Форма № Н-9.02

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі ТОВ "Внутрішні інженерні системи"**

Виконав: студент IV курсу, групи КІ-406

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

Роман ВОЛЯНСЬКИЙ

(ім'я та прізвище)

Керівник Володимир ШТОКАЛО

(ім'я та прізвище)

Рецензент

(ім'я та прізвище)

Тернопіль – 2026

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

Відділення **інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **фаховий молодший бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"30" березня 2026 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Волянському Роману Володимировичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі ТОВ "Внутрішні інженерні системи"**

керівник роботи Штокало Володимир Ярославович
(прізвище, ім'я, по батькові)

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

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

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

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	31.03	
2	Збір і узагальнення інформації	08.05	
3	Написання першого розділу	15.05	
4	Розробка технічного та робочого проекту	22.05	
5	Написання спеціального розділу	28.05	
6	Розрахунок економічної частини	1.06	
7	Написання розділу охорони праці	3.06	
8	Виконання графічної частини	8.06	
9	Оформлення проєкту	10.06	
10	Погодження нормоконтролю	11.06	
11	Попередній захист роботи	12.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 31 березня 2026 року

Студент _____ Роман ВОЛЯНСЬКИЙ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Володимир ШТОКАЛО
(підпис) ім'я та прізвище)

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

FTP (File Transfer Protocol) - протокол передачі файлів;

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту;

IDENT (Indentification Protocol) - протокол ідентифікації;

IP (Internet Protocol) – Інтернет-протокол;

ISP (Internet Service Provider) - провайдер доступу в Інтернет;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

NAT (Network Address Translation) – мережева трансляція адес;

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;

ОС - операційна система.

ВСТУП

У сучасному світі, де інформаційні технології стрімко розвиваються, комп'ютерні мережі стали невід'ємною частиною функціонування будь-якого підприємства. Локальні комп'ютерні мережі сприяють оперативному обміну інформацією, забезпечують спільний доступ до ресурсів, підвищують продуктивність працівників і оптимізують виробничі процеси. Добре спроєктована та надійна мережа гарантує стабільну роботу інформаційної системи підприємства, створюючи передумови для високого рівня захисту даних.

Кваліфікаційна робота присвячена розробці сучасної та ефективної комп'ютерної мережі для ТОВ «Внутрішні інженерні системи», що є актуальним через постійне зростання потреб в швидкій передачі даних, надійному з'єднанні між комп'ютерними станціями та безпечному доступі до корпоративних ресурсів.

Основною метою дослідження є створення проєкту комп'ютерної мережі для зазначеного підприємства, який забезпечить безперебійне функціонування мережевої інфраструктури та ефективну взаємодію користувачів.

Для досягнення поставленої цілі передбачено виконання низки завдань, серед яких:

- аналіз ключових аспектів діяльності підприємства;
- вивчення сучасних технологій у сфері мереж;
- проектування структури локальної комп'ютерної мережі;
- вибір оптимального мережевого обладнання;
- проведення економічного обґрунтування рішення;
- розгляд питань охорони праці та технічної безпеки.

Об'єктом дослідження є комп'ютерна мережа, яка забезпечує функціонування підприємства.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

Технічне завдання для кваліфікаційного проєкту розроблено відповідно до тематики: «Створення проєкту комп'ютерної мережі ТОВ "Внутрішні інженерні системи"».

Основна мета проєкту полягає у створенні сучасної локальної комп'ютерної мережі підприємства, яка забезпечить стабільний та безпечний обмін інформацією між його структурними підрозділами, доступ до внутрішніх мережевих ресурсів, серверного обладнання, а також до мережі Інтернет.

Для досягнення поставленої мети в процесі розробки кваліфікаціного проєкту необхідно виконати такі завдання:

- Провести аналіз поточної діяльності підприємства та визначити його специфіку.
- Сформувати вимоги до майбутньої мережевої інфраструктури.
- Спроєктувати логічну та фізичну структуру локальної комп'ютерної мережі.
- Обрати відповідне активне та пасивне мережеве обладнання для реалізації проєкту.
- Забезпечити надійний захист переданої інформації та налаштувати розмежування прав доступу користувачів.
- Провести оцінку економічної доцільності впровадження запланованого проєкту.

Розроблений проєкт має відповідати сучасним стандартам якості та стати основою для ефективної роботи підприємства в умовах динамічного бізнес-середовища.

1.1.1 Найменування та область застосування

Назва розробки: Проєкт комп’ютерної мережі ТОВ «Внутрішні інженерні системи».

Сфера застосування проєкту охоплює створення та підтримку інформаційної інфраструктури підприємства, яка забезпечує ефективну роботу локальної комп’ютерної мережі, серверного обладнання, мережевих сервісів, а також засобів комунікації між співробітниками компанії.

Розроблена мережа підходить для використання як в адміністративних, так і у виробничих приміщеннях підприємства, передбачаючи можливість її подальшого розширення та технічної модернізації.

1.1.2 Призначення розробки

Метою цієї розробки є створення надійної та функціональної комп’ютерної мережі для підприємства, яка зможе забезпечити:

- інтеграцію робочих станцій у загальну інформаційну систему;
- централізований доступ до серверів і баз даних;
- підключення до мережі Інтернет;
- надійний захист даних від несанкціонованого доступу;
- стабільний обмін інформацією між різними підрозділами;
- можливість здійснення резервного копіювання та мережевого адміністрування.

Проектована мережа повинна гарантувати безперебійну діяльність підприємства та відповідати вимогам сучасних інформаційних технологій.

1.1.3 Вимоги до апаратного та програмного забезпечення

До апаратного забезпечення пред'являються такі вимоги:

- використання сучасного мережевого обладнання, що відповідає актуальним технічним стандартам;
- підтримка Ethernet зі швидкістю передачі даних на рівні щонайменше 1 Гбіт/с;
- наявність маршрутизатора для забезпечення доступу до Інтернету;
- застосування керованих комутаторів для ефективного управління мережевими підключеннями;
- забезпечення безперебійного електроживлення для серверного обладнання з метою запобігання втраті даних й перебоям у роботі;
- використання серверів для організації файлових сховищ і надання мережевих сервісів.

До програмного забезпечення висуваються такі вимоги:

- впровадження сучасних операційних систем з підтримкою останніх оновлень та безпеки;
- підтримка мережевих протоколів TCP/IP для стабільної роботи мережевої інфраструктури;
- наявність ефективного антивірусного захисту для попередження та виявлення загроз;
- засоби резервного копіювання для відновлення даних у разі непередбачуваних ситуацій;
- можливість централізованого адміністрування мережі для оперативного контролю та налаштувань;
- підтримка систем моніторингу й інструментів для забезпечення мережевої безпеки.

1.1.4 Вимоги до документації

Під час реалізації проєкту необхідно підготувати наступну документацію:

- пояснювальну записку;
- схему локальної комп’ютерної мережі;
- схему структурованої кабельної системи;
- специфікацію обладнання;
- інструкцію для адміністрування мережі;
- інструкцію для користувачів;
- кошторис витрат на впровадження проєкту.

Вся документація має бути оформлена у відповідності до чинних стандартів та методичних рекомендацій навчального закладу.

1.1.5 Техніко-економічні показники

У результаті реалізації проєкту передбачається:

- зростання швидкості передачі даних;
- скорочення часу обробки інформації;
- підвищення надійності роботи мережі;
- зменшення ризику втрати даних;
- поліпшення інформаційної безпеки;
- зростання продуктивності праці співробітників підприємства.

Економічна вигода від проєкту досягається завдяки оптимізації роботи персоналу, скороченню простоїв обладнання та підвищенню ефективності інформаційного обміну.

1.1.6 Стадії та етапи розробки

Розробка проєкту здійснюється за такими етапами:

1. Аналіз діяльності підприємства та визначення вимог до мережі.
2. Формування структури комп’ютерної мережі.
3. Підбір відповідного мережевого обладнання та програмного забезпечення.
4. Створення логічної і фізичної схем мережі.
5. Проведення розрахунків вартості реалізації проєкту.
6. Планування заходів для забезпечення інформаційної безпеки.
7. Підготовка технічної документації.
8. Проведення тестування та оцінювання ефективності створеного проєкту.

1.1.7 Порядок контролю та прийому

Контроль за реалізацією робіт, пов'язаних із проєктуванням та запровадженням комп’ютерної мережі, здійснюється уповноваженими представниками підприємства відповідно до встановлених технічних вимог і визначених етапів виконання проєкту.

Після завершення процесу монтажу та налаштування мережевої інфраструктури проводиться всебічна перевірка функціональності мережевих пристроїв і каналів комунікації. Процес контролю охоплює такі етапи:

– перевірка правильності під’єднання мережевого обладнання;

– тестування якості передачі даних між робочими станціями;

– оцінка доступу до мережевих ресурсів і глобальної мережі Інтернет;

– моніторинг стабільності функціонування локальної мережі;

– аналіз відповідності технічним вимогам, визначеним підприємством.

Процедура прийому комп’ютерної мережі здійснюється після успішного завершення всіх етапів перевірки, які мають підтвердити функціональність і

надійність створеної мережевої інфраструктури. Завершальним кроком є введення мережі в експлуатацію та передача її до компетенції відповідального підрозділу для подальшого використання в діяльності підприємства.

1.2 Постановка задачі на розробку проєкту. Характеристика підприємства, для якого створюється проєкт мережі

Товариство з обмеженою відповідальністю «Внутрішні інженерні системи» (ТОВ «Внутрішні інженерні системи») є сучасним високотехнологічним підприємством, що спеціалізується на комплексному проєктуванні, монтажі, пусконалагодженні та сервісному обслуговуванні інженерних мереж для об'єктів промислового, комерційного та цивільного (житлового) призначення. Основним профілем та стратегічним напрямком діяльності компанії є:

Електромонтажні роботи та влаштування силових електромереж (проектування та монтаж внутрішніх і зовнішніх систем електропостачання, кабельних ліній, ГРЩ, ВРУ, систем блискавкозахисту та заземлення);

Слабкострумові кабельні системи (розгортання структурованих кабельних мереж (СКМ) категорій Cat.6/Cat.6A, систем безперебійної комутації, телефонії та автоматизації будівель);

Комплексні системи безпеки та відеоспостереження (впровадження інтелектуальних систем IP-відеоспостереження з елементами аналітики, систем контролю та управління доступом (СКУД), охоронної та пожежної сигналізації).

Додатковим (супутнім) вектором діяльності підприємства, що дозволяє надавати замовникам послуги у форматі «під ключ», є проєктування та влаштування суміжних кліматичних і гідротехнічних інженерних систем, а саме: систем опалення (включаючи індивідуальні теплові пункти та котельні),

вентиляції та кондиціонування повітря (HVAC), а також внутрішніх систем водопостачання та водовідведення.

Специфіка діяльності ТОВ «Внутрішні інженерні системи» вимагає постійного обміну великими обсягами графічних та інженерних даних між різними структурними підрозділами. Основними робочими інструментами інженерів та проєктувальників є важкі САПР-платформи (AutoCAD, Revit, SolidWorks) та системи кошторисних розрахунків (АВК-5), що зумовлює генерацію файлів креслень та 3D-моделей будівель значного обсягу (від десятків мегабайтів до кількох гігабайтів для одного об'єкта).

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Для мережі ТОВ «Внутрішні інженерні системи» було обрано логічну топологію «Ієрархічна зірка» (Hierarchical Star). Ця схема організації передбачає наявність центрального комутатора третього рівня (SW_CORE), до якого під'єднуються комутатори другого рівня та PoE-комутатор. Від них, у свою чергу, здійснюється підключення до кінцевих пристроїв, розташованих у кожному підрозділі.

Топологія «Ієрархічна зірка» має такі ключові переваги

- Підвищена надійність: відмова окремого вузла чи кабелю не впливає на функціонування інших сегментів мережі.

- Зручне адміністрування: кожен відділ під'єднаний через окремий комутатор, що значно спрощує діагностику та усунення несправностей.

- Легка масштабованість: додавання нових пристроїв або підрозділів не вимагає змін у поточній топології.

Мережу розділено на шість віртуальних підмереж (VLAN), які відповідають організаційній структурі підприємства. Список віртуальних мереж можна побачити у таблиці 2.1

Таблиця 2.1 - Віртуальні підмереж

1	2	3
10	FIN	Дирекція, фінансовий відділ, бухгалтерія
20	TECH	Виробничо-технічний відділ, переговорне відділення
30	WIFI_INT	Внутрішня Wi-Fi мережа для працівників
31	WIFI_GUEST	Гостьова Wi-Fi мережа (ізольована)

Продовження таблиці 2.1

1	2	3
40	SECURITY	Відділ охорони, IP-камери, IP-телефонія
60	SERVERS	Серверна, маршрутизатор, ядро мережі

Центральним елементом архітектури мережі виступає комутатор третього рівня SW_CORE (MikroTik CRS326), який забезпечує міжмережеву маршрутизацію між усіма VLAN. До нього під'єднані три комутатори другого рівня (SW_1, SW_2, SW_3), один PoE-комутатор (SW_POE), а також сервери S_1 і S_2 та маршрутизатор R_1. Інтернет-з'єднання організовано через маршрутизатор MikroTik RB4011. Він виконує функції міжмережевого екрану та NAT-шлюзу, що гарантує надійний захист локальної мережі від зовнішніх загроз.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

Фізична схема мережі розроблена відповідно до планування офісних приміщень ТОВ «Внутрішні інженерні системи» з урахуванням розташування робочих місць, серверного та комутаційного обладнання, точок бездротового доступу та засобів відеоспостереження. При цьому було забезпечено оптимальне зонування мережевої інфраструктури для підвищення ефективності її роботи та спрощення подальшого обслуговування. Додатково враховано можливість масштабування мережі у разі розширення кількості робочих місць або обладнання. Це дозволяє підтримувати стабільну продуктивність системи навіть при зростанні навантаження та кількості підключених пристроїв. Детальна інформація зображена в таблиці 2.2.

Таблиця 2.2 — Логічна адресація в ЛОМ

1	2	3	4	5	6	7
№ VLAN	Робоча група	Підрозділ / Приміщення	Позначення вузлів	Адреса підмережі	Маска	Шлюз
10	FIN	Дирекція, фінансовий відділ, бухгалтерія	SW_1, SW_2, WS_1–WS_9, PR_1–PR_3	192.168.10.0	/24	192.168.10.1
20	TECH	Відділ Сервісного Обслуговування, переговорна	SW_3, WS_10–WS_17, PR_4, IP_2	192.168.20.0	/24	192.168.20.1
30	WIFI_INT	Внутрішня Wi-Fi для працівників	AP_1, AP_2 (SSID: Internal)	192.168.30.0	/24	192.168.30.1
31	WIFI_GUEST	Гостьова Wi-Fi мережа	Гостьові бездротові пристрої (DHCP)	192.168.31.0	/24	192.168.31.1

Продовження таблиці 2.2

1	2	3	4	5	6	7
31	WIFI_GUEST	Гостьова Wi-Fi мережа	Гостьові бездротові пристрої (DHCP)	192.168.31.0	/24	192.168.31.1
40	SECURITY	Відділ охорони, відеоспостереження, IP-телефонія	WS_18, CAM_1–CAM_7, IP_1	192.168.40.0	/24	192.168.40.1
60	SERVERS	Серверна	R_1, SW_CORE, S_1, S_2	192.168.60.0	/24	192.168.60.1

Центральним активним елементом є комутатор третього рівня SW_CORE (MikroTik CRS326), який виконує міжмережеву маршрутизацію між усіма VLAN. До нього підключені три комутатори другого рівня (SW_1, SW_2, SW_3) та один PoE-комутатор (SW_POE), а також сервери S_1, S_2 та маршрутизатор R_1.

Доступ до мережі Інтернет організовано через маршрутизатор MikroTik RB4011, який виконує роль міжмережевого екрану та NAT-шлюзу, забезпечуючи захист внутрішньої мережі від зовнішніх загроз.

2.2.1 Типи кабельних з’єднань та їх прокладка

Для створення фізичної інфраструктури мережі використовується неекранована вита пара категорії Cat 6 (UTP Cat 6). Цей тип кабелю забезпечує передачу даних зі швидкістю до 1 Гбіт/с на дистанції до 100 метрів, що повністю відповідає потребам підприємства.[5]

Кабельні траси прокладаються у перфорованих лотках серії CM від компанії DKC, встановлених під стелею уздовж коридорів та у просторі приміщень. Лотки DKC мають низку важливих переваг: - Висока механічна надійність, що захищає кабелі від пошкоджень. - Перфорована конструкція забезпечує природну вентиляцію та відведення тепла. - Легкість установки за допомогою підвісних кронштейнів, закріплених до залізобетонних перекриттів. - Зручна можливість розширення та додавання нових кабельних трас без потреби демонтажу існуючих систем. - Наявність заземлювальних з’єднань, які забезпечують захист від статичної напруги.

Від лотків кабелі опускаються до робочих місць через гофровані труби або кабельні канали, прокладені вздовж стін. Підключення кінцевого обладнання здійснюється за допомогою стандартних розеток RJ-45, встановлених безпосередньо на робочих місцях.

Кабельні траси спроєктовані з урахуванням архітектурних особливостей приміщень і мінімізації довжини з’єднань, що дозволяє оптимізувати використання матеріалів і значно спростити подальшу експлуатацію системи.

2.2.2 Будова вузлів та необхідність їх застосування

Інфраструктура мережі підприємства зображена в таблиці 2.3.

Таблиця 2.3 – Основні вузли

1	2	3	4
Позначення вузла	Тип пристрою та модель	Кількість	Функціональне призначення / Підключення
R_1	Маршрутизатор MikroTik RB4011iGS+RM	1	Корпоративний інтернет-шлюз, Firewall, NAT, DHCP
SW_CORE	Центральний комутатор L3 MikroTik CRS326-24G-2S+RM	1	Ядро мережі, міжвекторна маршрутизація VLAN
SW_1	Керований комутатор доступу MikroTik CSS318-16G-2S+IN	1	Підключення користувачів: Кабінет директора + Фін. відділ
SW_2	Керований комутатор доступу MikroTik CSS318-16G-2S+IN	1	Підключення користувачів: Відділ бухгалтерії
SW_3	Керований комутатор доступу MikroTik CSS318-16G-2S+IN	1	Підключення користувачів: Технічний відділ
S_1	Сервер HPE ProLiant DL380 Gen11	1	Серверна інфраструктура: Контролер доменів, DNS, DHCP, файловий сервер

Продовження таблиці 2.3

1	2	3	4
S_1	Сервер HPE ProLiant DL380 Gen11	1	Серверна інфраструктура: Контролер доменів, DNS, DHCP, файловий сервер
S_2	Мережеве сховище Synology DS923+ (з ОС DSM)	1	Корпоративний NAS, бекап-сервер, зберігання відеоархіву NVR
WS_1–WS_18	Робочі станції (ПК співробітників)	18	Кінцеві вузли користувачів (Windows 11 Pro)
PR_1–PR_4	Мережеві офісні принтери	4	Периферійні пристрої друку в підрозділах
AP_1–AP_2	Стелі Wi-Fi точки доступу MikroTik cAP ax	2	Бездротовий сегмент (SSID: Internal / SSID: Guest)
CAM_1–CAM_7	Купольні IP-відеокамери	7	Система відеоспостереження офісу (VLAN 40)
IP_1–IP_2	Корпоративні IP-телефони	2	Стаціонарний IP-зв'язок (Охорона + Переговорна)

PoE-комутатор (SW_POE) є окремим пристроєм, що забезпечує живлення точок доступу (AP_1, AP_2), IP-камер (CAM_1–CAM_7) і IP-телефонів (IP_1)

через кабелі Cat 6. Це усуває необхідність у додаткових блоках живлення для кожного пристрою, суттєво спрощуючи монтажну роботу і зменшуючи кількість кабелів у системі. Точки доступу AP_1 та AP_2 налаштовані на одночасну роботу з двома SSID: внутрішньою мережею (VLAN 30) для співробітників компанії та гостьовою мережею (VLAN 31) для відвідувачів. Відеосервер S_2 виконує подвійне призначення: зберігає відеозаписи з камер CAM_1–CAM_7 у сегменті VLAN 40 та обслуговує потреби технічного відділу. Завдяки підключенню через SW_CORE він має доступ до обох необхідних підмереж, забезпечуючи ефективну взаємодію між пристроями. Розподіл портів центрального комутатора, типи з'єднань між мережевими пристроями та налаштуваннями VLAN для передачі мережевого трафіку наведено у таблицях 2.4 – 2.13.

