923+	шт.	1	36 000	36 000
13.	HPE ProLiant DL380 Gen11	шт.	1	520 000	520 000
Разом					689 385

Проведені розрахунки показали, що загальна сума матеріальних витрат становить 689 385 грн, що підтверджує необхідність їх врахування у кошторисі.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою 4.7:

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

де W – необхідна потужність, кВт; T – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 40 години, споживана потужність - 0,5 кВт/год., вартість 1 кВт електроенергії – 15,94 грн. Тому витрати на електроенергію будуть становити:

$$Z_e = 0,5 \cdot 40 \cdot 15,94 = 319 \text{ грн.}$$

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		68

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8–10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

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

де $T_{\text{в}}$ – транспортні витрати.

Виконаємо обчислення:

$$T_{\text{в}} = 689\,385 \cdot 0,09 = 62044,65 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Для визначення амортизаційних відрахувань застосовуємо формулу 4.9:

$$A = \frac{B_{\text{в}} \cdot N_{\text{А}}}{100\%} \cdot T, \quad (4.9)$$

де, A - амортизаційні відрахування за звітний період, грн.; $B_{\text{в}}$ - балансова вартість групи основних фондів на початок звітного періоду, грн.; $N_{\text{А}}$ - норма амортизації, %; T - фактична кількість відпрацьованих годин.

Враховуючи, що ПК використовується при роботі над даним проектом 40 год., балансова вартість ПК – 27600 грн., тому:

$$A = \frac{27600 \cdot 0,04}{150} \cdot 40 = 368 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		69

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$H_v = B_{o.l.} \cdot 0,2 \dots 0,6, \quad (4.10)$$

де H_v – накладні витрати.

$$H_v = 22960,35 \cdot 0,3 = 6888,1 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4, де зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	22960,35	3
Відрахування на соціальні заходи	5051,27	0,7

Продовження таблиці 4.4

1	2	3
Матеріальні витрати	689385	87,5
Витрати на електроенергію	319	0,05
Транспортні витрати	62044,65	7,8
Амортизаційні відрахування	368	0,05
Накладні витрати	6888,1	0,9
Собівартість	787016,37	100

Собівартість (C_B) НДР розрахуємо за формулою 4.11:

$$C_B = B_{o.n.} + B_{e.z.} + Z_{m.v.} + Z_e + T_e + A + H, \quad (4.11)$$

Собівартість дорівнює $C_B = 787016,37$ 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; ПДВ – ставка податку на додану вартість.

Підставимо наші значення у формулу та отримаймо результат:

$$Ц = 787016,37 \cdot (1 + 0,25) \cdot (1 + 0,2) = 1180524,55 \text{ грн.}$$

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		71

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності ($T_{ок}$), який можна визначити за формулою 4.13.

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

де K_B – затрати на проект; $\Gamma_{П}$ – грошовий потік за t – ий рік; t – відповідний рік роботи; i - величина дисконтної ставки (10...15%).

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

$$ЧТВ = -787016,37 + \frac{716318,28}{(1+0,1)} + \frac{716318,28}{(1+0,1)^2} = 456180,64$$

Термін окупності визначається за формулою 4.14:

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

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.

$$T_{ок} = 1 + \frac{122738,32}{716318,28} = 1,2$$

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

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
						72
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1	Собівартість, грн.	787016,37
2	Плановий прибуток, грн.	386 968,28
3	Ціна, грн.	1 180 524,55
4	Чиста теперішня вартість, грн.	456180,64
5	Термін окупності, рік	1,2

Загальна вартість розробленого проекту мережі компанії “WebTop” становить 1180524,55 грн. Термін окупності становить 1,2 роки.

					2026.КВР.123.406.12.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		73

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Розслідування та облік аварій на виробництві

Охорона праці є невід'ємною складовою будь-якої виробничої діяльності. У контексті функціонування компанії «WebTop», яка надає послуги в галузі інформаційних технологій та мережевої інфраструктури, питання безпечної організації праці набувають особливої ваги. Серед ключових аспектів охорони праці — своєчасне та правильне розслідування і облік аварій, що дозволяє мінімізувати ризики повторних подій та захистити здоров'я і життя працівників.

Правовою основою для розслідування та обліку аварій на виробництві в Україні є Закон України «Про охорону праці» (стаття 22), а також Порядок розслідування та обліку нещасних випадків, професійних захворювань та аварій на виробництві, затверджений постановою Кабінету Міністрів України від 17 квітня 2019 року № 337 (зі змінами, внесеними постановою від 27.12.2024 № 1542) [16, 20].