Таблиця 2.4 SW_CORE — Комутатор L3 (ядро мережі)

1	2	3	4	5	6	7	8
№ п/п	Позначення вузла	Порт вузла	Тип порту вузла	Назва пристрою	Порт пристрою	Тип порту	№ VLAN
1	R_1	ether 1	Access	SW_ CORE	ether1	Access	60
2	SW_1	ether 2	Trunk	SW_ CORE	ether2	Trunk	10, 60
3	SW_2	ether 2	Trunk	SW_ CORE	ether3	Trunk	10, 60
4	SW_3	ether 2	Trunk	SW_ CORE	ether4	Trunk	20, 60
5	SW_POE	ether 2	Trunk	SW_ CORE	ether5	Trunk	30, 31, 40, 60

Продовження таблиці 2.4

1	2	3	4	5	6	7	8
6	S_1	ether1	Access	SW_ CORE	ether6	Acces s	60
7	S_2	ether1	Access	SW_ CORE	ether7	Acces s	60

Таблиця 2.5 SW_1 — Кабінет директора + Фінансовий відділ (VLAN 10)

1	2	3	4	5	6	7	8
№ п/п	Позначення вузла	Порт вузла	Тип порту вузла	Назва пристрою	Порт пристрою	Тип порту	№ VLAN
8	WS_1	ether1	—	SW_1	ether1	Access	10
9	PR_1	ether1	—	SW_1	ether2	Access	10
10	WS_2	ether1	—	SW_1	ether3	Access	10
11	WS_3	ether1	—	SW_1	ether4	Access	10
12	WS_4		—	SW_1	ether5	Access	10
13	WS_5	—	Sw_1	ether6	Access	10	
14	PR_2	ether1	—	SW_1	ether7	Acce ss	10
15	SW_COR E	ether2	Trunk	SW_1	ether8		10, 60

Таблиця 2.6 SW_2 — Бухгалтерія (VLAN 10)

1	2	3	4	5	6	7	8
№п/п	Позначення вузла	Порт вузла	Тип порту вузла	Назва пристрою	Порт пристр ою	Тип порту	№ VLAN
16	WS_6	ether1	—	SW_2	ether 1	Access	10
17	WS_7	ether1	—	SW_2	ether 2	Access	10
18	WS_8	ether1	—	SW_2	ether 3	Access	10
19	WS_9	ether1	—	SW_2	ether 4	Access	10
20	PR_3	ether1	—	SW_2	ether 5	Access	10
21	SW_CORE	Ether3	Trunk	SW_2	ether 6	Trunk	10,60

Таблиця 2.7 SW_3 Технічний відділ + Переговорна (VLAN 20)

№п/п	Позначен ня вузла	Порт вузла	Тип порту вузла	Назва пристрою	Порт пристр ою	Тип порту	№ VLAN
22	WS_10	ethe r1	—	SW_3	Ether1	Access	20
23	WS_11	ethe r1	—	SW_3	Ether2	Access	20
24	WS_12	ethe r1	—	SW_3	Ether3	Access	20
25	WS_13	ethe r1	—	SW_3	Ether4	Access	20
26	WS_14	ethe r1	—	SW_3	Ether5	Access	20
27	WS_15	ethe r1	—	SW_3	Ether6	Access	20
28	WS_16	ethe r1	—	SW_3	Ether7	Access	20
29	WS_17	ethe r1	—	SW_3	Ether8	Access	20
30	PR_4	ethe r1	—	SW_3	Ether8	Access	20
31	IP_2	ethe r1	—	SW_3	Ether0	Access	20
32	SW_CORE	ethe r4	Trunk	SW_3	Ether1	Trunk	20, 60

Таблиця 2.8 SW_POE — PoE-комутатор (VLAN 30, 31, 40)

1	2	3	4	5	6	7	8
№ п/п	Позначення вузла	Порт вузла	Тип порту вузла	Назва пристрою	Порт пристрою	Тип порту	№VLAN
33	AP_1	ether1	—	SW_PoE	ether1	Trunk	30, 31
34	AP_2	ether1	—	SW_PoE	ether2	Trunk	30, 31
35	CAM_1	ether1	—	SW_PoE	ether3	Access	40
36	CAM_2	ether1	—	SW_PoE	ether4	Access	40
37	CAM_3	ether1	—	SW_PoE	ether5	Access	40
38	CAM_4	ether1	—	SW_POE	ether6	Access	40
39	CAM_5	ether1	—	SW_POE	ether7	Access	40
40	CAM_6	ether1	—	SW_POE	ether8	Access	40
41	CAM_7	ether1	—	SW_POE	ether9	Access	40
42	IP_1	ether1	—	SW_POE	Ether_0	Access	40
43	WS_18	ether1	—	SW_POE	ether11	Access	40
44	SW_CORE	ether5	Trunk	SW_POE	ether12	Trunk	30, 31, 40, 60

Таблиця 2.9 - IP-адресації вузлів VLAN 10 — FIN (Дирекція / Фінансовий відділ / Бухгалтерія)

1	2	3	4	5	6	7	8	9
№ п/п	Вузол	Кабінет / Відділ	Робоча група	VLAN	IP-адреса	Маска	Шлюз	DNS
1	SW_1	Кабінет директора	FIN	10	192.168.10.2	/24	192.168.10.1	192.168.60.2

Продовження таблиці 2.9

1	2	3	4	5	6	7	8	9
2	WS_1	Кабінет директора	FIN	10	192.168.10.10	/24	192.168.10.1	192.168.60.2
3	PR_1	Кабінет директора	FIN	10	192.168.10.11	/24	192.168.10.1	192.168.60.2
4	WS_2	Фінансовий відділ	FIN	10	192.168.10.20	/24	192.168.10.1	192.168.60.2
5	WS_3	Фінансовий відділ	FIN	10	192.168.10.21	/24	192.168.10.1	192.168.60.2
6	WS_4	Фінансовий відділ	FIN	10	192.168.10.22	/24	192.168.10.1	192.168.60.2
7	WS_5	Фінансовий відділ	FIN	10	192.168.10.23	/24	192.168.10.1	192.168.60.2
8	PR_2	Фінансовий відділ	FIN	10	192.168.10.24	/24	192.168.10.1	192.168.60.2
9	SW_2	Бухгалтерія	FIN	10	192.168.10.3	/24	192.168.10.1	192.168.60.2
10	WS_6	Бухгалтерія	FIN	10	192.168.10.30	/24	192.168.10.1	192.168.60.2
11	WS_7	Бухгалтерія	FIN	10	192.168.10.31	/24	192.168.10.1	192.168.60.2

Продовження таблиці 2.9

1	2	3	4	5	6	7	8	9
12	WS_8	Бухгалтерія	FIN	10	192.168.10.32	/24	192.168.10.1	192.168.60.2
13	WS_9	Бухгалтерія	FIN	10	192.168.10.33	/24	192.168.10.1	192.168.60.2
14	PR_3	Бухгалтерія	FIN	10	192.168.10.34	/24	192.168.10.1	192.168.60.2

Таблиця 2.10 — Таблиця IP-адресації вузлів VLAN 20 — TECH (Технічний відділ / Переговорна)

1	2	3	4	5	6	7	8	9
№ п/п	Вузол	Кабінет / Відділ	Робоча група	VLAN	IP-адреса	Маска	Шлюз	DNS
15	SW_3	Технічний відділ	TECH	20	192.168.20.2	/24	192.168.20.1	192.168.60.2
16	WS_10	Технічний відділ	TECH	20	192.168.20.10	/24	192.168.20.1	192.168.60.2
17	WS_11	Технічний відділ	TECH	20	192.168.20.11	/24	192.168.20.1	192.168.60.2

Продовження таблиці 2.10

1	2	3	4	5	6	7	8	9
18	WS_12	Технічний відділ	TECH	20	192.168.20.12	/24	192.168.20.1	192.168.60.2
19	WS_13	Технічний відділ	TECH	20	192.168.20.13	/24	192.168.20.1	192.168.60.2
20	WS_14	Технічний відділ	TECH	20	192.168.20.14	/24	192.168.20.1	192.168.60.2
21	WS_15	Технічний відділ	TECH	20	192.168.20.15	/24	192.168.20.1	192.168.60.2
22	WS_16	Технічний відділ	TECH	20	192.168.20.16	/24	192.168.20.1	192.168.60.2
23	WS_17	Технічний відділ	TECH	20	192.168.20.17	/24	192.168.20.1	192.168.60.2
24	PR_4	Технічний відділ	TECH	20	192.168.20.18	/24	192.168.20.1	192.168.60.2
25	IP_2	Переговорна	TECH	20	192.168.20.30	/24	192.168.20.1	192.168.60.2

Таблиця 2.11 — Таблиця IP-адресації вузлів VLAN 30 / 31 — Wi-Fi (Внутрішня / Гостьова)

1	2	3	4	5	6	7	8	9
№ п/п	Вузол	Розташування	Робоча група	VLAN	IP-адреса	Маска	Шлюз	DNS
26	SW_POE	Серверна	MGMT	30	192.168.30.2	/24	192.168.30.1	192.168.60.2
27	AP_1	Коридор / Зал	WIFI_INT	30	192.168.30.10	/24	192.168.30.1	192.168.60.2
28	AP_2	Перегов орна	WIFI_INT	30	192.168.30.11	/24	192.168.30.1	192.168.60.2
29	WIFI_GUEST	—	WIFI_GUEST	31	192.168.31.10–192.168.31.200 (DHCP)	/24	192.168.31.1	8.8.8.8

Таблиця 2.12 — Таблиця IP-адресації вузлів VLAN 40 — SECURITY (Охорона / Відеоспостереження / IP-телефонія)

1	2	3	4	5	6	7	8	9
№ п/п	Вузол	Розташування	Робоча група	VLAN	IP-адреса	Маска	Шлюз	DNS
30	WS_18	Відділ охорони	SECURITY	40	192.168.40.10	/24	192.168.40.1	192.168.60.2
31	CAM_1	Вхід / Вестибюль	SECURITY	40	192.168.40.21	/24	192.168.40.1	192.168.60.2
32	CAM_2	Коридор	SECURITY	40	192.168.40.22	/24	192.168.40.1	192.168.60.2
33	CAM_3	Фінансовий відділ	SECURITY	40	192.168.40.23	/24	192.168.40.1	192.168.60.2
34	CAM_4	Бухгалтерія	SECURITY	40	192.168.40.24	/24	192.168.40.1	192.168.60.2
35	CAM_5	Технічний відділ	SECURITY	40	192.168.40.25	/24	192.168.40.1	192.168.60.2
36	CAM_6	Переговорна	SECURITY	40	192.168.40.26	/24	192.168.40.1	192.168.60.2

Продовження таблиці 2.12

1	2	3	4	5	6	7	8	9
37	CAM_7	Вулиця / Парковка	SECURITY	40	192.168.40.27	/24	192.168.40.1	192.168.60.2
38	IP_1	Відділ охорони	SECURITY	40	192.168.40.30	/24	192.168.40.1	192.168.60.2

Таблиця 2.13 — Таблиця IP-адресації вузлів VLAN 60 — SERVERS (Серверна)

№ п/п	Вузол	Розташування	Робоча група	VLAN	IP-адреса	Маска	Шлюз	DNS
39	R_1	Серверна	SERVERS	60	192.168.60.1 / WAN: динамічна	/24	—	—
40	SW_CORE	Серверна	SERVERS	60	192.168.60.2	/24	192.168.60.1	217.196.160.44
41	S_1	Серверна	SERVERS	60	192.168.60.10	/24	192.168.60.1	217.196.160.44
42	S_2	Серверна	SERVERS	60	192.168.60.11	/24	192.168.60.1	217.196.160.44

2.3 Обґрунтування вибору мережевого обладнання для ТОВ «Внутрішні інженерні системи»

Вибір мережевого обладнання є важливим етапом у процесі проєктування корпоративної мережі, оскільки він визначає не лише її поточну продуктивність, але й впливає на можливість подальшого розширення, рівень безпеки, зручність управління, а також загальну вартість експлуатації протягом усього життєвого циклу.

Під час вибору обладнання для мережі ТОВ «Внутрішні інженерні системи» було враховано низку ключових критеріїв:

Технічна відповідність. - Обладнання повинно забезпечувати достатню кількість портів, підтримувати функції VLAN, PoE, а також маршрутизацію між VLAN, щоб відповідати заданим технічним характеристикам системи.

- Продуктивність - Особливу увагу приділяли пропускній здатності пристроїв та можливостям апаратного прискорення для забезпечення стабільної роботи мережі під високими навантаженнями.
- Надійність - Враховували показники середнього часу безвідмовної роботи (MTBF), якість компонентів, а також репутацію виробника, щоб мінімізувати ризик збоїв і додаткових витрат на ремонт.
- Оптимальність ціни щодо якості - Важливо було досягти балансу між вартістю обладнання та реальними потребами системи, уникаючи непотрібної переплати за надлишкові функції.
- Масштабованість - Обране обладнання має забезпечувати резерв портів та функціональності для можливого збільшення мережі без необхідності повної заміни апаратури.
- Уніфікована - екосистема управління. Єдиний інтерфейс для адміністрування всіх пристроїв мережі дозволяє значно скоротити витрати часу та зусиль під час налаштування й обслуговування.

Доступність на ринку України. Наявність офіційних постачальників, сертифікованого гарантійного сервісу та запасних частин була однією із базових вимог для забезпечення оперативного вирішення технічних питань

. З огляду на ці критерії, вибір мережевого обладнання здійснювався максимально ретельно, аби гарантувати довготривалу ефективність і надійність корпоративної мережі.

2.3.1 Маршрутизатор (шлюз, міжмережевий екран)

Вимоги до маршрутизатора

На підприємстві маршрутизатор виконує роль інтернет-шлюзу, забезпечує трансляцію адрес (NAT), функціонує як міжмережевий екран (firewall), відповідає за балансування навантаження, розподіл DHCP між VLAN-сегментами та, за необхідності, виступає у ролі VPN-сервера для безпечного віддаленого доступу. Пристрій повинен бути в rack-форм-факторі, що дозволяє його монтаж у серверній шафі, підтримувати операційну систему RouterOS з відповідним типом ліцензії та мати щонайменше 5 фізичних Ethernet-портів для підключення до мережевого ядра. Вибір маршрутизатора зображено в таблиці 2.14

Таблиця 2.14 — Порівняння маршрутизаторів

1	2	3	4
Критерій	MikroTik RB4011iGS+RM	TP-Link ER8411	Ubiquiti UniFi Dream Machine Pro
Ethernet-порти	10 x GE + 1 x SFP+ 10G	2 x WAN + 8 x LAN GE + 1 x SFP	1 x WAN + 8 x GE + 1 x SFP+

Продовження таблиці 2.14

1	2	3	4
RAM	1 GB	2 GB	4 GB
CPU	Quad-core AL21400	Quad-core 1.0 GHz	Quad-core 1.7 GHz
Throughput	до 9.8 Gbps	до 4 Gbps	до 3.5 Gbps
PoE-out	Ether10 (пасивний)	Немає	Немає
VPN	IPsec, PPTP, L2TP, OpenVPN (з апаратним прискоренням)	IPsec, PPTP, OpenVPN	WireGuard, OpenVPN
Firewall	RouterOS Firewall (повний)	Stateful Firewall	Stateful Firewall (UniFi)
Rack	Так, 1U	Так, 1U	Так, 1U
ОС	RouterOS v7	TP-Link ER OS	UniFi OS
Ціна (Україна)	≈ 8 800–9 500 грн	≈ 12 000–15 000 грн	≈ 35 000–45 000 грн

Обґрунтування вибору маршрутизатора

Для мережі ТОВ «Внутрішні інженерні системи» було обрано маршрутизатор MikroTik RB4011iGS+RM. Він оснащений 10 гігабітними Ethernet-портами та одним SFP+ портом на 10 Гбіт/с, а також має чотириядерний процесор і 1 ГБ оперативної пам’яті. Така конфігурація дозволяє ефективно виконувати завдання, пов’язані з firewall, NAT, DHCP, VLAN-маршрутизацією та VPN — одночасно і безперебійно, що оптимально для підприємства подібного масштабу.

Щодо ціни, модифікація RB4011iGS+RM у 2025–2026 роках в Україні доступна за 8 800–9 500 грн. Це дуже конкурентоспроможна пропозиція, враховуючи її технічні характеристики. Для порівняння: TP-Link ER8411 із нижчою продуктивністю коштує від 12 000 грн, а Ubiquiti Dream Machine Pro стартує від 35 000 грн і більше.

Серед дешевших варіантів зупинимося на TP-Link ER8411. Цей маршрутизатор пропонує приємний набір функцій та зручний веб-інтерфейс, але поступається MikroTik у пропускній здатності та гнучкості налаштувань для firewall і маршрутизації. Також його вища вартість у поєднанні з меншою функціональністю робить TP-Link менш виправданою інвестицією.

Розглянемо як альтернативу пристрій Ubiquiti UniFi Dream Machine Pro — дійсно продуктивне рішення з інтегрованим Wi-Fi контролером і зручним інтерфейсом UniFi. Втім, для офісу з 18 робочими місцями ця опція може здатися надмірно потужною та невиправдано дорогою, адже її вартість у 4–5 разів перевищує ціну RB4011iGS+RM. Такий вибір цілком обґрунтований для великих корпорацій чи готелів, але для невеликого офісу він не видається раціональним.

Натомість MikroTik RB4011iGS+RM [9] виглядає оптимальним варіантом завдяки відмінному балансу між продуктивністю, функціоналом RouterOS v7 та доступною ціною. Пристрій ідеально інтегрується в екосистему MikroTik у поєднанні з центральним комутатором та PoE-світчем, забезпечуючи стабільну та ефективну роботу мережі. Зовнішній вигляд маршрутизатора забражено на рисунку 2.1

Рисунок 2.1 - Маршрутизатор MikroTik RB4011iGS+RM

Центральний комутатор ядра мережі (L3 Switch)

Вимоги до центрального комутатора

Центральний комутатор виступає основою мережі, до якої під'єднуються всі access-комутатори, PoE-комутатор, сервери та маршрутизатор. До ключових вимог до нього належать: підтримка VLAN за стандартом 802.1Q, trunk-з'єднання, маршрутизація третього рівня (Layer 3) між VLAN, наявність щонайменше 24 Ethernet-портів, як мінімум два uplink-порти SFP+, а також відповідність rack-форм-фактору 1U. Вибір центрального комутатора описаний в таблиці 2.15.

Таблиця 2.15 — Порівняння центральних комутаторів

1	2	3	4
Критерій	MikroTik CRS326-24G-2S+RM (обраний)	TP-Link TL-SG3428 (дешевша альтернатива)	Cisco Catalyst 1000-24T (топ-сегмент)
Ethernet-порти	24 x GE	24 x GE	24 x GE
SFP/SFP+	2 x SFP+ 10G	4 x SFP	4 x SFP
5L3 маршрутизація	Так (RouterOS або SwOS)	Так (статична)	Так (повна L3)
VLAN	IEEE 802.1Q	IEEE 802.1Q	IEEE 802.1Q
Dual Boot OS	RouterOS / SwOS	Hi	Hi
PoE-in	Так	Hi	Hi
RAM	512 MB	Н/д	256 MB
CPU	800 MHz	Н/д	ARM

Продовження таблиці 2.15

1	2	3	4
Rack форм-фактор	1U	1U	1U
Ціна (Україна)	≈ 8 200–10 400 грн	≈ 5 500–7 000 грн	≈ 40 000–60 000 грн

Обґрунтування вибору центрального комутатора

Для ядра мережі обрано комутатор MikroTik CRS326-24G-2S+RM. [10] Він оснащений 24 гігабітними Ethernet-портами і двома 10G SFP+ портами, а функція Dual Boot (RouterOS або SwOS) забезпечує можливість використання його як повнофункціонального L3-комутатора або як спрощеного керованого комутатора, залежно від вимог.

Портова місткість: У рамках проєкту до центрального комутатора підключаються маршрутизатор R_1, access-комутатори SW_1, SW_2 і SW_3, PoE-комутатор SW_POE, а також сервери S_1 і S_2. Це становить лише 7 активних підключень із загальних 24 портів. У результаті залишаються вільними 17 портів, що дає значний резерв для майбутнього розширення мережі без потреби у заміні ядра. [12]

Дешевша альтернатива: Розглянуто TP-Link TL-SG3428. Він коштує на 2 000–3 000 грн менше та забезпечує базовий набір функцій для L2/L3 мереж. Однак має обмеження: тільки один SFP-порт із пропускною здатністю 1G замість двох 10G SFP+, меншу гнучкість у налаштуванні та відсутність Dual Boot. Це прийнятний бюджетний варіант, однак менш ефективний і перспективний для тривалого використання.

Топ-альтернатива: Cisco Catalyst 1000-24T є зразком надійності та визнаним стандартом у галузі мережевих рішень. Проте ціна в межах від 40 000 грн є

економічно невиправданою для мережі з усього сімома підключеннями до ядра. Крім того, для обслуговування обладнання Cisco потрібен високий рівень технічної кваліфікації адміністратора, а також значно дорожчі ліцензії.

Висновок: MikroTik CRS326-24G-2S+RM є оптимальним вибором, поєднуючи доступність, функціональність і зручність інтеграції в існуючу MikroTik-інфраструктуру. Для офісної мережі підприємства це обладнання забезпечує достатній запас потужності для поточних і майбутніх потреб. Зовнішній вигляд комутатора зображено на Рисунок 2.2

Скрипт конфігурації центрального комутатора винесено в Додаток Г.1

Рисунок 2.2 - MikroTik CRS326-24G-2S+RM

2.3.2 PoE-комутатор доступу

Вимоги до PoE-комутатора

PoE-комутатор виконує функцію забезпечення електроживлення та мережевого підключення для 12 пристроїв, серед яких: дві точки доступу Wi-Fi (AP_1, AP_2), сім IP-камер (CAM_1–CAM_7), один IP-телефон для використання охоронною службою (IP_1), одна робоча станція охорони (WS_18), а також передбачено uplink-з'єднання з центральним комутатором (SW_CORE). Із загальної кількості підключень щонайменше десять пристроїв потребують живлення за технологією PoE. Рохрахунок бюджету PoE зображено в таблиці 2.16

Таблиця 2.16 Розрахунок PoE-бюджету з запасом:

1	2	3	4
Пристрій	Кількість	Типова потужність	Разом
AP Wi-Fi	2	15 Вт	30 Вт
IP-камери	7	6 Вт	42 Вт
IP-телефон	1	6 Вт	6 Вт
Разом факт	—	—	78 Вт
Запас +40%	—	—	109 Вт
Рекомендований мінімум	—	—	≥ 150 Вт

Таким чином, PoE-бюджет комутатора має становити щонайменше 150 Вт, а для надійного запасу — понад 200 Вт. Також важливим критерієм була підтримка сучасних стандартів PoE для стабільного живлення пристроїв.

Під час вибору також враховувалася відповідність комутатора вимогам мережевої інфраструктури.

Тепер потрібно обрати оптимальний PoE комутатор. Вибір PoE зображено в таблиці 2.17

Таблиця 2.17— Порівняння PoE-комутаторів

1	2	3	4
Критерій	MikroTik CRS318-16P-2S+OUT (обраний)	TP-Link TL-SG1218MPE (бюджетна альтернатива)	Ubiquiti UniFi USW-Pro-24-PoE (топ)
PoE-порти	16 x GE PoE+	16 x GE PoE+	16 x PoE+ + 8 x PoE++
Uplink	2 x SFP+ 10G	2 x SFP 1G	2 x SFP+ 10G
PoE-бюджет	300–315 Вт	192–250 Вт	400 Вт

Продовження Таблиці 2.17

1	2	3	4
Max PoE на порт	30 Вт (802.3at)	30 Вт (802.3at)	60 Вт (802.3bt)
Керування	RouterOS / SwOS	Web Smart	UniFi контролер
VLAN	Так (повна)	Базова	Так (повна L3)
Корпус	IP55 (зовнішній)	Desktop/rack	Rack
Ціна (Україна)	≈ 11 200–15 900 грн	≈ 9 100–9 800 грн	≈ 35 000–55 000 грн
Max PoE на порт	30 Вт (802.3at)	30 Вт (802.3at)	60 Вт (802.3bt)
Керування	RouterOS / SwOS	Web Smart	UniFi контролер
VLAN	Так (повна)	Базова	Так (повна L3)
Корпус	IP55 (зовнішній)	Desktop/rack	Rack
Ціна (Україна)	≈ 11 200–15 900 грн	≈ 9 100–9 800 грн	≈ 35 000–55 000 грн

Обґрунтування вибору PoE-комутатора

Для сегмента PoE було обрано модель MikroTik CRS318-16P-2S+OUT (netPower 16P). Цей комутатор оснащений 16 PoE-портами із сумарним енергобюджетом у 300–315 Вт, а також має два SFP+ порти зі швидкістю 10G для uplink-з'єднання з центральним комутатором. Завдяки підтримці

RouterOS/SwOS забезпечується уніфікований інтерфейс адміністрування, що спрощує інтеграцію з іншими пристроями MikroTik.

Енергетичний запас PoE на рівні 300–315 Вт є більш ніж достатнім для забезпечення стабільної роботи системи. За реального споживання близько 78 Вт і рекомендованого мінімального резерву в 150 Вт, комутатор має більше ніж дворазовий запас. Такий рівень резерву є ключовим для гарантування надійного одночасного запуску всіх камер та точок доступу після відновлення живлення.

Комутатор встановлюється безпосередньо у серверній кімнаті, що дозволяє підключати кабелі від камер спостереження, точок доступу та пристроїв IP-телефонії без необхідності використання додаткових проміжних свічів на окремих поверхах. Такий підхід суттєво оптимізує процес монтажу, знижує кількість потенційних точок відмови в мережі та забезпечує централізоване управління живленням PoE-пристроїв, збільшуючи ефективність і надійність системи в цілому.

Бюджетна альтернатива — TP-Link TL-SG1218MPE. Цей комутатор обійдеться значно дешевше — на 2 000–6 700 грн (≈ 9 100–9 800 грн) — та забезпечує 16 PoE-портів. Однак його PoE-бюджет обмежений у межах 192–250 Вт, а SFP-порти підтримують лише 1G, тоді як бажаним є 10G. Управління здійснюється через Web Smart, що не дозволяє повноцінно реалізовувати функції VLAN на рівні RouterOS. Якщо мережа будується з двома SFP+ 10G uplink на центральному комутаторі, перехід до 1G uplink стане значним компромісом. Загалом цей варіант можна розглядати при мінімальному бюджеті, але його функціональність явно поступається іншим рішенням.

Смарт-альтернатива — Ruijie Reyee RG-ES218GC-P. Цей комутатор має також 16 PoE-портів із PoE-бюджетом 240 Вт, пропонує хмарне управління через платформу Ruijie Cloud і оснащений зручним інтерфейсом для управління системами відеоспостереження. Проте він не підтримує інтеграцію в екосистему MikroTik, має менший запас потужності для PoE, а uplink-порти обмежені характеристиками (2 x SFP 1G замість SFP+ 10G). Комутатор був би

прийнятним рішенням для мережі побудованої повністю на обладнанні Ruijie, але у цьому проєкті він створює автономний «острів» з окремою системою управління.

Топ-альтернатива — Ubiquiti UniFi USW-Pro-24-PoE. Це високопродуктивний комутатор, який пропонує PoE-бюджет у розмірі 400 Вт, функції L3 маршрутизації та чудовий інтерфейс управління UniFi. Проте його вартість, яка стартує від 35 000 грн, є надлишковою для тих потреб, які ставляться до PoE-комутатора в даній мережі. Даний варіант доцільний хіба що у масштабних проєктах: великих готелях або торгових комплексах, де використання уніфікованої екосистеми Ubiquiti стає стратегічним рішенням.

Окрім технічних характеристик, важливим чинником при виборі PoE-комутатора є наявність сервісної підтримки та регулярних оновлень прошивки. Це забезпечує своєчасне усунення виявлених вразливостей, підвищує рівень безпеки та дозволяє інтегрувати нові функції без заміни обладнання. Таким чином, якість технічної підтримки виробника має прямий вплив на довгострокову надійність мережевої інфраструктури.

Висновок: найоптимальнішим вибором залишається MikroTik CRS318-16P-2S+OUT. Він забезпечує достатньо PoE-підключень із значним запасом потужності, підтримує SFP+ 10G uplink і легко інтегрується в наявну MikroTik-інфраструктуру. Таким чином, реалізується уніфіковане управління всією мережею через один інтерфейс. Зовнішній вигляд PoE-комутатора наведено на рисунку 2.3. [11]

Рисунок 2.3 – PoE Комутатор

2.3.4 Перевірка портів і PoE-бюджету по вузлах

Було виконано аналіз завантаження комутаторів. В таблиці 2.18 зображено перевірку завантаження усіх комутаторів.

Таблиця 2.18 - Перевірка завантаження портів усіх комутаторів

1	2	3	4	5	6
Вузол	Модель обладнання	Доступні порти	Підключені пристрої	Зайнято портів	резерв портів
R_1	MikroTik RB4011iGS+RM	10 × GE + 1 x SFP+	ISP Провайдер, Uplink до SW_CORE	2	8 × GE + 1 × SFP+
SW_CORE	MikroTik CRS326-24G-2S+RM	24 × GE + 2 x SFP+	Лінії до: R_1, SW_1, SW_2, SW_3, SW_POE, S_1, S_2	7	17 × GE + 2 × SFP+
SW_1	MikroTik CSS318-16G-2S+IN	16 × GE + 2 x SFP+	5 × Робочих ПК (WS_1-5), 2 × Принтери (PR_1-2), 1 × Uplink до ядра	8	8 × GE + 2 × SFP+
SW_2	MikroTik CSS318-16G-2S+IN	16 × GE + 2 x SFP+	4 × Робочих ПК (WS_6-9), 1 × Принтер (PR_3), 1 × Uplink до ядра	6	10 × GE + 2 × SFP+

Продовження таблиці 2.18

1	2	3	4	5	6
SW_3	MikroTik CSS318-16G-2S+IN	16 × GE + 2 x SFP+	8 × Робочих ПК (WS_10-17), 1 × Принтер (PR_4), 1 × IP-телефон, 1 × Uplink	11	5 × GE + 2 × SFP+
SW_POE	MikroTik CRS318-16P-2S+OUT	16 × PoE GE + 2 x SFP+	2 × Wi-Fi AP, 7 × IP-камер, 1 × IP-телефон, 1 × ПК Охорони (WS_18), 1 × Uplink	12	4 × PoE + 1 × SFP+

Було виконано перевірку можливості живлення всіх PoE-пристроїв від обраного комутатора. В таблиці 2.19 зображено перевірку PoE-бюджету.

Таблиця 2.19. — Перевірка PoE-бюджету SW_POE

1	2	3	4	5
Пристрій	Кількість	Max PoE на порт	потужність	Сума
Точки доступу Wi-FiAP_1, AP_2	2	15.4Вт (802.3af)	12 Вт	24 Вт
IP-камери Cam_1 – Cam_7	7	15.4Вт (802.3af)	6 Вт	42 Вт

Продовження таблиці 2.19

1	2	3	4	5
IP-телефон IP_1	1	15.4Вт (802.3af)	5 Вт	5 Вт
Разом (факт)	10	—	—	71 Вт
Запас +50%	—	—	—	107 Вт
Максимальний резерв (бюджет − факт)	—	—	—	≈ 229 Вт
Бюджет SW_POE	—	—	—	300–315 Вт ✓

Результати розрахунків демонструють, що PoE-бюджет моделі CRS318-16P-2S+OUT значно перевищує необхідний рівень: за фактичного навантаження у 71 Вт та навіть у разі досягнення пікової позначки у 107 Вт залишається запас потужності понад 200 Вт. Такий резерв забезпечує надійну експлуатацію всіх підключених пристроїв, навіть при їх одночасному використанні, повністю виключаючи ризик перенавантажень електроживлення. Крім того, такий запас потужності дозволяє без проблем підключати нові пристрої у майбутньому, не турбуючись про обмеження енергоспоживання. Це робить модель CRS318-16P-2S+OUT оптимальним рішенням для масштабованих корпоративних мереж, де важлива стабільність та довготривала надійність роботи обладнання. Додатково, високий запас PoE-бюджету гарантує стабільну роботу навіть у випадку підключення енергоємних пристроїв, таких як IP-камери чи точки доступу Wi-Fi.

2.3.5 Зведена таблиця обраного обладнання

Було здійснено вибір мережевого обладнання відповідно до вимог проєкту. Обране обладнання та обґрунтування вибору наведено в таблиці 2.20.

Таблиця 2.20 — Обране обладнання та обґрунтування вибору

1	2	3	4	5	6
№	Вузол	Модель	Призначення	Ціна орієнтовно	Обґрунтування
1	R_1	MikroTik RB4011iGS+RM	Маршрутизатор, шлюз, firewall, NAT	≈8 800–9500 грн	Найкраще співвідношення ціна/продуктивність
2	SW_CORE	MikroTik CRS326-24G-2S+RM	Центральний L3 комутатор	≈ 8 200–10 400 грн	24 GE + 2×SFP+ 10G; Dual Boot; великий резерв портів; VLAN
3	SW_POE	MikroTik CRS318-16P-2S+OUT	PoE-комутатор доступу	≈11200 –15900 грн	16 PoE-портів; 300+ Вт PoE-бюджет; SFP+ 10G uplink; RouterOS
4	SW_1, SW_2	Керований GE-комутатор	Access-комутатори	≈1 500–3 000 грн/шт	Підключення WS та принтерів фінансового та бухгалтерського відділів

Продовження таблиці 2.20

1	2	3	4	5	6
5	SW_3	Керований GE-комутатор	Access-комутатор	≈ 2 000–4 000 грн	Підключення 8 WS + принтер + IP-телефон технічного відділу

Середня вартість активного мережевого обладнання оцінюється в межах 35 000–47 000 грн, при цьому до розрахунку не включені сервери, точки доступу, IP-камери та кабельна інфраструктура.

2.4 Монтаж і розміщення мережевого обладнання

Монтаж мережевої інфраструктури є ключовим етапом у процесі створення проєкту, коли теоретичні напрацювання втілюються в реальну, функціонуючу систему. Саме на цьому етапі можна оцінити правильність вибору активного обладнання, кабельної системи, схеми комутації, монтажних аксесуарів та загального підходу до організації простору. Якщо в ході логічного проєктування основна увага приділяється адресації, VLAN, ролям пристроїв і потокам трафіку, то на етапі монтажу важлива якість фізичного з'єднання, зручний доступ до обладнання, акуратність трасування кабелів та легкість подальшого обслуговування без необхідності демонтажу значної частини інфраструктури.

Для ТОВ «Внутрішні інженерні системи» доцільно реалізувати структуровану кабельну систему з централізованим розміщенням ключових активних вузлів у серверній кімнаті. Це означає, що маршрутизатор, центральний комутатор, PoE-комутатор, патч-панелі, UPS та допоміжні

елементи комутації розміщуються в одному контрольованому приміщенні, а всі горизонтальні лінії від робочих місць, точок доступу, камер відеоспостереження та інших кінцевих пристроїв сходяться саме до цієї точки. Такий підхід вважається класичним і найбільш практичним для офісної інфраструктури, оскільки він спрощує адміністрування, мінімізує кількість проміжних вузлів і створює зрозумілу топологію, яку легко супроводжувати протягом усього життєвого циклу мережі.

У цьому розділі детально описані ключові аспекти фізичного монтажу, серед яких: загальна концепція встановлення обладнання, вимоги до серверної кімнати, специфікації кабельної системи, правила прокладання трас, використання кабельних лотків DKC, встановлення точок доступу MikroTik cAP ax, організація PoE-живлення та проведення перевірки якості після завершення монтажних робіт. Особлива увага приділяється тих елементам мережі, які більшою мірою впливають на її стабільність і надійність: правильному поєднанню активного обладнання з кабельною інфраструктурою, забезпеченню достатнього запасу довжини кабелю, подачі живлення та доступності для технічного обслуговування.

2.4.1 Загальна концепція монтажу

Фізична структура мережі будується за принципом централізованої комутаційної точки, від якої променями розходяться основні кабельні траси. Це означає, що мережа проектується не як хаотична сукупність з’єднань, а як добре організована система, де кожен кабель має чітко визначену функцію, а кожен пристрій займає своє встановлене місце в загальній структурі. Такий підхід не тільки забезпечує технічну надійність, але й сприяє підтриманню організаційної дисципліни, що в умовах офісної роботи є не менш важливим за високу швидкість передачі даних.

Центральним вузлом мережевої інфраструктури виступає серверна кімната, де зосереджуються всі ключові елементи системи. Тут розміщуються пристрої ядра мережі, прокладаються патч-корди, виконуються необхідні комутаційні операції та здійснюється управління живленням і системами охолодження, а також контролюється фізичний доступ до обладнання. Така централізація мінімізує ризики ненавмисного втручання з боку користувачів і значно полегшує діагностику несправностей. Адміністратору достатньо отримати доступ лише до одного приміщення, аби мати повну картину стану критичної інфраструктури та швидко реагувати на будь-які проблеми.

Варто також зазначити, що якісний монтаж мережі – це не просто естетичне укладання кабелів. Це комплекс продуманих рішень, що охоплюють правильний вибір маршрутів прокладання кабелю, дотримання рекомендованих радіусів вигинів, уникнення надмірного натягу та механічних пошкоджень, забезпечення розмежування силових і слабкострумових ліній, а також створення запасу довжини для можливості подальшого обслуговування чи модернізації. Якщо зробити помилки на цьому етапі, їхні наслідки можуть проявитися не одразу, а через тривалий час у вигляді деградації сигналу, пошкоджень конекторів, збоїв у роботі PoE або труднощів при розширенні системи.

У межах цього проєкту було прийнято рішення використати традиційну офісну схему із горизонтальним прокладанням кабелів категорії Cat.6 до робочих місць, камер відеоспостереження, точок доступу Wi-Fi та інших допоміжних пристроїв. Такий підхід є економічно доцільним і виправданим із технічної точки зору: кабельна система повністю забезпечує потреби гігабітної мережі без значного збільшення витрат на матеріали. У зонах із потребою в більшому резерві пропускної здатності передбачено можливість застосування кабелю Cat.6A. Проте в більшості випадків стандартний Cat.6 виявляється оптимальним рішенням, поєднуючи високі технічні показники з раціональним використанням ресурсів.

2.4.2 Серверна кімната та розміщення вузлів

Серверна кімната є ключовим вузлом мережевої інфраструктури будь-якого підприємства, адже саме тут розташовані всі критичні елементи, які забезпечують стабільність і безперебійну роботу системи. Вимоги до цієї зони мають бути суворими не лише в контексті обмеження доступу, але й щодо підтримання оптимального мікроклімату, чистоти, ефективної вентиляції, надійного електропостачання та раціонального планування простору. Через безперервний або тривалий щоденний режим роботи активного обладнання необхідно забезпечити належний рівень охолодження та стабільне електроживлення з використанням джерел безперебійного живлення (UPS).

У типовій конфігурації серверна кімната обладнується 19-дюймовою шафою або стійкою, яка служить базою для розміщення маршрутизатора, комутаторів, патч-панелей, органайзерів, джерела безперебійного живлення та, за потреби, серверів резервного копіювання чи вузлів зберігання даних. У межах цього проєкту доцільно обрати шафу із запасом висоти для монтажу, оскільки додатковий простір завжди є перевагою. Він дозволяє уникнути перевантаження верхніх секцій обладнанням, полегшує організацію кабельних з'єднань і залишає місце для майбутньої установки додаткових компонентів.

Кожен пристрій у серверній має бути не лише відповідним чином розташований, але й логічно інтегрований у загальну монтажну схему. Наприклад, маршрутизатор забезпечує функції шлюзу та фільтрації трафіку, центральний комутатор виконує роль агрегатора для магістральних з'єднань, PoE-комутатор відповідає за електроживлення периферійних пристроїв, а патч-панелі слугують зручним перехідним елементом між горизонтальними лініями та активним обладнанням. Таке чітке розмежування ролей допомагає підтримувати порядок у структурі комутації та мінімізує ризик помилок під час змін у конфігурації. В таблиці 2.21 зображений склад серверної шафи

Таблиця 2.21 - Склад серверної шафи

Елемент	Призначення	Коментар
Патч-панель 24 порти	Завершення горизонтальних ліній	Формує зручну точку комутації
MikroTik RB4011iGS+RM	Маршрутизатор, шлюз, firewall	Забезпечує доступ до мережі та VPN
MikroTik CRS326-24G-2S+RM	Центральний комутатор	Агрегує всі основні лінії
MikroTik CRS318-16P-2S+OUT	PoE-комутатор	Живить камери, AP і IP-телефонію
UPS	Безперебійне живлення	Підтримує роботу критичних вузлів
Органайзери кабелю	Упорядкування патч-кордів	Дозволяють зберегти охайність монтажу
Маркування портів і ліній	Ідентифікація з’єднань	Полегшує обслуговування і ремонт

Розташування обладнання в межах однієї серверної шафи пропонує ще одну суттєву перевагу — значне скорочення довжини з'єднань, що робить їх більш охайними та передбачуваними. Це не лише сприяє естетичності монтажу, але й позитивно впливає на технічні характеристики: коротші патч-корди мають менший ризик випадкових пошкоджень, легше піддаються маркуванню та не спричиняють зайвого безладу в зоні комутації.

2.4.3 Принцип прокладання кабельних трас

Прокладання кабельних трас у сучасному офісному приміщенні має виконуватися відповідно до вимог структурованої кабельної системи (СКС).

Основною перевагою СКС є те, що кожне робоче місце чи пристрій отримує окремий кабельний маршрут до комутаційного центру, оминаючи випадкові проміжні з'єднання. Хоча такий підхід і вимагає більших початкових витрат, він значно спрощує подальше обслуговування та суттєво знижує ймовірність виникнення прихованих несправностей, які важко виявити без спеціального обладнання.

Кабельні траси зазвичай поділяють на горизонтальні та магістральні. Горизонтальні траси забезпечують підключення кінцевих пристроїв у межах одного поверху або функціональної зони, тоді як магістральні виконують роль з'єднувальних ліній між шафами, поверхами чи окремими технічними приміщеннями. У рамках даного проєкту основна увага приділяється саме горизонтальному прокладанню, оскільки більшість мережевих вузлів розташована в межах однієї будівлі та централізовано підключається до серверної кімнати.

Під час монтажу важливо суворо дотримуватись технічних стандартів прокладання кабелів. Не слід допускати різких вигинів, надмірного натягу, стискання чи перекручування кабелю, а також розташування поблизу силових ліній на мінімально допустимій відстані. Переплетення пар у кабелях витої пари виконує важливу функціональну роль: будь-яке порушення їхньої структури підвищує ризик появи перешкод і знижує стабільність з'єднання. Це особливо критично для довгих траєкторій, де кабель використовує максимум своїх технічних можливостей.