Відповідно до зазначеного Порядку, виробнича аварія — це раптова подія, що сталася на підприємстві або на підконтрольній йому території й призвела до загибелі або травмування людей, руйнування або пошкодження виробничих об'єктів, транспортних засобів, будівель, споруд, комунікацій та/або завдала матеріальних збитків [20].

Аварії класифікуються за двома категоріями:

- аварії I категорії — ті, внаслідок яких: загинуло п'ять або більше осіб, або травмовано десятьох і більше осіб; відбувся викид небезпечних речовин за межі санітарно-захисної зони; виникла загроза для значної кількості людей або для навколишнього природного середовища;

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		74

- аварії II категорії — ті, внаслідок яких: загинуло від одного до чотирьох осіб, або травмовано від чотирьох до дев'яти осіб; виникла загроза для працівників цеху чи дільниці; підприємство зупинено або виведено з ладу на зміну і більше.

Відповідно до статті 22 Закону України «Про охорону праці» та Порядку № 337, про аварію роботодавець або особа, яка керує виробництвом під час зміни, зобов'язані негайно повідомити: територіальний орган Держпраці; орган управління або наглядову раду підприємства; місцеву державну адміністрацію; територіальний орган ДСНС; відповідний підрозділ поліції; профспілковий орган; у разі травмування або загибелі — робочий орган Фонду соціального страхування [20].

Розслідування аварій здійснюється спеціально призначеними комісіями:

- аварія I категорії розслідується комісією, яку очолює представник центрального органу виконавчої влади або Держпраці;

- аварія II категорії розслідується комісією на чолі з представником органу, до сфери управління якого належить підприємство, або районної державної адміністрації, за узгодженням з відповідним органом нагляду за охороною праці.

Комісія з розслідування зобов'язана протягом десяти робочих днів розслідувати аварію, скласти акт встановленої форми (Н-5), визначити розмір завданих збитків і запропонувати заходи щодо запобігання подібним подіям.

Згідно з вимогами Порядку № 337, роботодавець та особа, яка керує виробництвом під час зміни, зобов'язані діяти відповідно до плану локалізації та ліквідації аварій, вжити першочергових заходів для рятування потерпілих і надання їм домедичної допомоги, локалізації аварії, встановлення меж небезпечної зони та обмеження доступу до неї людей, а також зберегти до прибуття комісії обстановку на місці події.

Облік аварій здійснюється підприємством у спеціальному журналі із зазначенням: причин події, розміру економічних втрат, тривалості простою,

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		75

запропонованих комісією заходів. Акт розслідування аварій I і II категорій направляється центральним органам державної виконавчої влади за їх вимогою. Один примірник акту розслідування аварії, яка спричинила нещасний випадок, зберігається на підприємстві не менше двох років.

Для компанії «WebTop» особливого значення набувають аварії, пов'язані з відмовами мережевої інфраструктури, серверного обладнання та систем електропостачання. Хоча такі події зазвичай не несуть прямої загрози здоров'ю персоналу, вони можуть призвести до матеріальних збитків та порушення технологічних процесів. Тому компанія зобов'язана мати розроблений план локалізації та ліквідації аварій, а також проводити своєчасне розслідування і облік будь-яких виробничих інцидентів відповідно до чинного законодавства.

5.2 Інженерні заходи щодо зниження рівня акустичного шуму на робочих місцях персоналу компанії «WebTop»

Акустичний шум є одним із ключових шкідливих виробничих факторів на підприємствах будь-якої галузі, в тому числі в ІТ-компаніях. Серверне обладнання, система охолодження, комп'ютерна техніка та вентиляційні установки формують постійний фоновий шум у приміщеннях компанії «WebTop», що може негативно позначатись на здоров'ї та продуктивності інженерів мережі.

В Україні нормування виробничого шуму регулюється такими нормативними документами:

- ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку» — основний нормативний акт, що встановлює допустимі рівні звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях [15];

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		76

- Державні санітарні норми допустимих рівнів шуму в приміщеннях житлових та громадських будинків і на території житлової забудови (наказ МОЗ від 22.02.2019 № 463) [14];

- ДСТУ 2867 та ДБН В.1.1-31:2013 «Захист територій, будинків і споруд від шуму», які регламентують оцінку шумового навантаження та акустичний розрахунок будівельно-конструктивних рішень.

Відповідно до ДСН 3.3.6.037-99, допустимий рівень шуму на постійних робочих місцях у виробничих приміщеннях та на території підприємства становить 80 дБА [15]. Для офісних приміщень, обладнаних персональними комп'ютерами або іншою офісною технікою, допустимий рівень шуму встановлений на рівні 50 дБА (постійний рівень), максимальний — 65 дБА [14]. Таким чином, робочі місця інженерів мережі «WebTop», розташовані в офісних приміщеннях, повинні відповідати саме цим вимогам.

Джерелами шуму в приміщеннях компанії «WebTop» є:

- серверне та мережеве обладнання (сервери, комутатори, маршрутизатори, системи безперебійного живлення) з їх системами охолодження;

- персональні комп'ютери та ноутбуки з вентиляторами охолодження;

- системи кондиціонування і вентиляції;

- технологічне обладнання суміжних приміщень;

- зовнішній шум із вулиці та сусідніх будівель.

Для зниження рівня акустичного шуму на робочих місцях застосовуються такі інженерні заходи [15]:

1. Зниження шуму у джерелі його виникнення:

Вибір менш шумного обладнання з нижчими рівнями акустичного випромінювання (наприклад, серверні блоки та комутатори з характеристиками шуму не вище 45–50 дБА). Застосування вентиляторів із

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		77

зниженою кількістю обертів та систем рідинного охолодження для серверного обладнання. Своєчасне технічне обслуговування обладнання (заміна зношених підшипників, мастило рухомих деталей).

2. Звукоізоляція та звукопоглинання:

Розміщення серверних стійок у виокремленому серверному приміщенні з підвищеним рівнем звукоізоляції — звуконепроникними стінами, дверима та підлогою. Використання акустичних кожухів, корпусів і екранів для найгучнішого обладнання. Облицювання стін, стелі і підлоги серверних та технічних приміщень звукопоглинаючими матеріалами (мінераловатні плити, акустичні панелі з перфорованого металу тощо). Установка глушників у системах вентиляції та кондиціонування.

3. Планувальні та архітектурні рішення:

Розташування найгучнішого обладнання якомога далі від робочих місць персоналу. Улаштування подвійних акустичних дверей між серверним приміщенням і офісним простором. Використання підвісних акустичних стель та перегородок із звукопоглинаючим наповнювачем для розподілу відкритого офісного простору.

4. Вібраційна ізоляція:

Установка обладнання на антивібраційних фундаментах, гумових підкладках та пружинних амортизаторах для зменшення структурного шуму, що передається через конструкції будівлі.

5. Організаційні та технічні заходи:

Встановлення раціонального режиму роботи для шумного обладнання. Скорочення часу перебування персоналу поруч із джерелами шуму. Надання засобів індивідуального захисту (беруші, навушники) у випадках, коли інших заходів недостатньо для досягнення допустимих рівнів.

Ефективність запроваджених заходів перевіряється шляхом інструментального вимірювання рівнів шуму на робочих місцях із використанням шумомірів класу точності 1 або 2 (відповідно до ДСТУ 2867).

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		78

Результати вимірювань порівнюються з нормованими значеннями, встановленими ДСН 3.3.6.037-99 [7]. Вимірювання повинні проводитись не рідше одного разу на рік, а також після введення в дію нового обладнання або після суттєвого реконструювання приміщень.

Для проведення точної порівняльної оцінки ефективності впроваджуваних архітектурно-планувальних рішень та звукоізолювальних конструкцій використовуються стандартні методики інженерних акустичних розрахунків[2]. Комплекс запропонованих інженерних заходів дозволяє знизити рівень акустичного шуму в офісних зонах компанії «WebTop» до нормативних значень, що забезпечить комфортні та безпечні умови праці для всього персоналу.

5.3 Організація системи управління охороною праці та проведення інструктажів для інженерів мережі в компанії «WebTop»

Ефективна охорона праці в компанії «WebTop» базується на функціонуванні системи управління охороною праці (СУОП) — комплексного механізму організаційних, технічних та нормативних заходів, спрямованих на запобігання травматизму, профзахворюванням і аваріям. Правовою основою для створення та функціонування СУОП є Закон України «Про охорону праці» [16] та НПАОП 0.00-4.21-04 «Типове положення про систему управління охороною праці».