Для забезпечення практичності монтажу рекомендується залишати невеликий резерв довжини на кожному кінці кабелю. Цей запас дозволяє провести повторну обробку кінців, перемістити розетку чи замінити конектор без потреби повністю перекладати кабель. У реальній експлуатації такі резерви стають рятівним рішенням, яке допомагає уникнути складних і витратних ремонтів.

2.4.4 Вибір кабельної інфраструктури

Основним вибором для створення локальної мережі є кабель вита пара категорії Cat.6. Він поєднує універсальність із високою пропускною здатністю, забезпечуючи стабільну гігабітну швидкість передачі даних на стандартних офісних відстанях. При цьому його вартість не обтяжує бюджет проєкту, що робить цей варіант оптимальним. Для підприємств, де більшість робочих станцій, камер спостереження та периферійних пристроїв працюють на швидкості 1 Гбіт/с, Cat.6 стає практичним і економічно вигідним рішенням.

Серед основних переваг цього стандарту — вища смуга пропускання та покращена захищеність від перехресних наведень у порівнянні з Cat.5e. Це особливо важливо для довгих сегментів кабелів або у випадках, коли кілька ліній прокладаються близько одна до одної у спільних кабельних лотках. Хоча кабель Cat.6A дозволяє передавати дані зі швидкістю до 10 Гбіт/с на більш значних відстанях, у контексті стандартного офісного проєкту використання такого кабелю є фінансово недоцільним через надмірність його характеристик для задач поточного рівня.

Окрім магістральних кабелів, у мережевій інфраструктурі використовуються патч-корди різної довжини, розетки RJ-45, конектори, модульні вставки та різноманітні аксесуари для кріплення і організації кабельної системи. Ці елементи відіграють не менш важливу роль, ніж сам основний кабель, оскільки саме від їхньої якості залежить стабільність контактів, зручність монтажу і подальше обслуговування мережі. Економія на таких компонентах є хибною стратегією, оскільки дешевий конектор чи неякісний патч-корд можуть стати «вузьким місцем», що вплине на ефективність усієї системи.

Ще одним важливим аспектом проєктування мереж є чітке маркування кабелів. Кожна лінія повинна бути позначена з обох кінців за допомогою зрозумілих і однозначних міток. Це значно спрощує процес обслуговування інфраструктури, зокрема пошук конкретного кабелю, який веде до камери,

точки доступу, робочого місця чи принтера. Такий підхід дозволяє заощадити час під час діагностики або переналаштування обладнання.

2.4.5 Кабельні лотки DKC

Одним із ключових компонентів фізичного монтажу є система кабельних лотків, яка визначає основний маршрут прокладання трас у приміщенні. У цьому проєкті оптимальним варіантом є використання кабельних лотків DKC, адже ця продукція зарекомендувала себе на ринку завдяки широкому асортименту типорозмірів і аксесуарів, а також високому рівню міцності та довговічності. Таке рішення особливо актуальне для офісних просторів, де кабельна інфраструктура повинна не лише функціонувати ефективно, а й виглядати естетично та професійно.

Лотки DKC забезпечують зручність і безпеку прокладання кабелів уздовж стін, під стелею або в технічних зонах. Вони дають змогу уникнути хаотичного розташування кабелів, що часто призводить до їх пошкодження, заплутування та ускладнень під час подальшого обслуговування. Крім того, металеві лотки є ідеальним вибором для великих офісних приміщень, де необхідно організувати велику кількість слабкострумових мереж.

Система DKC включає безліч компонентів, таких як прямі секції, кути, з’єднувачі, підвіси, кронштейни, кришки та допоміжні аксесуари. Кожен елемент відіграє важливу роль: окремі компоненти створюють повороти траси, інші забезпечують надійне кріплення або захищають кабелі від пилу й механічних пошкоджень. Завдяки модульній конструкції систему можна легко розширювати або змінювати без потреби в демонтажі всього маршруту. Переваги лотків DKC зображено в таблиці 2.22

Таблиця 2.22 - Переваги лотків DKC

Перевага	Практичний ефект
Механічна міцність	Кабелі надійно захищені від деформації
Модульність	Легке добудовування нових ділянок
Великий вибір аксесуарів	Зручно формувати повороти й розгалуження
Акуратність монтажу	Краще обслуговування і візуальний порядок
Довговічність	Менша ймовірність передчасної заміни

У практичному вимірі саме лоткова система відіграє ключову роль у забезпеченні якості монтажу, оскільки навіть найсучасніше обладнання може функціонувати ненадійно, якщо кабелі проложені хаотично або з порушенням технічних стандартів. Тому на етапі проєктування лотків слід враховувати не лише поточну кількість ліній, але й можливе майбутнє розширення. Це дозволить уникнути необхідності повної переробки маршрутів через кілька років.

2.4.6 Підключення точок доступу

Wi-Fi точки доступу на підприємстві розташовуються таким чином, щоб забезпечити рівномірне покриття робочих зон і звести до мінімуму появу «мертвих» зон радіосигналу. Особливо це актуально в офісах, де користувачі очікують стабільного бездротового з’єднання не лише біля своїх робочих місць, але й у залах для переговорів, коридорах, зонах відпочинку та суміжних приміщеннях. З огляду на це, розміщення точок доступу повинне базуватися не на випадковості, а на ретельному аналізі геометрії простору.

У проєкті застосовано точки доступу MikroTik cAP ax, які зазвичай встановлюються на стелі або у верхній частині стін. Така позиція забезпечує природний розподіл сигналу, оскільки антени функціонують у відкритому

просторі без значних перешкод. Окрім технічної ефективності, стельове розміщення має естетичну перевагу: точки доступу не створюють незручностей для користувачів і не займають корисного простору на столах чи стінах в зоні досяжності.

Кожна точка підключається за допомогою одного кабелю Cat.6, який одночасно забезпечує передавання даних і живлення через технологію PoE. Це суттєво спрощує процес встановлення, адже відпадає потреба прокладати окрему лінію для живлення 220 В до місця монтажу обладнання. Такий підхід не лише скорочує складність інсталяції, але й підвищує надійність роботи системи через зменшення кількості розеток, блоків живлення та точок потенційного перегріву.

Важливо зазначити, що точки доступу в даній архітектурі є більше, ніж лише засобом для забезпечення бездротового покриття. Вони інтегруються у загальну модель безпеки й логічної організації мережі. Це включає підтримку сегментації трафіку для внутрішніх і гостьових мереж, роботу з VLAN та централізоване адміністрування. Завдяки цьому адміністратори можуть оперативно змінювати параметри мережі без необхідності фізичного втручання в налаштування кожної точки.

2.4.7 Монтаж PoE-пристроїв

PoE-обладнання вимагає ретельної уваги під час монтажу, адже воно поєднує функції мережевого обладнання та джерела електроживлення. На відміну від звичайних Ethernet-пристроїв, для PoE-камер або точок доступу важливими є не лише цілісність каналу передачі даних, а й стабільність напруги, яка передається тим же кабелем. Таким чином, якість кабельної інфраструктури, правильність обтиску та резерв по потужності набувають вирішального значення.

У цьому проєкті всі PoE-пристрої підключені до централізованого PoE-комутатора. Таке рішення значно полегшує керування живленням, дозволяючи адміністратору моніторити навантаження на окремі порти, дистанційно перезавантажувати пристрої, контролювати реальне споживання енергії та запобігати перевантаженням. Цей підхід суттєво ефективніший у порівнянні з використанням окремих PoE-інжекторів, які розташовані по всій будівлі й ускладнюють управління.

Особливу увагу при монтажі PoE-ліній потрібно приділяти якості кінцевих конекторів. Для безперервно працюючих пристроїв, як-от камери відеоспостереження, погана якість з’єднань або неправильний обтис кабелю можуть спричинити періодичні збої в роботі, втрачені відеопотоки чи навіть повний розрив зв’язку саме в найкритичніший момент. Тому монтаж слід виконувати максимально обережно, з подальшим обов’язковим тестуванням кожної лінії після завершення робіт.

2.4.8 Організація робочих місць

Робочі місця в рамках мережі підприємства повинні бути реалізовані так, щоб забезпечувати користувачам стабільний та інтуїтивно зрозумілий доступ до необхідних ресурсів. При цьому важливо мінімізувати видимість кабелів і уникати використання тимчасових рішень. Для кожного робочого місця варто передбачити принаймні одну виділену мережеву лінію, а для критично важливих посад — дві. Це дасть змогу оперативно підключати додаткові пристрої або створювати резервні канали у разі виникнення потреби.

В офісах бухгалтерії, адміністрації, керівництва та технічних відділів розетки повинні розташовуватися з урахуванням можливості майбутнього перепланування приміщень. Оскільки меблі можуть змінюватися, а робочі зони — переміщатися, мережа повинна залишатися гнучкою і функціональною

незалежно від таких змін. Тому під час проєктування кабельної системи доцільно залишати певний запас її ресурсів і уникати надмірної жорсткої прив'язки до поточної організації простору.

Окремі точки підключення бажано передбачити також для принтерів, IP-телефонів та іншого периферійного обладнання. Це сприятиме більш ефективному логічному розподілу трафіку і в подальшому дозволить змінювати функціональне призначення окремих портів без необхідності модифікувати фізичну схему прокладання кабелів.

2.4.9 Контроль якості монтажу

Після завершення монтажних робіт обов'язково проводиться ретельна перевірка якості всіх кабельних та комутаційних з'єднань. Цей етап не можна розглядати як просту формальність, адже саме він засвідчує повну готовність мережі до експлуатації. У рамках контрольних заходів перевіряється правильність обтиску контактів, наявність чи відсутність обривів, коротких замикань, переплутаних пар, а також точність маркування всіх ліній відповідно до проектної схеми.

Окрім електротехнічної перевірки, особлива увага приділяється функціональному тестуванню. Це включає перевірку активації лінків на комутаторах, отримання IP-адрес, стабільності передачі трафіку через VLAN, доступність шлюзу, роботу Wi-Fi, живлення PoE-пристроїв і справність серверних сервісів. Якщо хоча б один із цих компонентів функціонує нестабільно, мережа потребує додаткового налаштування ще до її здачі в експлуатацію.

Критично важливим також є створення чіткої та зрозумілої документації після завершення монтажу: має бути підготовлена схема портів, таблиця відповідності кабелів, план розташування точок доступу, список комутаційних

з’єднань та базові інструкції для технічного персоналу. Правильно оформлена документація забезпечує зручну керованість мережею, перетворюючи її на структуровану систему, а не просто на випадковий набір працюючих з’єднань.

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

Вибір операційних систем і прикладного програмного забезпечення є ключовим етапом у проєктуванні корпоративної мережі, оскільки саме програмна складова визначає ефективність використання апаратних ресурсів, швидкість доступу користувачів до необхідних сервісів, зручність адміністрування інфраструктури та загальний рівень її безпеки. Якщо апаратна частина мережі виступає фізичним фундаментом системи, то програмна частина визначає правила її функціонування, способи взаємодії між вузлами, процедури доступу до ресурсів і підходи до захисту інформації. Таким чином, у контексті ТОВ «Внутрішні інженерні системи» програмне забезпечення слід сприймати не як додатковий елемент, а як один із центральних факторів, що впливають на стабільність та ефективність усієї мережевої інфраструктури.

Для успішного проєктування важливо підібрати операційні системи, які чітко відповідатимуть функціональним завданням різних компонентів мережі. Зокрема, робочі станції повинні використовувати сучасні, інтуїтивно зрозумілі системи, які підтримують офісні програми та забезпечують високу сумісність. Сервери мають базуватися на стабільній платформі, здатній ефективно виконувати функції мережевих сервісів, а для мережевих сховищ необхідна спеціалізована система управління даними з можливістю резервного копіювання та контролем доступу. Тому цей розділ присвячено обґрунтуванню вибору операційних систем для клієнтських пристроїв, серверів і NAS, а також визначенню основних програмних засобів, які забезпечуватимуть щоденну

роботу мережі, адміністрування, обмін файлами та базове технічне обслуговування.

Одним із визначальних принципів у доборі програмного забезпечення є забезпечення узгодженості між усіма компонентами мережевої системи. Операційна система робочої станції повинна безперебійно взаємодіяти з такими функціями, як підтримка мережевих послуг, доступ до принтерів і спільних папок, віддалений доступ і інтеграція систем безпеки. У свою чергу, серверна ОС має забезпечувати підтримку необхідних мережевих ролей, бути здатною до безперервної цілодобової роботи, дозволяти гнучке адміністрування та мінімізувати навантаження на апаратну частину. У такій концепції вибір програмного забезпечення більше не є випадковим підбором інструментів — це продумана архітектурна складова корпоративної мережі.

2.5.1 Загальні вимоги до програмного середовища

Корпоративне програмне забезпечення має відповідати низці критично важливих вимог, узгоджених між собою. Насамперед, воно повинно забезпечувати стабільну та надійну роботу користувачів у повсякденному режимі, мінімізуючи ймовірність технічних збоїв, надмірно тривалих перезавантажень або виникнення конфліктів між різними системними компонентами, як-от драйверами. Крім того, вагоме значення має інтеграція актуальних механізмів забезпечення інформаційної безпеки, включно з контролем доступу до даних, комплексними технологіями шифрування, регулярними оновленнями безпеки та можливістю централізованого управління системою. Третій ключовий аспект — сумісність програмного забезпечення зі стандартними офісними, графічними та мережевими застосунками, необхідними для повсякденного функціонування підприємства.

Для компанії «Внутрішні інженерні системи» особливого значення набуває практичність запропонованих рішень у контексті їхньої експлуатації. Ураховуючи специфіку діяльності організації, де в корпоративній мережі взаємодіють спеціалісти різного профілю — зокрема адміністративний персонал, бухгалтерія, технічні працівники та інженери — операційна система на робочих станціях повинна бути інтуїтивно зрозумілою для кінцевих користувачів, підтримувати виконання загальноприйнятих офісних завдань та не вимагати довготривалого навчання. У той же час серверні компоненти системи мають бути достатньо адаптивними й функціональними, щоб технічний персонал міг ефективно налаштовувати мережеві служби, резервне копіювання даних та права доступу без зайвих технічних обмежень.

Не менш істотним фактором є економічна обґрунтованість вибору програмного забезпечення для використання в корпоративному середовищі. Надмірне зростання витрат на його придбання чи підтримку є недоцільним для підприємства. Відтак, у тих випадках, коли можливо застосувати безкоштовні або умовно безкоштовні програмні рішення без компромісів щодо їхньої якості та функціональності, такі варіанти повинні бути пріоритетними. З огляду на це запропонована модель передбачає комбіноване використання комерційного програмного забезпечення для робочих станцій — де критичними є простота в користуванні та наявність офіційної підтримки — і вільно розповсюджуваного серверного ПЗ як ефективного засобу оптимізації ліцензійних витрат.

2.5.2 Операційна система для робочих станцій

Для забезпечення ефективності роботи на робочих станціях доцільним є використання операційної системи Windows 11 Pro. Вибір цієї платформи обумовлений її сучасністю, надійною підтримкою та адаптованістю до потреб корпоративного середовища. Windows 11 Pro вдало поєднує зручність для

кінцевого користувача з корисними інструментами для системного адміністратора, забезпечуючи при цьому сумісність із широким спектром офісного, спеціалізованого та мережевого програмного забезпечення.

Однією з ключових переваг Windows 11 Pro є винятковий рівень сумісності з популярними бізнес-додатками. У корпоративних структурах широко застосовуються різні офісні пакети, системи електронного документообігу, браузерні CRM-платформи, клієнти віддаленого доступу, а також програми для роботи з PDF-документами, архіваторами та захищеного обміну файлами. З огляду на високу поширеність і тривалу підтримку цієї ОС розробниками прикладного програмного забезпечення, ризик виникнення програмних конфліктів значно знижений. Такий підхід спрощує процес налаштування та розгортання робочих місць.

Безпекові можливості Windows 11 Pro також відповідають вимогам сучасного корпоративного середовища. Серед основних функцій слід виділити підтримку UEFI Secure Boot, модуль TPM 2.0, функціонал шифрування BitLocker, політики облікових записів і гнучке керування правами доступу. Це дозволяє посилити захист робочих місць від несанкціонованого доступу, а також зберегти локальні дані від втрати у разі крадіжки пристроїв або фізичного пошкодження носіїв інформації. Крім того, регулярне оновлення безпеки ОС є важливим засобом у протидії сучасним кіберзагрозам.

З точки зору адміністративних потреб Windows 11 Pro пропонує значні переваги. Система підтримує інтеграцію до доменів, застосування групових політик, виконання віддаленого адміністрування, а також забезпечує взаємодію через PowerShell та інші стандартні інструменти технічної підтримки. Такі функції сприяють централізації управління робочими станціями, автоматизації типових налаштувань та оновлень, скорочуючи витрати часу на обслуговування користувачів.

Окремо варто зазначити продуктивність Windows 11 Pro в умовах реального офісного навантаження. Завдяки підтримці багатозадачності система

демонструє високу швидкість роботи з сучасними процесорами, значними обсягами оперативної пам’яті, швидкими SSD-накопичувачами та сучасними мережевими адаптерами. Це робить її придатною не лише для виконання рутинних офісних завдань, але й для складніших сценаріїв використання, таких як обробка великих таблиць, робота зі складною документацією, графічними редакторами чи корпоративними веб-додатками.

Таким чином, обрання операційної системи Windows 11 Pro для використання на робочих станціях є виваженим рішенням як у технічному, так і в експлуатаційному аспектах. Її впровадження гарантує зручність, стабільність і сумісність для кінцевих користувачів, одночасно забезпечуючи системним адміністраторам багатий інструментарій для ефективного управління корпоративною IT-інфраструктурою.

2.5.3 Операційна система для серверів

Для серверної мережевої інфраструктури доцільно використовувати Ubuntu Server 24.04 LTS. Цей вибір обґрунтовано стабільністю, надійністю, безпекою та придатністю системи для безперервної роботи в умовах режиму 24/7. З огляду на завдання підприємства, де сервер виконує функції центру мережевих служб, файлового сховища, платформи для віртуалізації й системи резервного керування, зазначені характеристики є найважливішими.

Ubuntu Server уникає надмірного навантаження на апаратне забезпечення через відсутність графічних компонентів, що дозволяє ефективно використовувати доступні ресурси. Це особливо критично для серверів, яким необхідно зосереджувати обчислювальну потужність на наданні мережевих послуг замість підтримки графічного інтерфейсу. Легка архітектура системи забезпечує оптимальне використання ресурсів процесора, оперативної пам’яті

та дискових підсистем, що позитивно впливає як на продуктивність, так і на стабільність роботи.

Серед суттєвих переваг Ubuntu Server виділяється високий рівень гнучкості. Операційна система підтримує широкий спектр серверних служб, таких як DHCP, DNS, SMB, FTP, SSH, платформи моніторингу, віртуалізації, контейнеризації та інші популярні рішення. Це забезпечує можливість поступового розширення функціоналу мережі підприємства без необхідності зміни програмного середовища. Таким чином, сервер може бути адаптований до конкретних потреб організації — від простого файлового сховища до комплексного центру мережевих служб.

Ще однією важливою перевагою є акцент на безпеці. ОС включає механізми розмежування прав доступу, детальне журналювання подій, оновлення безпеки та захист мережевих портів. У поєднанні із засобами контролю трафіку це дозволяє формувати безпечне середовище для управління корпоративними даними. Для підприємства, де необхідно гарантувати захист службової документації, резервних копій та конфіденційних файлів, такі аспекти мають визначальне значення.

Не варто забувати і про фінансову вигоду. Використання Ubuntu Server виключає витрати на ліцензії, що значно знижує бюджетні навантаження на реалізацію проєкту. Водночас безкоштовний статус системи не впливає на її потужність: Ubuntu Server забезпечує повноцінний набір інструментів для вирішення серверних завдань та має підтримку численної спільноти користувачів і обширної документації.

Отже, Ubuntu Server 24.04 LTS — це оптимальний варіант для реалізації серверного вузла мережі ТОВ «Внутрішні інженерні системи». Він об'єднує в собі характеристики стабільності, багатофункціональності, високого рівня безпеки та економічної ефективності.

2.5.4 Програмне забезпечення мережевого сховища

Операційна система DSM (DiskStation Manager), розроблена компанією Synology спеціально для використання в мережевих сховищах, таких як модель DS923+, забезпечує інтегроване апаратно-програмне середовище. Цей підхід дозволяє створити високоефективний інструмент для управління даними, оскільки всі компоненти працюють в тісній гармонії, що оптимізує функціональні можливості пристрою.

DSM пропонує широкий спектр інструментів для адміністрування файлів, управління користувачами, організації спільного доступу до ресурсів та виконання резервного копіювання. Ці функції є особливо цінними для корпоративних мереж, де мережеве сховище часто відіграє роль центрального вузла для обміну важливими документами, архівації робочих матеріалів та зберігання резервних копій даних. У цьому контексті система DSM наділяє адміністратора можливістю оперативно створювати спільні папки, налаштовувати права доступу, визначати квоти зберігання, застосовувати обмеження та впроваджувати політики безпеки.

Суттєвою перевагою DSM є також підтримка RAID-масивів і потужних інструментів моніторингу стану накопичувачів. Оскільки надійність збереження даних є критично важливою, система забезпечує своєчасний контроль за станом дисків, сповіщає про можливі технічні несправності та дозволяє реалізувати високонадійні структури зберігання даних. Це сприяє не лише зручності у користуванні, але також гарантує захист конфіденційної інформації від втрати або пошкодження.

Додатковою цінністю DSM є її інтуїтивно зрозумілий веб-інтерфейс, який значно спрощує процес адміністрування системи. Використання текстових команд мінімізується, що знижує бар'єр для початківців і робить рішення доступним навіть для організацій з обмеженим штатом технічного персоналу. Водночас функціональність платформи залишається досить широкою для

підтримки як базових операцій з файлами, так і більш складних завдань, таких як резервне копіювання або синхронізація даних.

2.5.6 Узгодження програмних рішень

У будь-якому проєкті критично важливим є забезпечення узгодженості програмного забезпечення на всіх рівнях. Робочі станції мають безперебійно підключатися до сервера, взаємодіяти з мережевим сховищем (NAS), використовувати спільні папки, друкувати документи, працювати з електронною поштою та мати доступ до внутрішніх сервісів. Для цього операційна система клієнтських машин, серверна ОС та програмне забезпечення NAS повинні підтримувати сумісність у протоколах, методах авторизації та способах роботи з файлами.

Комбінація Windows 11 Pro, Ubuntu Server і DSM утворює цілісну архітектуру, де кожен компонент ефективно виконує свою функцію. Клієнтські пристрої забезпечують зручність користувачів, серверна ОС організовує гнучке надання мережевих послуг, а NAS відповідає за надійне зберігання даних і резервування. Такий розподіл завдань сприяє оптимізації мережевого навантаження, спрощує адміністрування й полегшує керування інфраструктурою..

Таким чином, саме якісний вибір програмного забезпечення визначає загальну ефективність мережевого проєкту. Навіть найкраща фізична інфраструктура не зможе забезпечити комфортної роботи користувачів без правильної інтеграції операційних систем і сервісів. Тому цей етап є так само важливим, як вибір мережевого обладнання чи проєктування кабельної системи.

2.6 Тестування та налагодження мережі

Тестування та налаштування мережі є ключовим завершальним етапом технічної частини проєкту, на якому перевіряється відповідність роботи інфраструктури тому, що було заплановано під час логічного та фізичного проєктування. Саме на цьому етапі оцінюється правильність вибору активного обладнання, кабельної системи, налаштувань адресації, VLAN, маршрутизації, бездротових сегментів та програмного забезпечення. Якщо монтаж підтверджує коректність фізичних з'єднань, то тестування демонструє ефективність функціонування мережі як єдиної інтегрованої системи.

Для ТОВ «Внутрішні інженерні системи» цей етап має особливе значення, адже створена інфраструктура повинна забезпечувати безперебійну роботу адміністративного та технічного персоналу, точок доступу, серверів, мережевого сховища та периферійних пристроїв. У такій мережі недостатньо просто забезпечити фізичне з'єднання між окремими вузлами — критично важливо підтвердити коректність функціонування кожного сегмента відповідно до проєктних специфікацій. При цьому передачі даних необхідно здійснювати без втрат, затримок чи конфліктів між підмережами.

Процес тестування організовується за послідовним принципом перевірки від нижчих рівнів до вищих. Спершу проводять оцінку роботи кабельної інфраструктури, далі тестують функціонування комутаційних пристроїв, перевіряють логічну структуру мережі, маршрутизацію, доступ до серверів, роботу бездротових сегментів та мережевих сервісів. Такий підхід дозволяє оперативно локалізувати потенційні проблеми: якщо вони виникають на фізичному рівні, немає сенсу переходити до перевірки конфігурації VLAN або серверного обладнання.

2.6.1 Перевірка кабельної інфраструктури

Перший крок у діагностиці мережі — це ретельна перевірка кабельних ліній, які забезпечують фізичну основу всієї мережі. На цьому етапі необхідно переконатися в цілісності кожної лінії, правильності обтиску, відсутності розривів, коротких замикань, переплутаних пар та пошкоджених конекторів. Якщо кабельна інфраструктура змонтована з порушеннями, наступні етапи перевірки не дадуть надійного результату. Саме тому перевірці кабельної системи слід приділити пріоритетну увагу.

На практиці така перевірка здійснюється за допомогою мережевих тестерів або схожого обладнання, що дозволяє визначити правильність підключення всіх жил згідно зі схемою, відсутність помилок у обтиску і відповідність технічним параметрам. Особливо важливо тестувати кабелі, підключені до PoE-пристроїв і точок доступу. Дефекти в таких лініях можуть спричиняти не лише втрати зв’язку, але й нестабільність живлення, що значно ускладнює роботу пристроїв.

Крім того, необхідно окремо перевірити довжину кабелю на відповідність допустимим нормам і оцінити правильність його прокладання. Надмірний натяг, різкі вигини або розташування в безпосередній близькості до силових кабелів можуть не проявлятися одразу, але в довгостроковій перспективі призводять до збоїв у роботі. Саме тому кабельна система повинна розглядатися як критичний елемент інфраструктури, а не другорядна технічна деталь.

2.6.2 Перевірка активного обладнання

Після завершення перевірки кабельної інфраструктури наступним етапом стає оцінювання функціональності активного мережевого обладнання. На цьому рівні критично важливо пересвідчитися, що такі елементи, як

комутатори, маршрутизатори, точки доступу, сервери та системи зберігання даних (NAS), належним чином ініціалізуються, коректно взаємодіють із підключеними лініями, отримують постійне живлення та функціонують відповідно до попередньо заданих параметрів конфігурації. У корпоративних мережах вирішальним є забезпечення стабільної роботи активного обладнання протягом тривалого періоду без спонтанних перезавантажень чи втрати з'єднання.

Процедура перевірки комутаторів включає аналіз індикації портів, підтвердження наявності активних з'єднань, контроль правильності функціонування магістральних (uplink) і доступових (access) портів, а також перевірку справності подачі живлення через PoE (Power over Ethernet), якщо така функція підтримується. У контексті маршрутизаторів перевіряються такі аспекти, як безперешкодний доступ до Інтернету, ефективність механізмів NAT, коректність фільтрації трафіку, доступність локальних підмереж і здатність маршрутизатора впоратися з передачею даних без ознак перевантаження. Щодо точок доступу, увагу приділяють оцінюванню якості радіосигналу, стабільності підключення клієнтських пристроїв і правильності маршрутизації трафіку до внутрішньої мережі.

Окрім технічної функціональності, важливо також визначити, чи відповідає активне обладнання запланованому дизайну мережевої інфраструктури. Так, наприклад, центральні комутатори мають виконувати роль агрегаторів трафіку, а не лише слугувати проміжними вузлами передачі даних. Аналогічно, точки доступу повинні бути інтегровані у загальну архітектуру мережевої структури та працювати в рамках VLAN або серверної логіки, а не функціонувати як ізольовані одиниці. У випадку виявлення дисфункціонального пристрою або невідповідності його ролі визначеним параметрам, важливо здійснити необхідні коригувальні заходи до моменту остаточного введення мережевої системи в експлуатацію.

2.6.3 Налаштування VLAN і логічної адресації

Однією з ключових складових налаштування мережевої інфраструктури є ретельна перевірка VLAN і логічної адресації. Саме ці функціональні механізми сприяють ізоляції трафіку між різними відділами, забезпечують високу безпеку мережі та спрощують адміністрування. У процесі тестування необхідно перевірити, чи належить кожен порт комутатора до потрібної VLAN згідно із проєктною документацією, а також упевнитися, що передача трафіку між підмережами здійснюється виключно через спеціально налаштовані маршрути або дозволені шлюзи.

Для перевірки VLAN проводяться тести доступу до внутрішніх ресурсів, серверів та шлюзів із різних робочих станцій. Якщо виявляється, що співробітники одного відділу не мають доступу до своїх ресурсів або, навпаки, отримують доступ до даних інших відділів, це свідчить про проблеми в конфігурації. У таких випадках важливо проаналізувати тегування портів, режими (trunk/access), налаштування портів на комутаторах та відповідність IP-адрес заданому плану адресації.

Перевірка логічної адресації також відіграє критично важливу роль. Кожна робоча станція мусить отримати коректну IP-адресу зі своєї підмережі, разом із відповідними маскою, шлюзом і, за потреби, адресою DNS-сервера. Помилки в адресації можуть призвести до того, що користувачі матимуть доступ лише до локальних ресурсів або взагалі втратять можливість працювати в мережі. Тому тестування IP-налаштувань є не менш важливим завданням, ніж фізична перевірка кабельних з’єднань.

2.6.4 Перевірка маршрутизації та доступу до ресурсів

Після завершення налаштування VLAN і адресації обов’язково потрібно перевірити коректність маршрутизації між різними сегментами мережі. У корпоративному середовищі критично важливо забезпечити чітке дотримання правил доступу, щоб підмережі могли взаємодіяти лише відповідно до заданих політик, запобігаючи хаотичному й неконтрольованому доступу між ними. Особлива увага має бути приділена відділам, які працюють із конфіденційною інформацією, адже від налаштувань маршрутизації залежить не лише доступ до спільних ресурсів, але й рівень обмеження цього доступу.

Для оцінки функціональності мережі проводиться серія перевірок: встановлюється зв’язок між робочою станцією та маршрутизатором, тестується взаємодія станції із сервером та NAS, а також перевіряється можливість виходу у зовнішню мережу. Успішні результати тестування свідчать про те, що мережа не тільки коректно побудована фізично, але й працює відповідно до логічної моделі, закладеної у проєкті. Якщо ж в процесі перевірки виявляється неможливість доступу до окремих сервісів, необхідно провести детальний аналіз маршрутів, фільтраційних правил, налаштувань шлюзів, масок та політик доступу.

Як правило, саме на цьому етапі стає очевидним рівень якості проєктування мережі. Системний підхід до адресації та сегментації забезпечує передбачуваність роботи маршрутизації, з мінімальною потребою у корекціях. Однак якщо початковий дизайн мережі був недостатньо продуманим, тестування швидко виявить проблемні місця, які необхідно усунути до фінальної здачі проєкту в експлуатацію.

2.6.5 Тестування бездротового сегмента

Важливим етапом є перевірка бездротового сегмента мережі. Для компанії критично важливо, аби Wi-Fi забезпечував не лише можливість підключення, а й стабільну та якісну роботу в різних точках приміщення. Тому під час налаштування проводиться ретельне тестування рівня сигналу, стабільності з'єднання, швидкості передачі даних і коректності роумінгу у випадку наявності кількох точок доступу.

Кожна точка доступу повинна гармонійно інтегруватися в загальну архітектуру мережі, що дозволить обмежити доступ користувачів бездротового сегмента виключно до дозволених ресурсів. У разі потреби, їм може бути призначено окремий VLAN. Це рішення сприяє ефективному розмежуванню гостьового трафіку та внутрішнього корпоративного, що підвищує як безпеку мережі, так і її стабільність. У процесі тестування перевірки проходять не лише наявність Wi-Fi з'єднання, а й правильний розподіл трафіку по сегментах та стабільність роботи при навантаженнях.

Значення цього етапу дуже високе, адже саме бездротові мережі найчастіше використовуються в зонах відкритого доступу, для мобільних пристроїв або тимчасових підключень. Збої в роботі Wi-Fi можуть суттєво погіршити зручність роботи співробітників і вплинути на загальне сприйняття якості всієї IT-інфраструктури.

2.6.6 Налагодження серверних сервісів

Після підтвердження фізичної та логічної структури мережі настає етап перевірки роботи серверних сервісів. Цей процес охоплює тестування доступу до файлових ресурсів, мережевих папок, систем резервного копіювання, служб автентифікації, DNS, DHCP та інших критично важливих сервісів,

передбачених у проєкті. Саме цей крок дозволяє оцінити, чи здатна мережа ефективно забезпечувати щоденні потреби підприємства.

Сервери мають коректно реагувати на запити клієнтських пристроїв, надавати необхідні ресурси та забезпечувати стабільність роботи упродовж усього робочого циклу. Для систем зберігання даних (NAS) важливо перевірити доступ до файлів, відповідність прав користувачів, коректність резервного копіювання та швидкість передачі даних. Безперебійна робота серверної інфраструктури є важливим показником успішної реалізації проєкту, адже саме від серверів залежить збереження й доступ до корпоративної інформації.

Однак під час налаштування та тестування слід особливу увагу приділити продуктивності. Навіть за умови формальної працездатності сервіс може не справлятися з високим одночасним навантаженням або мати значні затримки в доступі до даних. Таким чином, тестування повинно враховувати як функціональну, так і практичну ефективність роботи мережі.

2.7 Обґрунтування вибору засобів захисту мережі

Захист мережі є ключовим елементом сучасних корпоративних проєктів, адже будь-яка мережева інфраструктура, що забезпечує доступ до внутрішніх ресурсів, користувацьких даних та зовнішніх сервісів, потребує всебічного захисту. Загрози у вигляді несанкціонованого доступу, шкідливого програмного забезпечення, помилок користувачів чи цілеспрямованих мережевих атак мають бути нейтралізовані за допомогою надійних заходів безпеки. Для ТОВ «Внутрішні інженерні системи» це завдання особливо важливе, адже у внутрішній мережі обробляються конфіденційні дані, такі як службові документи, комерційна інформація, бухгалтерські записи, проєктні файли та технічна документація.

При виборі рішень для забезпечення безпеки необхідно враховувати комплексний підхід. Захист лише зовнішніх каналів або встановлення одного антивірусного рішення не може гарантувати повної безпеки. Ефективна стратегія повинна включати багатошаровий захист: охорону робочих станцій, серверів, мережевих сховищ, а також управління маршрутизацією і сегментацією трафіку. Лише завдяки інтеграції різних компонентів системи безпеки можна створити ефективну модель, де окремі рівні доповнюють один одного та суттєво знижують ризик втрати чи компрометації даних.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з налаштування програмного забезпечення серверів

Налаштування серверного програмного забезпечення є ключовим практичним етапом при впровадженні корпоративної мережі, оскільки саме від серверної інфраструктури залежить ефективне функціонування мережевих служб, доступ користувачів до ресурсів, обмін даними, централізоване збереження інформації та управління окремими сегментами системи. У межах реалізації цього проєкту серверна частина мережі ТОВ «Внутрішні інженерні системи» була побудована на базі серверів HPE ProLiant DL380 Gen11, оснащених операційною системою Ubuntu Server 24.04 LTS, у комбінації з мережевим сховищем Synology DS923+, яке працює під управлінням DSM. Така архітектура забезпечує створення гнучкого, надійного і водночас економічно оптимального середовища для підтримки ключових бізнес-сервісів підприємства.

Перед тим як розпочати безпосередню конфігурацію серверного обладнання, необхідно переконатися в його повній готовності. Важливо впевнитися, що апаратна частина коректно змонтована, підключена до мережі, має стабільне джерело живлення й доступна для початкового налаштування. Крім того, слід перевірити наявність усіх необхідних інсталяційних носіїв, адміністративного доступу, правильність встановлення IP-адрес та дотримання розробленої раніше мережевої топології. Лише після цих попередніх етапів можна переходити до встановлення та налаштування програмного забезпечення. Недогляд або помилка на стартовому етапі можуть стати причиною серйозних збоїв у подальшій роботі всієї мережевої інфраструктури.

3.1.1 Початкове встановлення Ubuntu Server

Після увімкнення сервера HPE ProLiant DL380 Gen11 виконувалося завантаження із інсталяційного носія операційної системи Ubuntu Server 24.04 LTS. На етапі встановлення було обрано базову конфігурацію серверного режиму без використання графічного інтерфейсу. Такий підхід зумовлений пріоритетом корпоративних вимог, що передбачають забезпечення стабільності, раціональне використання ресурсів та ефективність адміністрування через консоль або віддалений доступ замість фокусування на візуальних компонентах. Ця практика є поширеною при розгортанні серверних середовищ, оскільки вона дозволяє оптимально використовувати ресурси виключно для виконання службових завдань.

Під час процесу інсталяції системи визначаються ключові параметри, такі як мова, часовий пояс, розкладка клавіатури, ім’я хосту сервера, обліковий запис адміністратора та його пароль. Особливу увагу слід приділити вибору імені хоста, адже воно слугує основним ідентифікатором сервера в мережевій інфраструктурі. Для об’єктів проєктування рекомендовано використовувати зрозуміле й логічне позначення, яке відображає функціональне призначення вузла у системі, наприклад "gateway" або "server".

По завершенні інсталяції нової системи необхідно виконати перший вхід до неї та перевірити базову коректність налаштованих параметрів. На цьому етапі доцільно провести оновлення системного програмного забезпечення для застосування актуальних пакетів безпеки та виправлення помилок. Використання команд керування пакетами дозволяє оперативно привести систему у відповідний робочий стан і підготувати її до подальшого налаштування. Варто зауважити, що встановлення найсвіжіших оновлень

одразу після інсталяції є критично важливим, оскільки початковий інсталяційний образ може містити застарілі версії програмних компонентів.

3.1.2 Налаштування мережевого інтерфейсу

Для стабільної роботи серверу необхідно забезпечити коректне налаштування мережевого інтерфейсу. У цьому проєкті сервер використовує два логічно відокремлені мережеві напрями: один інтерфейс для підключення до зовнішньої або транзитної мережі, а інший — для обслуговування внутрішнього сегмента чи службової підмережі. Така структура дозволяє ефективно розділити трафік і забезпечити безпечну взаємодію між різними вузлами.

Мережеві параметри в Ubuntu Server 24.04 LTS налаштовуються за допомогою Netplan. Ця утиліта дозволяє визначати у конфігураційному YAML-файлі IP-адреси, шлюзи, маршрути та параметри DHCP, якщо вони потрібні. Основна перевага Netplan полягає у спрощеній структурі: вся конфігурація описується в одному файлі, який можна легко модифікувати, а зміни застосовуються однією стандартною командою. Такий підхід є інтуїтивним, прозорим і повністю відповідає принципам сучасного серверного адміністрування.

Для внутрішнього інтерфейсу доцільно використовувати статичну IP-адресу, щоб забезпечити постійний доступ до сервера за одним і тим самим адресним простором. Це є критично важливим для таких задач, як підключення клієнтів, обробка DNS-запитів, передача файлів та інші службові операції. Після налаштування необхідно перевірити правильність застосування нової

конфігурації, доступність мережевих інтерфейсів і коректність роботи маршрутизації.

3.1.3 Встановлення базових сервісів

Після налаштування серверної мережі важливо встановити базовий набір інструментів і служб, які часто використовуються в адміністративній діяльності. До них належать SSH для віддаленого доступу, мережеві утиліти для діагностики стану інтерфейсів, текстові редактори, інструменти моніторингу системних ресурсів та засоби для управління пакетами. Наявність цих компонентів значно полегшує подальшу роботу адміністратора, забезпечуючи можливість виконання всіх основних завдань без потреби у фізичному доступі до серверної кімнати.

Ключову роль в адміністративному процесі відіграє OpenSSH Server. Його інсталяція дозволяє адміністратору керувати сервером віддалено, підключатися до нього з будь-якої робочої станції та виконувати команди через зашифрований канал. У корпоративному середовищі це є не просто зручністю, а критично важливим елементом для оперативного обслуговування. За допомогою SSH можна змінювати конфігурації системи, аналізувати журнали, виконувати оновлення та контролювати стан служб без необхідності фізичної присутності біля сервера.

Окрім того, варто інсталювати необхідні системні утиліти, які забезпечують перевірку мережевих з’єднань, моніторинг системного навантаження та контроль роботи окремих сервісів. Ці засоби корисні не тільки на етапі початкового налаштування серверу, але й під час повсякденної експлуатації. Вони допомагають швидко визначати причини можливих збоїв або перевіряти

коректність роботи серверних компонентів, забезпечуючи стабільну та безперебійну роботу системи.

3.1.4 Налаштування маршрутизації та NAT

Оскільки сервер у цьому проєкті виконує роль шлюзу та ключового мережевого вузла для внутрішньої інфраструктури, необхідно активувати функцію пересилання пакетів між мережевими інтерфейсами. Це дає змогу забезпечити передачу трафіку між внутрішньою підмережею та зовнішніми ресурсами, а також організувати вихід користувачів в інтернет через централізований і контрольований канал.

Для впровадження цієї функції в Linux потрібно ввімкнути IP forwarding. Після цього налаштовуються правила NAT, які дозволяють маскувати внутрішню мережеву адресацію за допомогою однієї або кількох зовнішніх IP-адрес. Ця практика є загальноприйнятим стандартом у корпоративних мережах, оскільки за її допомогою внутрішні пристрої здатні отримувати доступ до зовнішніх сервісів без прямого виставлення в інтернет, що значно покращує рівень безпеки.

Фільтрація трафіку налаштовується за допомогою nftables або іншого аналогічного інструменту. Рекомендується дозволяти лише ті порти та протоколи, які є критично необхідними для коректного функціонування сервера. Серед таких — SSH для доступу адміністраторів, DNS-запити, а також специфічні сервіси, якщо вони використовуються в межах мережі. Увесь інший трафік слід обмежувати, щоб мінімізувати поверхню атак і унеможливити несанкціонований доступ до вузла.