Система управління охороною праці (СУОП) — це частина загальної системи управління організацією, яка сприяє запобіганню нещасним випадкам та професійним захворюванням на виробництві, а також небезпеки для третіх осіб, що виникають у процесі господарювання, і включає в себе комплекс взаємопов'язаних заходів спрямованих на виконання вимог законодавчих та нормативно-правових актів з охорони праці [22]. Управлінська діяльність у межах СУОП базується на циклічному підході, що

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		79

включає безперервне планування, організацію практичних заходів, контроль та оперативне коригування виявлених невідповідностей [1, 2].

Суб'єктом управління в СУОП на підприємстві є керівник, а у відповідних підрозділах — керівники структурних підрозділів та служб. Об'єктом управління є умови праці, виробниче середовище та рівень безпеки технологічних процесів [21].

Функціонування СУОП у компанії «WebTop» забезпечується через:

- створення служби охорони праці або призначення відповідального спеціаліста (залежно від чисельності персоналу);
- затвердження Положення про СУОП та посадових інструкцій з питань безпеки для кожної категорії посад;
- розробку та затвердження інструкцій з охорони праці для інженерів мережі;
- організацію навчання, перевірки знань та інструктажів із питань охорони праці;
- проведення внутрішнього аудиту охорони праці та атестації робочих місць;
- облік, аналіз та оцінку ризиків виникнення нещасних випадків і аварій;
- планування та реалізацію заходів щодо покращення умов праці [21, 22].

Основні елементи СУОП включають: запобіжні та контролюючі заходи щодо небезпеки та ризику; порядок попередження аварійних ситуацій, готовність до них і ліквідацію їх наслідків; процедури оцінки на відповідність вимогам безпеки; систему обліку, аналізу та оцінки ризиків; порядок розслідування нещасних випадків; систему перевірок (аудиту) з визначення ефективності; моніторинг виконання та оцінки результативності [22].

Інструктажі з охорони праці для інженерів мережі

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		80

Одним із ключових елементів СУОП є навчання та інструктажі персоналу. Відповідно до НПАОП 0.00-4.12-2005 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці», інструктажі за характером і часом проведення поділяються на п'ять видів [18]:

1. Вступний інструктаж проводиться спеціалістом служби охорони праці (або іншим відповідальним фахівцем за наказом керівника) з усіма новоприйнятими працівниками, незалежно від їх освіти, стажу та посади, а також з особами, які проходять виробничу практику або відрядженими. Для інженерів мережі «WebTop» вступний інструктаж охоплює: загальні вимоги безпеки, правила поведінки в офісі та на об'єктах мережевої інфраструктури, правила пожежної безпеки, порядок дій у надзвичайних ситуаціях [18].

2. Первинний інструктаж на робочому місці проводиться до початку самостійної роботи безпосереднім керівником (начальником відділу, керівником служби). Для інженерів мережі він включає: ознайомлення з конкретним робочим місцем, обладнанням, яке використовується, порядком роботи з активним мережевим обладнанням, правилами електробезпеки під час монтажу та обслуговування кабельних ліній, вимогами до роботи у серверних приміщеннях (контроль температури, вентиляція, піднімання важкого обладнання) [18].

3. Повторний інструктаж проводиться на робочому місці індивідуально або з групою працівників одного фаху. Для інженерів, які виконують роботи підвищеної небезпеки — не рідше одного разу на 3 місяці, для решти — не рідше одного разу на 6 місяців. Мета — відновлення та закріплення знань з охорони праці [18].

4. Позаплановий інструктаж проводиться у разі: введення нових або зміни чинних нормативних актів з охорони праці; зміни технологічного процесу або заміни чи модернізації обладнання; порушень працівниками

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		81

вимог НПАОП; перерви в роботі понад 30 календарних днів (для робіт підвищеної небезпеки) або понад 60 днів (для інших робіт); на вимогу органів нагляду або вищого керівництва [18].

5. Цільовий інструктаж проводиться з інженерами мережі перед виконанням разових та нетипових робіт: робіт із наряд-допуском (виконання електромонтажних робіт на висоті, монтаж в зонах з підвищеним ризиком), ліквідації аварій та надзвичайних ситуацій, виконання польових робіт на телекомунікаційних об'єктах. Зміст і обсяг цільового інструктажу визначаються залежно від виду виконуваних робіт [18].