3.1.5 Налаштування DNS-служби

DNS є одним із ключових компонентів будь-якої мережі, оскільки відповідає за перетворення доменних імен у IP-адреси. Це дає змогу користувачам взаємодіяти з ресурсами через зрозумілі імена, уникаючи необхідності запам’ятовувати складні числові адреси. У корпоративному середовищі DNS відіграє ще важливішу роль, спрощуючи адміністрування завдяки централізованому управлінню іменами серверів, NAS, шлюзів та інших внутрішніх служб.

Для реалізації цього завдання доцільно звернутися до легкого й гнучкого інструмента DNS, такого як dnsmasq або його аналоги. Налаштування такого рішення включає вибір інтерфейсу прослуховування, визначення внутрішніх адрес, підключення зовнішніх DNS-серверів для резолвінгу та створення локальних записів для внутрішніх доменних імен. Останній пункт особливо корисний, адже локальні записи дозволяють швидко звертатися до серверів мережі за лаконічними та зручними для запам’ятовування іменами.

Під час конфігурації важливо забезпечити стабільну роботу служби, а також мінімізувати додаткове навантаження на систему. Для невеликих та середніх корпоративних мереж таке рішення є оптимальним, адже воно вдало поєднує простоту адміністрування із функціональністю, що відповідає стандартним потребам. Після запуску служби варто перевірити резолвінг як внутрішніх, так і зовнішніх доменів, а також переконатися в правильній маршрутизації запитів.

Регулярне оновлення та моніторинг DNS-записів є критично важливими, адже навіть незначні помилки у конфігурації можуть призвести до недоступності сервісів та збоїв у роботі всієї мережі.

3.1.6 Налаштування мережевого сховища Synology DS923+

Одним із ключових завдань є повне налаштування мережевого сховища Synology DS923+, яке виконує роль централізованої платформи для зберігання файлів, резервних копій і спільних ресурсів у корпоративній мережі. У процесі первинного налаштування пристрою через веб-інтерфейс DSM необхідно задати мережеві параметри, зокрема встановити статичну IP-адресу, призначити ім’я пристрою та налаштувати базові параметри безпеки. Ці дії гарантують стабільне функціонування пристрою в мережі і спрощують його подальше обслуговування.

Після завершення роботи з мережевими налаштуваннями переходять до створення RAID-масиву та файлового тому. У корпоративному середовищі рекомендовано застосовувати відмовостійкі конфігурації, наприклад RAID 5, які надають оптимальне співвідношення продуктивності, ємності та надійності. Завдяки такій конфігурації дані залишаються доступними навіть у разі виходу з ладу одного жорсткого диска, що має важливе значення для підприємств, де втрата інформації недопустима.

Наступним етапом у DSM є створення спільних папок, налаштування прав доступу для користувачів і груп, а також конфігурація служби SMB для забезпечення зручної інтеграції з робочими станціями Windows. Протокол SMB вважається одним із найбільш ефективних механізмів організації спільного доступу до файлів в офісному середовищі, оскільки дозволяє інтегрувати NAS у файлову систему користувачів максимально прозоро. Після налаштувань виконується перевірка доступу, щоб гарантувати, що всі користувачі та групи бачать лише ті ресурси, до яких вони мають авторизований доступ, і виключити можливість випадкового отримання прав на конфіденційні дані.

3.1.7 Перевірка роботи серверних сервісів

Після завершення процесу налаштування серверів обов’язковим етапом є проведення ретельного тестування всіх встановлених сервісів. До переліку обов’язкових перевірок належать тестування доступу через SSH, оцінка коректності маршрутизації, перевірка функціонування DNS, доступ до мережевого сховища даних (NAS), тестування операцій читання та запису файлів, а також аналіз стабільності роботи серверу в умовах реального навантаження. Будь-яка нестабільність у роботі хоча б одного з компонентів може негативно вплинути на функціонування всієї корпоративної мережі.

Перевірка здійснюється як безпосередньо з сервера, так і за допомогою клієнтських робочих станцій. Такий комплексний підхід дозволяє оцінити не лише технічний запуск окремих служб, але і їх фактичну доступність для кінцевих користувачів. Зокрема, потрібно переконатися, що клієнтські пристрої коректно виконують резолюцію DNS-імен, мають безперешкодний доступ до файлового сховища, здатні встановлювати віддалені підключення до серверів і не стикаються з проблемами адресації або іншими конфліктами в мережі.

У разі виявлення проблемних моментів необхідно застосувати відповідні заходи, включаючи внесення змін до конфігураційних файлів, аналіз системних журналів, корекцію прав доступу або параметрів мережевих служб. Отже, початкове налаштування серверів не може вважатися завершеним без належного етапу перевірки й тестування. Лише після усунення всіх недоліків і отримання позитивних результатів тестувань сервер може бути визнаний повністю готовим до інтеграції і експлуатації в рамках корпоративної інфраструктури.

3.2 Інструкція з налаштування активного комутаційного обладнання

Налаштування активного мережевого обладнання виконується відповідно до затверджених у проєкті схем адресації та сегментації мережі компанії ТОВ «Внутрішні інженерні системи». У запропонованій структурі кожна категорія пристроїв має свій унікальний VLAN, а IP-адреси вже чітко розподілені між підмережами. Такий підхід забезпечує можливість налаштування комутаторів, дотримуючись реальної топології без участі уявних або зайвих сегментів.

Під час конфігурації необхідно орієнтуватися виключно на затверджені елементи мережі: робочі станції, принтери, сервери, точки доступу Wi-Fi, камери відеоспостереження та керовані комутатори. Для адміністративного доступу передбачено використання службових IP-адрес, зафіксованих у таблицях адресації. Наприклад, центральний комутатор налаштовується за IP-адресою 192.168.30.2, шлюзовий сервер — за адресою 192.168.60.2. Внутрішні сервіси доступні через сервер з адресою 192.168.60.5, а бездротовим точкам доступу виділено службовий діапазон 192.168.30.10–192.168.30.11.

Усі ці адреси узгоджено з проєктною таблицею IP-адресації, тому налаштування слід виконувати строго на їхній основі, уникаючи впровадження умовних чи зайвих елементів у мережеву структуру.

3.2.1 Первинне підключення та безпечний старт

Перед початком налаштування кожний комутатор спершу підключають до джерела живлення, а також до сервісного порту адміністративної станції. Якщо пристрій використовувався раніше, варто виконати скидання до заводських налаштувань. Це особливо актуально для обладнання MikroTik, адже старі

конфігурації, такі як правила bridge, VLAN чи адресація, можуть викликати конфлікти із новою схемою мережі.

Після скидання слід задати нове ім’я для пристрою, встановити пароль адміністратора і переконатися в доступності інструментів WebFig або WinBox (залежно від моделі комутатора). Для організації зручно використовувати назви, що одразу вказують на функціональну роль пристрою. Наприклад, центральний комутатор може отримати назву CRS326-MAIN, комутатор бухгалтерії — SW-BOH, технічного відділу — SW-TECH, PoE-комутатор — SW-POE. Такий підхід спрощує ідентифікацію кожного вузла в мережі.

Наступним етапом налаштовується керуюча IP-адреса для комутатора, яка має бути уникальною. Наприклад, центральний комутатор можна призначити на адресу 192.168.30.2, комутатор бухгалтерії — на 192.168.10.3, технічного відділу — на 192.168.20.2, а PoE-комутатор — на 192.168.30.2 чи іншу адресу з адміністративної підмережі відповідно до схеми. Важливо, щоб всі пристрої мали чіткі службові адреси та уникали дублювання IP-адрес інших вузлів у мережі.

3.2.2 Налаштування центрального комутатора

Центральний комутатор є ключовим елементом комутаційної схеми, з якого починається логічне об'єднання всієї інфраструктури мережі. Для реалізації цього підходу створюється міст (bridge), до якого підключаються всі необхідні фізичні порти. Порти, що ведуть до комутаторів доступу, налаштовуються в режимі trunk, тоді як порти для кінцевих пристроїв або серверних вузлів виступають у ролі access-портів і отримують відповідний VLAN ID.

У нашій мережі до центрального комутатора можуть бути підключені: шлюзовий сервер з IP-адресою 192.168.60.2, серверний вузол 192.168.60.5, PoE-

комутатор SW_POE з адресою 192.168.30.2, а також uplink-порти комутаторів доступу для VLAN 10, 20, 30, 31 і 40. Кожен із зазначених VLAN відповідає конкретній підмережі проєкту: VLAN 10 — фінансовий відділ, VLAN 20 — технічний відділ, VLAN 30 — адміністрування й управління, VLAN 31 — гостьовий Wi-Fi, VLAN 40 — служба охорони.

Після створення bridge потрібно визначити правила для роботи з VLAN. Для trunk-портів у таблиці VLAN задаються tagged-значення, що дозволяє передавати трафік кількох VLAN одночасно. У випадку access-портів застосовуються untagged-значення разом із призначенням PVID для відповідного VLAN. Наприклад, якщо до порту підключено комутатор бухгалтерії SW_2 із IP-адресою 192.168.10.3, його uplink-порт має нести трафік VLAN 10. Водночас кінцеві порти для роботи пристроїв WS_6–WS_9 і принтера PR_3 налаштовуються в режимі access у межах цього ж сегмента. Аналогічно для технічного відділу: доступ повинні забезпечувати access-порти для пристроїв WS_10–WS_17 і PR_4 у межах VLAN 20.

Наступний крок — активація функції VLAN filtering на центральному комутаторі. Цей параметр слід увімкнути лише після повного і коректного налаштування таблиці VLAN. Передчасна активація може спричинити порушення зв’язку із пристроєм через помилки у конфігурації tagged/untagged-параметрів, що повністю позбавить доступу до комутатора. Тому рекомендується виконувати процес налаштування поетапно з обов'язковою перевіркою кожного виконаного кроку, щоб мінімізувати ризики технічних збоїв.

Таким чином, правильне налаштування центрального комутатора та його портів забезпечує узгоджену роботу всієї мережевої інфраструктури, створюючи надійну основу для стабільного функціонування корпоративних сервісів.

3.2.3 Налаштування комутаторів доступу

У нашому проєкті комутатори доступу розташовуються в окремих функціональних зонах: бухгалтерія, фінансовий відділ, технічний відділ, а також серверна/патч-панельна зона. На цих комутаторах порти для робочих станцій налаштовуються у режимі access для відповідного VLAN, а uplink-порти працюють у режимі trunk. Це означає, наприклад, що комутатор SW_1, розташований у кабінеті директора, обслуговує робочі станції WS_1 і PR_1 у VLAN 10; SW_2 обслуговує бухгалтерські робочі місця WS_6-WS_9 та PR_3; а SW_3 забезпечує роботу технічного відділу (WS_10-WS_17 і PR_4).

Управляючі IP-адреси для цих комутаторів розподіляються таким чином: для SW_1 — 192.168.10.2, для SW_2 — 192.168.10.3, а для SW_3 — 192.168.20.2. Такий підхід відповідає IP-таблиці проєкту й дозволяє швидко ідентифікувати та адмініструвати кожен вузол у мережі. У випадку, якщо комутатор підтримує Web-інтерфейс, необхідно задати IP-адресу, маску підмережі, шлюз та режими VLAN для відповідних портів. Якщо ж використовується SwOS без Web-інтерфейсу, то основну увагу слід приділити налаштуванню таблиці VLAN, параметрам портів і PVID.

У процесі налаштування важливо забезпечити, щоб порти для підключення до робочих станцій приймали тільки untagged-трафік відповідного VLAN. Наприклад, порт для підключення WS_10 у технічному відділі має бути прив’язаний до VLAN 20, тоді як порт для WS_30 у бухгалтерії — до VLAN 10. Це потрібно для забезпечення коректної роботи кінцевих пристроїв без необхідності обробляти теги VLAN; вони повинні отримувати лише свою робочу підмережу. При цьому uplink-порти до центрального комутатора мають бути налаштовані на передачу tagged-трафіку з кількох VLAN одночасно.

Після завершення конфігурації кожного комутатора слід перевірити доступність всіх відповідних вузлів у мережі згідно з проєктом. Наприклад, у

сегменті FIN повинні працювати WS_1-WS_9 і принтери PR_1-PR_3; у сегменті TECH — WS_10-WS_17 і PR_4; а у VLAN 40 — WS_18 і камери CAM_1-CAM_3. У разі появи додаткових або невідомих пристроїв це може свідчити про неправильне підключення до порту або помилкове налаштування VLAN.

3.2.4 Налаштування PoE-комутатора і точки доступу

У представленій мережевій архітектурі PoE-комутатор виконує завдання підтримки доступу до точок доступу AP_1, AP_2 та інших PoE-сумісних пристроїв, якщо їх використання передбачено в проєкті. Його IP-адреса повинна бути інтегрована в службову або адміністративну підмережу. Як приклад, можна розглянути адресу 192.168.30.2. Особливу увагу слід приділити налаштуванню портів живлення комутатора, оскільки частина портів може бути спеціально призначена для живлення PoE точок доступу, тоді як інші порти функціонуватимуть як uplink-з'єднання.

Для забезпечення коректного функціонування AP_1 та AP_2 необхідно підключати їх безпосередньо до PoE-портів, щоб уникнути необхідності застосування окремих блоків живлення. При конфігурації бездротових пристроїв кожен з них отримує статичні адреси в межах тієї ж підмережі, наприклад, 192.168.30.10 і 192.168.30.11, або інші IP-адреси, визначені у заданій адресній схемі. Це сприяє центральному управлінню Wi-Fi системою та спрощує пошук і обслуговування точок доступу.

У разі, якщо точки доступу працюють у VLAN 30 або VLAN 31, критично підтримувати відповідність конфігурації uplink-портів комутатора параметрам VLAN. Зокрема, необхідно забезпечити проходження потрібного VLAN через відповідний порт. Для внутрішньої Wi-Fi мережі зазвичай використовується VLAN 30, у той час як для гостьового доступу виділяється VLAN 31 з повною

сегментаційною ізоляцією від внутрішніх корпоративних ресурсів. У такому випадку PoE-комутатор виконує не лише функцію фізичного розподілу мережі, але й виступає інструментом логічного сегментування бездротової інфраструктури.

3.2.5 Практична перевірка портів і адрес

Після завершення конфігурації необхідно ретельно перевірити всі вузли мережі, забезпечуючи відповідність запланованій структурі проєкту. Кожен порт і VLAN слід звірити з таблицею адресації. Наприклад, якщо порт комутатора відділу бухгалтерії відповідає робочій станції WS_8 з адресою 192.168.10.32, то підключення ноутбука до цього порту повинно забезпечувати отримання IP-адреси з VLAN 10, а не VLAN 20 чи 30. Аналогічно, WS_15 у технічному відділі має отримувати адресу з діапазону 192.168.20.x.

Уся адресація в мережі повинна строго відповідати попередньо визначеній таблиці. У проєкті не повинно бути «фантомних» елементів, таких як WS_38, якщо вони не передбачені під час планування. Симетричність мережі полягає в суворому дотриманні затвердженої схеми: 18 комп’ютерів, службові комутатори, по одному чи двом принтерам на відділ, точки доступу (AP), камери спостереження, сервер і файлове сховище (NAS). Така структура точно відповідає реальним потребам підприємства та запобігає необґрунтованому ускладненню й перевантаженню мережі.

Для перевірки налаштування рекомендується застосовувати простий і ефективний метод контролю: послідовна перевірка п'яти ключових елементів — порт, VLAN, IP-адреса, доступ до шлюзу та доступ до сервера. Якщо всі ці параметри співпадають із запланованими, це означає, що комутаційна частина

налаштована коректно. У разі виявлення розбіжностей налаштування необхідно виправити, допоки вони повністю не відповідатимуть проєктним вимогам.

3.3 Інструкція з використання тестових наборів та тестових програм

Тестування мережі є невід'ємною складовою завершального етапу після монтажу та налаштування обладнання, адже саме цей процес підтверджує відповідність реальної інфраструктури задуму проєкту. У межах цього дипломного проєкту тестування повинно проводитися в повній відповідності до конфігурації побудованої мережі ТОВ «Внутрішні інженерні системи». Це передбачає врахування реальних вузлів, актуальної IP-адресації та фактичної структури VLAN. Іншими словами, об'єктом перевірки має стати не умовна мережа, а ті конкретні сегменти, які заплановані у проєкті: 18 робочих станцій, 4 принтери, комутатори доступу, центральний комутатор, точки доступу, серверний вузол, NAS, а також сегменти для охоронних систем і Wi-Fi.

З практичної точки зору засоби тестування поділяються на дві основні категорії. Перша — це апаратні інструменти для аналізу кабельної інфраструктури, друга — програмні рішення для перевірки логіки мережевих процесів: маршрутизації, функціональності сервісів, доступності та пропускної здатності. Лише гармонійне поєднання цих підходів забезпечує комплексний результат. Адже навіть за ідеального стану кабелів помилки у налаштуваннях VLAN або маршрутизації можуть призвести до порушення роботи мережі. Відповідно, тестування слід проводити поетапно та з урахуванням усіх деталей.

3.3.1 Використання апаратних тестових наборів

Для первинної діагностики фізичної інфраструктури мережі використовується тестер на кшталт Fluke Networks MicroScanner MS2 або інший аналогічний прилад із подібним набором функцій. Цей пристрій дозволяє оперативно оцінити стан кабельної системи, зокрема перевірити цілісність проводів, правильність їхнього підключення, наявність обривів, коротких замикань, переплутаних пар і базові параметри лінії. У практичній роботі це є одним із найбільш зручних інструментів, адже він дає змогу швидко з’ясувати стан кабелю без потреби у повному розбиранні мережевих підключень.

Щоб виконати перевірку за допомогою такого тестера, основний модуль підключається до одного кінця кабелю, а віддалений модуль — до іншого. Після запуску тестування пристрій відображає інформацію про те, чи всі жили кабелю під’єднані коректно, чи відповідає розпінування стандарту T568B і чи відсутні пропуски чи переплутування у парах. У разі виникнення помилки під час розпінування дисплей пристрою покаже невідповідність порядкових номерів жил. Така перевірка є надзвичайно корисною для компонентів мережі, які з’єднують робочі станції (WS_1–WS_18), принтери (PR_1–PR_4), точки доступу (AP_1, AP_2) та камери спостереження (CAM_1–CAM_3).

Окрему увагу слід приділяти перевірці кабелів, що постачають живлення до PoE-пристроїв, адже для таких компонентів якість провідника впливає не лише на передачу даних, але й на стабільність живлення. Якщо у лінії спостерігається підвищений опір, пошкодження жил або проблеми зі стабільністю контакту, це може стати причиною періодичних збоїв роботи обладнання, як-от камер чи точок доступу. Тому PoE-кабелі до пристроїв AP_1, AP_2 та CAM_1–CAM_3 слід тестувати із особливою ретельністю.

Додатковою функцією професійних тестових наборів є визначення довжини лінії або виявлення інших її характеристик. Для офісної мережі це важливо не стільки з точки зору точних вимірів, скільки для підтвердження того, що довжина кабелю не перевищує припустимих нормативів і не має прихованих дефектів. У процесі перевірки бажано одразу документально фіксувати результати тестування у робочій таблиці, щоб кожна з ліній мала чітке підтвердження своєї придатності для експлуатації.

3.3.2 Перевірка кабельних ліній у реальній мережі

Після первинної апаратної перевірки слід ретельно пройтися по всіх лініях мережі, звіряючись із таблицею IP-адресації. Цей процес передбачає перевірку кожного вузла з урахуванням його відповідності VLAN, підмережі та IP-адреси. Наприклад, для вузлів фінансового сегмента — WS_1, WS_2, WS_3, WS_4, WS_5 та PR_1, PR_2 — необхідно підтвердити їхню приналежність до VLAN 10 і перевірити отримання адрес з підмережі 192.168.10.0/24. В свою чергу, для бухгалтерії слід перевірити вузли WS_6, WS_7, WS_8, WS_9 і PR_3, які також мають належати до VLAN 10, однак розташовуватись на окремих робочих місцях і бути під'єднаними до визначених портів комутаторів.

Для технічного відділу перевіряються вузли WS_10–WS_17 та PR_4, які потрібно прив’язати до VLAN 20 з адресацією у межах 192.168.20.x. Окрему увагу слід приділити робочій станції охорони WS_18 у VLAN 40 з IP-адресою 192.168.40.10, а також камерам CAM_1, CAM_2 та CAM_3 у тому самому сегменті. Уся ця перевірка має на меті встановити, чи відповідає фізичне підключення логічному плану мережі. У разі помилкового підключення порту до неправильного VLAN це відразу проявиться у вигляді хибної адреси або відсутності зв’язку зі шлюзом.

На практиці важливо не лише переконатися в наявності з’єднання, але й перевірити правильність маршрутизації. Наприклад, робоча станція у VLAN 10 повинна «бачити» шлюз 192.168.10.1 і використовувати DNS 192.168.60.2. У свою чергу, пристрої у VLAN 20 мають працювати через шлюз 192.168.20.1. Якщо ж шлюз не відповідає чи IP-адреса не співпадає із заданою в таблиці, необхідно переглянути конфігурацію відповідного комутатора та параметри мережевого вузла для усунення несправностей.

3.3.3 Використання програмних тестів і утиліт

Після завершення перевірки фізичної частини мережі необхідно скористатися програмними інструментами для діагностики та контролю логіки її функціонування. До основних утиліт для тестування належать: ping, tracert (або traceroute), ipconfig (або ifconfig), nslookup (або dig), netstat, route і iPerf3. Кожна з цих програм має своє призначення та надає змогу перевіряти певні аспекти роботи мережі.

Команда ping використовується для перевірки доступності мережевих вузлів. Наприклад, з робочої станції у сегменті VLAN 10 можна протестувати доступність шлюзу 192.168.10.1, DNS-сервера 192.168.60.2, сервера 192.168.60.5 і NAS. Якщо відповіді надходять без втрат, а затримка є нормальною, це свідчить про базову працездатність мережі. У разі втрат пакетів або значної затримки слід досліджувати причини, які можуть полягати у несправності кабелів, некоректній роботі комутатора чи проблемах маршрутизації.

Команда tracert допомагає проаналізувати маршрут передавання трафіку до кінцевого вузла. Цей інструмент особливо корисний для діагностики у мережах із VLAN, оскільки дозволяє відстежити проходження пакетів через шлюзи та

проміжні маршрутизатори. Якщо маршрут не відповідає очікуваній логіці чи пакети зупиняються в процесі передавання, це вказує на можливі помилки у налаштуваннях VLAN, trunk-з'єднань або маршрутизації на пристроях.

Утиліти ipconfig або ifconfig потрібні для перевірки IP-адреси пристрою, визначення її відповідності потрібній підмережі, а також правильності налаштування шлюзу та DNS. Це особливо критично, якщо кожен сегмент мережі має свої унікальні адресні простори, наприклад: - 192.168.10.x — для фінансового відділу; - 192.168.20.x — для IT-відділу; - 192.168.30.x — для адміністративного персоналу; - 192.168.31.x — для гостьового Wi-Fi; - 192.168.40.x — для систем безпеки.

Якщо IP-адреса пристрою не відповідає зазначеній сегментації, є підстави вважати, що DHCP налаштований неправильно або порт комутатора підключено до невірного VLAN.

Інструменти nslookup чи dig призначені для тестування коректності роботи DNS-серверів. Наприклад, якщо в мережі зареєстровано імена gateway.webtop або nas.webtop, вони мають належним чином перетворюватися у відповідні IP-адреси, наприклад 192.168.60.2 або 192.168.60.5. Це спрощує доступ до службових ресурсів як для кінцевих користувачів, так і для адміністраторів.

Команди netstat та route дозволяють аналізувати відкриті підключення та маршрутизацію в мережі, а утиліта iPerf3 використовується для вимірювання пропускної здатності між різними вузлами. Особливо цінно використовувати iPerf3 для перевірки міжсегментної швидкості передачі даних, що допомагає виявити потенційні проблеми на trunk-лініях або між сервером і комутатором. Якщо результати тестування показують значно нижчий рівень пропускної здатності, ніж очікувалося, це свідчить про наявність вузьких місць у мережі, які слід усунути.

3.3.4 Перевірка відповідності VLAN і таблиці адресації

Окремою та важливою частиною тестування є перевірка відповідності фактичної роботи мережі початковому проєкту, зокрема звірка IP-адресації та VLAN. Саме на цьому етапі потрібно впевнитися, що кожен вузол отримав свою передбачену адресу. Наприклад, у робочій групі SW_1 повинен бути налаштований на 192.168.10.2, WS_1 — на 192.168.10.10, PR_1 — на 192.168.10.11, а роль шлюзу виконує пристрій із адресою 192.168.10.1. Аналогічно, для технічного відділу повинно бути забезпечено, щоб WS_10 отримував адресу 192.168.20.10, а PR_4 — 192.168.20.18.

Сегмент адміністрування та служби комутації також передбачає чітко визначений розподіл адрес. Наприклад, комутатор SW_POE повинен працювати на 192.168.30.2, точки доступу AP_1 і AP_2 — на 192.168.30.10 і 192.168.30.11 відповідно, а сервери або шлюзи у цьому сегменті можуть мати адреси 192.168.60.2 і 192.168.60.5 залежно від своїх функцій. Гостьова мережа організована у підмережі 192.168.31.0/24, а для охоронного сегмента виділено окремий діапазон — 192.168.40.0/24. Усі ці параметри необхідно перевірити під час тестування не лише теоретично, але й безпосередньо на обладнанні.

Якщо виявиться невідповідність, потрібно одразу порівняти реальний стан із таблицею портів і налаштувань. Наприклад, якщо WS_16 отримав адресу поза діапазоном 192.168.20.0/24, це вказує на помилки в налаштуванні порту або некоректний PVID для відповідного VLAN. З цієї причини програмні тести завжди повинні виконуватися в комплексі з перевіркою фізичної топології комутації, щоб уникнути невідповідностей і забезпечити коректну роботу мережі.

3.3.5 Перевірка результатів і документування

Результати тестування варто записувати у робочому журналі або електронній таблиці для забезпечення системності та зручності аналізу. У цьому документі рекомендовано вказувати назву пристрою, його IP-адресу, VLAN, результати перевірки ping, доступ до сервера, підключення до NAS та стан фізичного кабелю кожного вузла мережі. Такий формат дозволяє створити цілісне уявлення про мережеву інфраструктуру і забезпечує можливість швидко повернутися до перевірки при виникненні змін або помилок.

Особливо важливим буде документування для дипломного проєкту, адже воно демонструє структурований і професійний підхід до виконання завдань. Якщо після монтажу та налаштування мережа грамотно протестована й оформлена в документах, це підтверджує завершеність інженерного циклу, а не демонструє випадково зібрану систему. Окрім того, для підприємства подібна документація матиме довгострокову користь: вона значно полегшить підтримку та обслуговування створеної інфраструктури навіть по завершенню роботи над дипломною частиною.

3.4 Інструкція по налаштуванню засобів захисту мережі

Налаштування засобів захисту мережі є ключовим етапом у впровадженні корпоративної інфраструктури, адже саме на цьому рівні формується стійкість системи до несанкціонованого доступу, збоїв, людських помилок та впливу шкідливого софту. У проєкті ТОВ «Внутрішні інженерні системи» захист орієнтовано на багаторівневий підхід, що включає безпеку робочих станцій, серверного вузла, мережевого сховища, сегментацію за VLAN, контроль

доступу між сегментами та резервування даних. Цей підхід оптимально підходить для невеликих і середніх корпоративних мереж, оскільки він забезпечує баланс між простотою адміністрування та високим рівнем безпеки.

Перед початком налаштувань важливо переконатися, що мережа вже діє згідно з затвердженою схемою адресації. Зокрема, фінансовий сегмент має користуватися підмережею 192.168.10.0/24, технічний — 192.168.20.0/24, адміністративний і службовий — 192.168.30.0/24, гостьовий Wi-Fi — 192.168.31.0/24, а охоронний — 192.168.40.0/24. Така логічна структура дозволяє будувати захист систематично, виходячи з чітко визначених зон довіри, а не випадкових рішень.

3.4.1 Захист робочих станцій

Перший рівень захисту починається з робочих станцій, адже саме вони найчастіше виступають джерелом потенційних загроз через активність користувачів, підключення зовнішніх пристроїв, завантаження файлів або взаємодію з мережевими ресурсами. У рамках нашого проєкту робочі місця WS_1-WS_18 слід захистити стандартними інструментами операційної системи: вбудованим брандмауером, антивірусним забезпеченням та обмежувальними політиками доступу.

Для станцій, що працюють на базі Windows 11 Pro, доцільно увімкнути Microsoft Defender і налаштувати брандмауер Windows таким чином, щоб залишити тільки ті правила, які необхідні для коректної роботи з мережевими ресурсами, друкарськими пристроями та файловими сервісами. Якщо немає потреби в прямому доступі до адміністративних портів, їх слід заблокувати. Це особливо актуально для офісного середовища, де працівники можуть мати справу з конфіденційними фінансовими або технічними даними.

Крім того, варто використовувати для робочих станцій локальні облікові записи з мінімальними правами доступу або доменні облікові записи зі строго обмеженими привілеями. Такий підхід мінімізує ризик ненавмисних або свідомих змін у важливих системних параметрах з боку користувачів. Це має особливе значення для комп'ютерів директора, працівників бухгалтерії та технічного відділу, оскільки саме на цих пристроях здійснюється доступ до різноманітних груп чутливих даних.

3.4.2 Захист серверного вузла

Серверний вузол є центральним елементом мережі, тому до його безпеки висуваються найвищі вимоги. У рамках нашого проєкту сервер на базі Ubuntu Server 24.04 LTS має бути захищений на рівні системних служб, мережевих правил, облікових записів та доступу до ресурсів. Одним із першочергових завдань є обмеження відкритих портів і активація лише тих сервісів, які дійсно необхідні для роботи: SSH, DNS, маршрутизація, а за потреби — файлові чи внутрішньомережеві функції.

Для забезпечення безпеки в Linux доцільно використовувати механізм фільтрації, наприклад nftables. У налаштуваннях слід чітко визначити правила, які пропускають вхідний трафік лише з відповідних сегментів мережі, таких як VLAN 10, VLAN 20 або VLAN 30, відповідно до зон, зв'язаних із сервером. Трафік з інших підмереж варто обмежувати, застосовуючи принцип мінімально необхідних прав. Такий метод не тільки зменшує можливості для потенційних атак, але й відповідає основним принципам кібербезпеки.

Для віддаленого доступу через SSH варто впровадити автентифікацію за ключем, що є безпечнішим варіантом у порівнянні з використанням лише пароля. Це значно ускладнює несанкціонований доступ до адміністративного

каналу сервера. Бажано також змінити стандартний порт SSH або обмежити доступ до нього виключно для адміністративної підмережі. Важливо, щоб в рамках дипломного проєкту було продемонстровано не тільки можливість використання SSH, але й його грамотне та безпечне налаштування, яке відповідає найкращим практикам кіберзахисту.

3.4.3 Захист мережевого сховища NAS

Мережеве сховище Synology DS923+ використовується як платформа для зберігання спільних файлів і резервних копій, тож його безпека має бути пріоритетом. Для початку рекомендується встановити статичну IP-адресу для NAS, обмежити доступ лише до необхідних VLAN і створити спільні папки з чітко визначеними правами доступу для окремих груп користувачів. Наприклад, фінансовий відділ повинен мати доступ лише до своїх ресурсів, технічний відділ — до своїх, тоді як адміністрація має мати розширені права керування.

У системі DSM варто активувати автентифікацію користувачів, змінити стандартні облікові записи адміністратора та, за можливості, відключити анонімний доступ. Особливу увагу слід приділити також увімкненню функції журналювання подій. Це дозволить відстежувати, хто, коли і які дії виконував із файлами чи папками. Такий підхід є надзвичайно важливим у корпоративному середовищі, де зберігаються критично важливі документи та резервні дані.

Ще одним невід’ємним елементом захисту NAS є організація регулярного резервного копіювання. Це допоможе мінімізувати наслідки технічних збоїв або атак шкідливого програмного забезпечення. У разі випадкового видалення або пошкодження даних можливість швидкого відновлення з резервної копії

гарантує безперервність бізнес-процесів. Таким чином, резервне копіювання слід розглядати не як додатковий захід, а як ключовий компонент комплексної стратегії безпеки.

3.4.4 Сегментація і міжмережевий контроль

Одним із ключових засобів забезпечення безпеки в рамках проєкту є використання сегментації мережі за допомогою VLAN. Поділ на VLAN 10, 20, 30, 31 і 40 дозволяє створити ізольовані сегменти для фінансового, технічного, адміністративного, гостьового і охоронного відділів. Це забезпечує мінімізацію взаємодії між пристроями різних груп у межах мережі, якщо лише такі дії не прописані в переліку дозволених правил доступу.

Для контролю міжсегментного доступу можна використовувати шлюз або маршрутизуючий сервер. Наприклад, робочі станції фінансового відділу можуть отримати повноваження доступу до NAS-сховища чи принтерів, але водночас залишатись відокремленими від гостьового Wi-Fi та систем відеоспостереження. Гостьовий VLAN 31 передбачено для максимальної ізоляції: його призначенням є лише вихід в інтернет без доступу до жодних внутрішніх ресурсів. У випадку з охоронним VLAN 40, навпаки, необхідно надати доступ до спеціалізованих служб або архівів відеозаписів, ізолюючи при цьому цей сегмент від офісних робочих станцій.

Такий підхід до сегментації значно знижує ризик поширення загроз по внутрішній мережі в разі компрометації одного з вузлів. Наприклад, якщо один із пристроїв гостьової мережі буде заражений шкідливим програмним забезпеченням, це не вплине безпосередньо на фінансовий відділ або серверний сегмент. Отже, VLAN у цьому проєкті виступає не лише інструментом для

впорядкування мережевої інфраструктури, а ще й ефективним елементом захисту інформаційної безпеки.

3.4.5 Захист бездротового сегмента

Особливу увагу необхідно зосередити на налаштуванні точок доступу AP_1 та AP_2, оскільки бездротовий сегмент мережі є одним із найбільш вразливих у корпоративному середовищі. Для забезпечення високого рівня безпеки Wi-Fi слід використовувати сучасні протоколи шифрування, такі як WPA2 або WPA3, впроваджувати складні паролі, а також створювати окремі профілі для внутрішньої та гостьової мережі, якщо це можливо. Доступ до внутрішнього SSID має бути дозволений виключно співробітникам, тоді як гостьовий має бути цілком ізольований від корпоративних ресурсів.

На точках доступу варто відключити небажані функції, які не є критично необхідними для виконання завдань проєкту. Крім того, слід обмежити доступ до адміністративного інтерфейсу, дозволяючи його лише з адрес службової підмережі. У разі використання VLAN необхідно переконатися, що внутрішній та гостьовий VLAN чітко розділені. Помилка в цьому налаштуванні може призвести до доступу гостьових користувачів до корпоративних ресурсів, чого слід категорично уникати.

Також важливо використовувати унікальні назви мереж та не залишати стандартні заводські конфігурації. Це не лише полегшує адміністрування, але й покращує контроль над тим, хто саме отримує доступ до мережі. Для компаній із постійною офісною роботою такі підходи мають особливе значення, адже бездротовий доступ часто слугує першим пунктом входу до внутрішньої інфраструктури.

3.4.6 Резервне копіювання і відновлення

Захист мережевої інфраструктури повинен реалізовуватися не лише засобами фільтрації та контролю доступу, але й включати ефективні механізми для відновлення даних у разі збоїв. У межах цього проєкту до процесу резервного копіювання необхідно залучити як файловий сервер, так і найбільш критично важливі робочі папки. У якості ключового або проміжного елементу резервування може бути використаний мережевий накопичувач (Network Attached Storage, NAS), який також може слугувати сховищем для архівів конфігурацій мережевого обладнання.

Доцільним є здійснення періодичного резервування конфігурацій комутаторів, серверних служб, таблиць маршрутизації та інших важливих параметрів налаштувань. У разі технічного збою або помилок людського фактора оперативне відновлення цих даних сприятиме мінімізації простоїв системи. У корпоративному середовищі така стратегія має безпосередній економічний вплив, дозволяючи суттєво зменшити втрати, спричинені незапланованими зупинками роботи.

Для підвищення надійності доцільно використовувати принцип кількох копій, передбачаючи окреме зберігання основних і резервних даних. Це мінімізує можливість втрати інформації у випадку несправності носія або обладнання. Таким чином, резервне копіювання не слід розглядати як додаткову функцію, а як ключовий елемент загальної системи захисту.

Важливим елементом стратегії резервування є автоматизація процесів, що дозволяє зменшити ризик людських помилок та забезпечити своєчасне створення копій без додаткового навантаження на персонал.

3.5 Інструкція з експлуатації та моніторингу в мережі

Етап експлуатації та моніторингу мережі завершує процес практичної реалізації корпоративної інфраструктури, адже саме в цей момент система переходить із режиму налаштувань до повноцінної щоденної роботи. Для ТОВ «Внутрішні інженерні системи» важливо не лише коректно впровадити мережу згідно з проєктом, але й гарантувати її стабільне функціонування, здійснювати постійний контроль стану ключових вузлів, оперативно виявляти несправності та своєчасно реагувати на можливі зміни. Ця інструкція розроблена для опису правил щоденної експлуатації, періодичного моніторингу та перевірки основних мережевих компонентів.

Перед початком експлуатації необхідно впевнитись, що всі вузли функціонують у штатному режимі: робочі станції успішно отримують IP-адреси відповідних підмереж, комутатори доступні через службові IP, сервери забезпечують коректну роботу сервісів, а NAS-сховища і точки доступу працюють без жодних збоїв. Надзвичайно важливим є дотримання узгодженості між фактичною роботою мережі та проєктною таблицею адресації. У цій інфраструктурі використовуються такі IP-сегменти: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, 192.168.31.0/24, 192.168.40.0/24, а також резервована службова частина мережі для серверних ресурсів.

3.5.1 Щоденна перевірка мережі

Щоденна експлуатація розпочинається з проведення швидкої перевірки доступності основних мережевих вузлів. Адміністратору або відповідальній

особі необхідно переконатись у коректній роботі центрального комутатора, сервера, NAS, точок доступу та критичних робочих станцій. Для цього достатньо виконати перевірку з використанням ping, оцінити стан індикаторів портів, перевірити наявність підключення користувачів до мережі та доступ до внутрішніх ресурсів.

Особливу увагу треба приділяти вузлам, які забезпечують виконання ключових бізнес-процесів компанії. Наприклад, для фінансового відділу це робочі станції WS_1–WS_5 та принтери PR_1 і PR_2, для бухгалтерії — WS_6–WS_9 і PR_3, для технічного відділу — WS_10–WS_17 і PR_4, а для охорони — WS_18 та камери спостереження CAM_1–CAM_3. У разі виявлення недоступності або нестабільної роботи будь-якого з цих вузлів необхідно якомога швидше локалізувати причину проблеми та усунути її.

Також під час щоденної перевірки слід контролювати правильність IP-адресації. Кожен користувач повинен отримати саме ту IP-адресу, яка відповідає його VLAN. Наприклад, адреси фінансового сегмента мають перебувати в діапазоні 192.168.10.x, технічного — 192.168.20.x, адміністративно-службового — 192.168.30.x, гостьового — 192.168.31.x, а охоронного — 192.168.40.x. Якщо IP-адреса не відповідає очікуваній, це може свідчити про проблеми з DHCP-сервером, налаштуванням портів комутатора або неправильну VLAN-прив’язку, що потребує негайного аналізу та виправлення.

3.5.2 Моніторинг активного обладнання

Активні мережеві пристрої, такі як комутатори, точки доступу та серверні вузли, потребують регулярного й детального моніторингу для забезпечення їх

стабільної роботи. У процесі експлуатації доцільно періодично перевіряти стан портів, наявність лінку, рівень помилок, завантаженість каналів і загальний функціональний стан обладнання. Для пристроїв MikroTik ці завдання можна виконувати за допомогою WebFig, WinBox або інтерфейсу командного рядка (CLI), а для серверних систем застосовуються SSH, журнали подій і спеціалізовані інструменти моніторингу.

Центральний комутатор CRS326-24G-2SRM має забезпечувати стабільність trunk-з’єднань і коректну маршрутизацію трафіку між VLAN. Також необхідно регулярно перевіряти комутатори доступу CSS318-16G-2SIN на правильність налаштування портів, що особливо важливо при підключенні до них робочих станцій чи периферійних пристроїв, таких як принтери. Для точок доступу cAP ax, AP_1 і AP_2 особливу увагу слід приділяти силі бездротового сигналу, чисельності активних клієнтів та справності PoE-живлення.

У контексті управління бездротовою мережею критично важливо моніторити можливе перевантаження точок доступу та оцінювати якість сигналу в різних частинах приміщення. Якщо користувачі стикаються із проблемами, такими як повільна швидкість з'єднання або нестабільність мережі, першочергово потрібно проаналізувати фізичне розташування точки доступу, рівень сигналу, навантаження на канал і наявність джерел інтерференції. Завдяки таким заходам більшість потенційних перебоїв можна запобігти ще до того, як вони перетворяться на серйозні проблеми.

3.5.3 Моніторинг серверів і сервісів

У контексті адміністрування мережевих інфраструктур серверна складова повинна підлягати окремому та ретельному моніторингу, адже вона виконує критичну функцію забезпечення доступу до шлюзу, DNS-серверів, файлових

ресурсів та системного управління. Зокрема, на сервері з операційною системою Ubuntu Server 24.04 LTS необхідно здійснювати постійний контроль за такими параметрами, як рівень завантаженості центрального процесора, обсяг використання оперативної пам’яті, рівень заповнення дискового простору, а також стан ключових служб, які включають SSH, DNS, NAT та правила мережевої безпеки. Для забезпечення належного моніторингу рекомендується застосовувати системні журнали, спеціалізоване програмне забезпечення для відстеження стану системи, а також інструменти для оперативного сповіщення про виникнення помилок.