Реєстрація інструктажів здійснюється у журналах встановленої форми: вступний інструктаж — у журналі реєстрації вступного інструктажу; первинний, повторний, позаплановий та цільовий — у журналі реєстрації інструктажів з питань охорони праці на робочому місці (форма визначена додатком 6 до Типового положення НПАОП 0.00-4.12-2005) [18].

Усі інструктажі, крім вступного, проводить безпосередній керівник робіт. Факт проведення інструктажу засвідчується підписами як інструктора, так і інструктованого.

Ефективна організація СУОП і системи інструктажів у компанії «WebTop» дозволяє: підтримувати належний рівень безпеки на робочих місцях інженерів мережі; своєчасно виявляти і усувати потенційні ризики; виконувати вимоги законодавства з охорони праці та уникати адміністративної відповідальності; сприяти формуванню культури безпеки серед персоналу компанії.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		82

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проєкт локальної обчислювальної мережі для офісного приміщення компанії «WebTop». У ході проєктування було впроваджено гібридну фізичну топологію, яка базується на ієрархічній зірці з використанням високошвидкісних магістральних Trunk-лінків. Провідний та бездротовий сегменти мережі побудовані з дотриманням сучасних мережевих стандартів, серед яких технологія високошвидкісної гігабітної передачі даних по мідному кабелю IEEE 802.3ab (1000Base-T), передовий бездротовий стандарт Wi-Fi 6 або IEEE 802.11ax, а також механізм логічного тегування трафіку IEEE 802.1Q.

Спроектовано логічну та фізичну топологію мережі підприємства/ Підібрано відповідне сучасне апаратне та програмне забезпечення, а при виборі активного обладнання враховано наявність гігабітних портів RJ-45 та закладено можливість горизонтального і вертикального масштабування локальної мережі в майбутньому. Описано процедуру детального налаштування активного обладнання через консольні інтерфейси CLI та спеціалізовані вебінтерфейси SwOS і DSM. Також розроблено покрокову технологічну інструкцію з тестування, моніторингу та налагодження мережі за допомогою системних утиліт діагностики. Логічна та фізична топології локальної мережі подані в графічній частині кваліфікаційної роботи.

В економічній частині роботи проведено техніко-економічне обґрунтування та здійснено детальний розрахунок повної вартості робіт із проєктування, закупівлі активного і пасивного заліза, монтажу СКС і запуску в експлуатацію корпоративної мережі.

Останній розділ роботи описує питання охорони праці, виробничої санітарії та техніки безпеки при розгортанні, монтажі та обслуговуванні засобів обчислювальної техніки та мережевого обладнання.

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		83

ПЕРЕЛІК ПОСИЛАНЬ

1. Охорона праці та цивільний захист / О. Г. Левченко, О. І. Полукаров, В. В. Зацарний, Ю. О. Полукаров, О. В. Землянська ; за ред. О. Г. Левченка. - К. : КПІ ім. Ігоря Сікорського, 2019. - 417 с.
2. Охорона праці в галузі / В. М. Курепін, Д. Д. Марченко, Д. В. Курепін. - М. : МНАУ, 2023. - 586 с.
3. ССМР [Електронний ресурс] - Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/ССМР> - Дата доступу: 10.04.2026
4. Digitus Шафа Wall Mounting Dynamic Basic, 19" 12U 600x450, RAL 9005 Bautools [Електронний ресурс] - Режим доступу до ресурсу: <https://prom.ua/ua/p2501728118-digitus-shkaf-wall.html> - Дата доступу: 12.04.2026
5. HPE ProLiant DL380 Gen11 Intel Xeon-S 4509Y 8-Core (2.60GHz 22.5MB) 32GB (1 x 32GB) 8 x SFF x1 U.3 BC MR408i-o 1000W [Електронний ресурс] - Режим доступу до ресурсу: <https://www.senetic.ua/product/P70456-421> - Дата доступу: 15.04.2026
6. IEEE 802.11 [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/IEEE_802.11 - Дата доступу: 09.04.2026
7. IEEE 802.11ax [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/IEEE_802.11ax - Дата доступу: 11.04.2026
8. MikroTik cAP ax (cAPGi-5НахD2НахD) [Електронний ресурс] - Режим доступу до ресурсу: <https://www.technotrade.com.ua/Products/MikroTik-cAP-ax.php> - Дата доступу: 15.04.2026
9. MikroTik CRS326-24G-2S+RM [Електронний ресурс] - Режим доступу до ресурсу: <https://www.technotrade.com.ua/Products/MikroTik-CRS326-24G-2SplusRM.php> - Дата доступу: 15.04.2026

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		84

10. MikroTik CSS318-16G-2S+IN [Електронний ресурс] - Режим доступу до ресурсу: <https://www.technotrade.com.ua/Products/MikroTik-CSS318-16G-2Splus-IN.php> - Дата доступу: 15.04.2026

11. NAS-сервер Synology DiskStation DS923+ [Електронний ресурс] - Режим доступу до ресурсу: <https://e-server.com.ua/uk/nas-server-synology-diskstation-ds923> - Дата доступу: 15.04.2026

12. Temporal Key Integrity Protocol [Електронний ресурс] - Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol - Дата доступу: 10.04.2026

13. Віртуальні локальні мережі (vlan). [Електронний ресурс] - Режим доступу до ресурсу: <https://studfile.net/preview/7012359/page:10/> - Дата доступу: 11.04.2026

14. Державні санітарні норми допустимих рівнів шуму в приміщеннях житлових та громадських будинків і на території житлової забудови : Наказ МОЗ України від 22.02.2019 № 463. [Електронний ресурс] - Режим доступу до ресурсу: <https://zakon.rada.gov.ua/go/z0281-19> - Дата доступу: 25.05.2026

15. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку». [Електронний ресурс] - Режим доступу до ресурсу: <https://zakon.rada.gov.ua/rada/show/va037282-99#Text> - Дата доступу: 25.05.2026

16. Закон України «Про охорону праці» від 14.10.1992 № 2694-ХІІ (зі змінами) [Електронний ресурс] - Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2694-12> - Дата доступу: 25.05.2026

17. Кабель комп'ютерний Одескабель UTP 8x0,51 КПВ-ВП (350) 4x2x0,51 (UTP-cat.5E) мідь. [Електронний ресурс] - Режим доступу до ресурсу: <https://epicentrk.ua/ua/shop/kabel-kompyuternyy-odeskabel-5ekat-utp-kpv-vp-350-4kh2kh0-51.html> - Дата доступу: 12.04.2026

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		85

18. НПАОП 0.00-4.12-2005 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці». [Електронний ресурс] - Режим доступу до ресурсу:

https://minio.kyivcity.gov.ua/kyivcity/sites/14/dokumentu/vidu_instruktojiiv.pdf -

Дата доступу: 26.05.2026

19. Патч-панель DIGITUS 19" 1U, 24 порти, 5e UTP в зборі [Електронний ресурс] - Режим доступу до ресурсу: <https://e-server.com.ua/uk/patch-paneli/patch-paneli-utp-uk/patch-panel-digitus-19-1u-24-porti-5e-utp-v-zbori-detail> -

Дата доступу: 12.04.2026

20. Постанова Кабінету Міністрів України «Про затвердження Порядку розслідування та обліку нещасних випадків, професійних захворювань та аварій на виробництві» від 17.04.2019 № 337 (зі змінами від 27.12.2024 № 1542). [Електронний ресурс] - Режим доступу до ресурсу:

<https://zakon.rada.gov.ua/laws/show/337-2019-%D0%BF> - Дата доступу:

25.05.2026

21. Система управління охороною праці підприємства. Тема 2 : методичні матеріали / Академія гірничих наук. [Електронний ресурс] - Режим доступу до ресурсу:

https://aop.nmu.org.ua/ua/metodicki/specialist/opg/lzi/%D0%A2%D0%B5%D0%BC%D0%B02_%D0%A1%D0%A3%D0%9E%D0%9F.pdf - Дата доступу:

26.05.2026

22. Система управління охороною праці (СУОП) // Інформаційний портал Сумської міської ради. [Електронний ресурс] - Режим доступу до ресурсу:

<https://smr.gov.ua/en/2016-03-14-08-10-17/informatsijni-materiali/informatsijni-materiali-z-pitan-sotszakhistu/13708-cistema-upravlinnya-okhoronoyu-pratsi-suop.html> - Дата доступу: 26.05.2026

23. Тестер кабелю Fluke Networks MicroScanner™ (MS2-KIT) [Електронний ресурс] - Режим доступу до ресурсу:

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		86

<https://masteram.com.ua/uk/fluke-networks-microscanner-ms2-kit-2772451/> -

Дата доступу: 18.04.2026

					<i>2026.КВР.123.406.12.00.00 ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		87