Окремої уваги потребує мережеве сховище Synology DS923+, яке також повинно знаходитися під регулярним наглядом з боку адміністратора. Зокрема, важливо систематично перевіряти статус RAID-масивів, технічні характеристики жорстких дисків, кількість доступного дискового простору, стан спільних папок та точність функціонування механізмів резервного копіювання. У разі використання NAS-сховища для архівації конфігурацій або робочих файлів необхідно контролювати не лише доступність даних, але й їхню цілісність. Такий підхід дозволяє запобігти ризикам, коли пристрій технічно функціонує нормально, проте резервні копії не створюються належним чином або зазнають пошкодження.

Особливу роль у забезпеченні стабільності роботи інфраструктури виконують журнали подій. Вони слугують ключовим інструментом для виявлення спроб несанкціонованого доступу, помилок автентифікації, змін у параметрах доступу або збоїв служб. На основі аналізу журналів подій здійснюється не тільки діагностика технічних несправностей, але й розробка планів щодо подальших дій для відновлення або оптимізації роботи системи. Таким чином, ретельний моніторинг журналів подій є невід’ємною складовою ефективного управління IT-інфраструктурою.

3.5.4 Контроль безпеки та доступу

Під час експлуатації комп'ютерної мережі важливо враховувати не лише технічну доступність її компонентів, але й забезпечення належного контролю за тим, хто саме підключається до системи, які ресурси використовуються і чи не виникають порушення політик доступу між віртуальними локальними мережами (VLAN). Для досягнення цього рівня безпеки необхідно систематично перевіряти наявність підозрілих або невідомих пристроїв у мережі, виявляти можливе підключення користувачів із гостьового сегмента до внутрішньої мережі та аналізувати будь-які зміни у правах доступу до серверних ресурсів.

В обов'язки адміністратора входить моніторинг та підтримка належного функціонування міжмережевого екрану, регулярне оновлення засобів антивірусного захисту на робочих станціях, контроль доступу через протокол SSH і актуалізація списку облікових записів користувачів. У разі, якщо співробітник залишає організацію чи змінює підрозділ, необхідно оперативно переглянути його права доступу, щоб мінімізувати ризик потенційних зловживань і спростити управління ресурсами.

Для підтримання безпеки в сегменті Wi-Fi мережі слід регулярно оцінювати її стан. Необхідно перевіряти актуальність паролів, забезпечення використання сучасних стандартів шифрування, таких як WPA2 або WPA3, а також дотримання ізоляції між основною і гостьовою мережами. Для офісних мереж варто впровадити плановий графік таких перевірок, проводячи їх, наприклад, щотижня або після внесення будь-яких змін у конфігурацію мережевого обладнання.

3.5.5 Реакція на збої та відновлення

Жодна мережа не може бути абсолютно захищеною від можливих збоїв, тому в інструкціях обов’язково має бути прописаний чіткий алгоритм дій на випадок нештатних ситуацій. Наприклад, якщо один із комутаторів перестає відповідати, насамперед слід перевірити живлення, наявність лінку, правильність конфігурації порту та фізичне підключення. У разі некоректної роботи серверного сервісу першочергово виконують аналіз журналів і перевіряють стан служб, лише після цього переходять до внесення змін у конфігурацію.

Коли недоступний NAS або виникають труднощі з доступом до файлів, необхідно проаналізувати стан RAID-масиву, перевірити диски, права доступу та актуальність резервних копій. У випадку проблем із Wi-Fi слід оцінити стан точок доступу, PoE-живлення, коректність налаштувань VLAN і силу сигналу. Така послідовність допомагає оперативно ідентифікувати проблему, уникаючи безсистемних перевірок та зайвих витрат часу.

Після ліквідації збоїв рекомендується залишати короткий запис у журналі експлуатації, вказуючи деталі події: що саме трапилося, який елемент мережі вийшов із ладу, які дії вжили та до якого результату вони привели. Така документація сприяє створенню практичної бази для майбутньої підтримки мережі та значно полегшує роботу адміністратора під час вирішення аналогічних інцидентів у майбутньому.

У випадку повторюваних інцидентів доцільно проводити детальний аналіз причин та розробляти профілактичні заходи для їх недопущення в майбутньому.

3.5.6 Регламент обслуговування

Для забезпечення стабільності роботи мережі доцільно запровадити регулярний графік обслуговування. Щодня слід перевіряти доступність ключових вузлів мережі та працездатність сервісів. Раз на тиждень аналізуються журнали подій, перевіряється актуальність резервних копій і стан бездротового сегмента мережі. Щомісяця проводиться оновлення системного програмного забезпечення, ревізія прав доступу та оцінка загального технічного стану обладнання. Такий підхід дозволяє підтримувати інфраструктуру в стабільному та прогнозованому робочому стані.

Регламентне обслуговування має ще одну вагому перевагу — воно допомагає вчасно виявляти дрібні відхилення, які згодом можуть призвести до значних проблем. Наприклад, незначне зростання кількості помилок на мережевому порту чи епізодичні розриви зв’язку у Wi-Fi можуть бути раннім сигналом несправностей у кабелі, точці доступу або комутаторі.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проєкту комп'ютерної мережі для ТОВ «АВЕРС НК» 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 проекту, інженер, технік. В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

Таблиця 4.1 – Середній час виконання НДР та стадії технологічного процесу

1	2	3	4
№ п/п	Назва операції	Виконавець	Середній час виконання операції, год.
1.	Передпроєктне обстеження об'єкта	керівник проекту	8

Продовження таблиці 4.1

1	2	3	4
2.	Проектування мережі	інженер	24
3.	Вибір необхідного мережевого обладнання	керівник проекту	10
4.	Монтаж мережі	технік	24
5.	Тестування мережі	інженер	4
6.	Здача проекту в експлуатацію	керівник проекту	2
Разом			72

Загальний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для ТОВ «АВЕРС НК» становить 72 години.

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:

$$З_{осн.}=Т_с \cdot К_г \ , \qquad (4.1)$$

де Тс – тарифна ставка, грн.; Кг – кількість відпрацьованих годин.

Основна заробітна плата становить:

1. Керівник проекту: $З_{осн1} = 300 \cdot 20 = 6000$ грн.;

2. Інженер: $З_{осн2} = 220 \cdot 28 = 6160$ грн.;

3. Технік: $З_{осн3} = 120 \cdot 24 = 2880$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 6000 + 6160 + 2880 = 15040 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати та обчислюється за формулою 4.2:

$$З_{дод.}=З_{осн.} \cdot К_{допл.} \ , \qquad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам: 0,1–0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту: $З_{дод1} = 6000 \cdot 0,13 = 780$ грн.;

2. Інженер: $З_{дод2} = 6160 \cdot 0,13 = 800,80$ грн.;

3. Технік: $З_{дод3} = 2880 \cdot 0,13 = 374,40$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод} = 780 + 800,80 + 374,40 = 1955,20 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою 4.3:

$$В_{о.п.}=З_{осн.}+З_{дод.}, \quad (4.3)$$

$$В_{о.п} = 15040+ 1955,20 = 16995,20 \text{ грн.}$$

Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде обчислюватися за формулою 4.4:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з.}= 16995,20 \cdot 0,22 = 3738,9 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці були узагальнені та систематизовані для подальшого використання у фінансовому плануванні підприємства. Отримані дані дозволяють здійснити детальний аналіз структури витрат, визначити їхню динаміку та оцінити вплив на загальний бюджет. Розрахунки витрат на оплату праці зображені у таблиці 4.2

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівни-ків	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарах ув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	300	20	6000	780	-	-
2	Інженер	220	28	6160	800,80	-	-
3	Технік	120	24	2880	374,40	-	-
Разом				15040	1955,20	3738,9	20734,14

Загальні витрати на оплату праці становлять 20734,14 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i, \tag{4.5}$$

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

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi}, \tag{4.6}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

1	2	3	4	5
Обладнання	Одиниці виміру	Фактично витрачено матеріалів	Ціна одиниці, грн.	Загальна сума витрат, грн.
Комутатор D-Link DGS-1520-52	шт.	1	49999	49999
Міжмережевий екран TP-LINK Omada ER7406	шт.	1	6804	6804
Сервер Dell PowerEdge R750xs	шт.	3	109505	328515

Продовження таблиці 4.3

1	2	3	4	5
SSD диск CUSU C300 2TB 2.5" SATAIII	шт.	6	8499	50994
Точка доступу TP-Link EAP653	шт.	1	3959	3959
PoE-інжектор 2E PowerLink PSE801G (1xGE, 1xGE PoE, 802.3af/at	шт.	1	629	629
Мережевий принтер HP Color LaserJet Pro 3202dn	шт.	7	13632	95424
ДБЖ Smart-UPS LogicPower 6000 PRO RM	шт.	1	73000	73000
LAN кабель Cablexpert CAT6, 305м	шт.	5	9999	49995
Шафа монтажна настінна CMS MGSWA 21U	шт.	1	15040	15040

Продовження таблиці 4.3

1	2	3	4	5
Патч-панель 19" 24xRJ-45 UTP Pipo 1U cat.6	шт.	2	1434	2868
Кабельний організатор Digitus 19' 1U, перфорований	шт.	2	579	1158
Подовжувач до серверної шафи Qoltec RACK 1.8м 4 розетки	шт.	1	859	859
Розетка однопортова Cablexpert RJ-45, 6 cat, зовнішня	шт.	36	94	3384
Патч-корд Cablexpert CAT6 UTP 3 м	шт.	36	99	3564
Патч-корд литий RITAR UTP RJ45 Cat.6 0.5м	шт.	40	73	2920
Короб пластиковий АСКО STEP 25x16x2000мм	шт.	35	63,89	2236,15
Сітчастий лоток Ardic 100x50 мм, оцинкований,	м	110	213,97	23536,70
Разом				714884,85

Загальна сума матеріальних витрат становить 714884,85 грн.

4.4 Розрахунок витрат на електроенергію

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

$$З_е = W \cdot T \cdot S \ , \qquad (4.7)$$

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

Час роботи ПК над даним проєктом становить 34 години, споживана потужність - 0,7 кВт/год., вартість 1 кВт електроенергії – 15,94 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0{,}7 \cdot 34 \cdot 15{,}94 = 379{,}37 \text{ грн.}$$

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.

$$Т_в = З_{м.в.} \cdot 0{,}08 \ldots 0{,}1, \qquad (4.8)$$

де $Т_В$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_В = 714884,85 \cdot 0,08 = 57190,79 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань застосовуємо формулу 4.9:

$$A = \frac{Б_В \cdot Н_А}{100\%} \cdot Т, \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн. $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації, %? Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК використовується при роботі над даним проектом 34 год., балансова вартість ПК – 38000 грн., тому:

$$А = \frac{38000 \cdot 0,04}{150} \cdot 34 = 344,53 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати - це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

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.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6\,, \tag{4.10}$$

де $Н_В$ – накладні витрати.

$$Н_В = 16995{,}20 \cdot 0{,}3 = 5098{,}56 \text{ грн.}$$

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 НДР

Зміст витрат	Сума, грн.	В% до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	16995,20	1,8
Відрахування на соціальні заходи	3738,9	0,4
Матеріальні витрати	714884,85	89,97
Витрати на електроенергію	379,37	0,05
Транспортні витрати	57190,79	7,2
Амортизаційні відрахування	344,53	0,04
Накладні витрати	5098,56	0,54
Собівартість	798 632,2	100

Собівартість ($С_в$) НДР розрахуємо за формулою 4.11:

$$C_B = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + Т_в + А + Н_в, \quad (4.11)$$

Собівартість дорівнює $С_В$ = 798 632,2 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = Св \cdot (1+Р_{рен}) \cdot (1+ПДВ), \quad (4.12)$$

де $Р_{рен.}$ – рівень рентабельності; ПДВ – ставка податку на додану вартість.

$$Ц = 798\,632{,}2 \cdot (1+0{,}3) \cdot (1+0{,}2) = 1\,245\,866{,}23 \text{ грн.}$$

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 ($Т_{ок}$), який можна визначити за формулою 4.13.

$$ЧТВ = -К_В + \sum_{i=1}^{t} \frac{ГП}{(1+i)^t}, \quad (4.13)$$

де $К_В$ – затрати на проект; $Г_п$ – грошовий потік за t – ий рік; t – відповідний рік проекту; i - величина дисконтної ставки (10…15%).

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

$$ЧТВ = -798\,632{,}2 + \frac{704676{,}03}{(1+0{,}15)} + \frac{704676{,}03}{(1+0{,}15)^2} = 346966{,}12$$

Термін окупності визначається за формулою 4.14:

$$T_{ОК} = T_{ПВ} + \frac{H_В}{Г_{ПР}}, \quad (4.14)$$

де $Т_{ПВ}$ – період до повного відшкодування витрат, років; $Н_В$ – невідшкодовані витрати на початок року, грн.; $Г_{ПР}$ – грошовий потік на початок року, грн.

$$T_{ок} = 1 + \frac{185869{,}88}{704676{,}03} = 1{,}3$$

Отримані результати свідчать про високу економічну доцільність впровадження проєкту, оскільки термін окупності є коротким, а значення ЧТВ є позитивним. Це свідчить про ефективність використання інвестиційних ресурсів та обґрунтованість прийнятих рішень. Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники розробки мережі

1	2	3
№ п/п	Показник	Значення
1	Собівартість, грн.	798 632,2
1	2	3
2	Плановий прибуток, грн.	447 234,03
3	Ціна, грн.	1 245 866,23
4	Чиста теперішня вартість, грн.	346966,12
5	Термін окупності, рік	1,3

Загальна вартість розробленої мережі для ТОВ «АВЕРС НК» становить 1245866,23 грн. Термін окупності становить 1,3 роки.

5. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Забезпечення пожежобезпеки в приміщенні ТОВ «Внутрішні інженерні системи»

Загальна характеристика та нормативно-правова база

Пожежна безпека на підприємстві ТОВ «Внутрішні інженерні системи» є одним із найважливіших аспектів охорони праці, враховуючи специфіку діяльності компанії. Офісні приміщення, а особливо серверні кімнати та комутаційні вузли, характеризуються високою концентрацією електронно-обчислювальної техніки, мережевого обладнання, кабельних трас та джерел безперебійного живлення (ДБЖ). Згідно з чинним законодавством України, зокрема Кодексом цивільного захисту України та «Правилами пожежної безпеки в Україні» (наказ МВС № 1417),[4]

керівництво компанії зобов'язане забезпечити належний рівень пожежної безпеки.

Приміщення ТОВ «Внутрішні інженерні системи» за вибухопожежною та пожежною небезпекою, згідно з ДСТУ Б В.1.1-36:2016, відносяться до категорії «В» (пожежонебезпечні), оскільки в них знаходяться горючі матеріали (ізоляція кабелів, пластикові корпуси обладнання, папір) у кількостях, достатніх для виникнення пожежі при взаємодії з джерелом запалювання.

Аналіз потенційних причин виникнення пожежі

Основними джерелами запалювання та причинами пожеж в умовах ІТ-підприємства можуть бути:

- Електричні фактори*:* коротке замикання в електромережах, перевантаження електропроводки через підключення великої кількості обладнання, великий перехідний опір у місцях неякісного з’єднання контактів, пробій ізоляції кабелів.

- Теплові фактори*:* перегрів блоків живлення серверів HPE, комутаторів MikroTik та робочих станцій внаслідок несправності систем охолодження (кулерів) або порушення температурного режиму в приміщенні.

- Людський фактор*:* необережне поводження з вогнем, паління у невизначених місцях, використання несправних побутових електроприладів (чайників, обігрівачів) на робочих місцях.

- Аварії ДБЖ*:* коротке замикання акумуляторних батарей або їх тепловий розгін у разі виходу з ладу контролерів заряду.

Організаційні заходи пожежної безпеки

У ТОВ «Внутрішні інженерні системи» розроблено та впроваджено комплексну систему організаційних заходів. Наказом керівника призначено особу, відповідальну за пожежну безпеку. Усі працівники під час прийняття на роботу проходять вступний протипожежний інструктаж, а також первинний інструктаж безпосередньо на робочому місці. Повторні інструктажі проводяться не рідше одного разу на рік.[1][3]

У коридорах, офісах та серверній кімнаті розміщено плани евакуації, розроблені відповідно до ГОСТ 12.1.114-82, із зазначенням шляхів евакуації, місць розташування первинних засобів пожежогасіння, ручних пожежних сповіщувачів та телефонів виклику ДСНС (101). Шляхи евакуації утримуються вільними, не захаращуються меблями чи обладнанням, а двері на шляхах евакуації відкриваються назовні.

Технічні заходи та системи протипожежного захисту

Для мінімізації ризиків пожежі на етапі проектування мережі та електропостачання реалізовано наступні технічні рішення:

- Уся структурована кабельна система (СКС) та силові лінії виконані кабелями з маркуванням «нг-LS» (не поширюють горіння при груповій прокладці, зі зниженим димо- та газовиділенням).
- Електрощитові та серверні стійки обладнані пристроями захисного відключення (ПЗВ) та автоматичними вимикачами з відповідними номіналами спрацьовування.
- Приміщення обладнані автоматичною пожежною сигналізацією (АПС). У серверній встановлено димові та теплові сповіщувачі, підключені до приймально-контрольного приладу, який виведений на пульт централізованого спостереження.

Засоби пожежогасіння

Враховуючи, що в приміщеннях ТОВ «Внутрішні інженерні системи» знаходиться дороговартісна комп'ютерна техніка під напругою до 1000 В, застосування водних та пінних вогнегасників категорично заборонено. Основним засобом первинного пожежогасіння обрано вуглекислотні вогнегасники типів ВВК-2 та ВВК-5.

Дія діоксиду вуглецю (CO2) базується на витісненні кисню з осередку горіння та різкому охолодженні (до -70 °C). Вуглекислота є діелектриком, не залишає слідів на мікросхемах та не викликає корозії, що робить її ідеальною для гасіння серверного та мережевого обладнання. Вогнегасники розміщені на спеціальних підставках у легкодоступних місцях, з розрахунку не менше одного

вогнегасника на 20 кв. м площі серверної, та проходять щорічне технічне обслуговування.

5.2 Хімічні негативні фактори. Заходи і засоби захисту людини

Джерела хімічної небезпеки в ІТ-середовищі

Традиційно вважається, що робота інженерів, програмістів та мережевих адміністраторів не пов'язана з впливом шкідливих хімічних речовин. Однак сучасні офісні та серверні приміщення ТОВ «Внутрішні інженерні системи» мають приховані хімічні фактори, які при тривалому впливі можуть викликати хронічні захворювання, алергічні реакції та зниження працездатності.

Основними джерелами хімічного забруднення повітря робочої зони є:

- Копіювально-множильна техніка та лазерні принтери. Під час роботи лазерних принтерів під дією коронних розрядів та ультрафіолетового випромінювання відбувається іонізація повітря з утворенням озону (O3) та оксидів азоту (NO, NO2). Озон належить до першого класу небезпеки (ГДК у повітрі робочої зони — 0,1 мг/м³). Крім того, під час друку виділяється дрібнодисперсний пил тонеру, який містить сажу, полімери та сліди важких металів.
- Електронно-обчислювальна техніка. Під час роботи серверного та мережевого обладнання, особливо при пікових навантаженнях, відбувається нагрівання друкованих плат, пластикових корпусів та ізоляції проводів. Це призводить до емісії летких органічних сполук (ЛОС), зокрема фенолу, формальдегіду, стиролу, а також полібромованих дифенілових етерів (PBDE),

які використовуються як антипірени (речовини, що запобігають горінню пластику).

- Джерела безперебійного живлення *(ДБЖ).* Свинцево-кислотні акумулятори (SLA), що використовуються в серверних кімнатах, є потенційним джерелом виділення водню та парів сірчаної кислоти у разі порушення режиму заряду, розгерметизації або перегріву батарей.

Вплив хімічних факторів на організм людини

Постійне вдихання повітря з перевищеним вмістом озону та ЛОС викликає подразнення слизових оболонок очей і верхніх дихальних шляхів, головний біль, підвищену втомлюваність. Тонерний пил здатен проникати глибоко в легені, викликаючи з часом професійні захворювання бронхів та алергічні реакції. Випари формальдегіду мають канцерогенний та мутагенний вплив.

Комплекс заходів та засобів захисту

Для забезпечення нормативних показників якості повітря згідно з ГОСТ 12.1.005-88 («Загальні санітарно-гігієнічні вимоги до повітря робочої зони») у ТОВ «Внутрішні інженерні системи» реалізовано наступні інженерно-технічні та санітарно-гігієнічні заходи:

- Системи вентиляції та кондиціонування. Основною мірою боротьби з хімічним забрудненням є ефективний повітрообмін. В офісних приміщеннях змонтована припливно-витяжна вентиляція зі штучним спонуканням. Розрахунок вентиляції проведено з урахуванням виділення тепла та шкідливих

газів від техніки (повітрообмін не менше 30–40 м³/год на одного працівника). Серверна кімната обладнана незалежною прецизійною системою кондиціонування та вентиляції.

- Раціональне планування приміщень. Усі потужні мережеві принтери та копіювальні апарати винесені з приміщень, де постійно працюють інженери, в окрему спеціально обладнану зону з посиленою місцевою витяжною вентиляцією. Це унеможливлює накопичення озону та тонерного пилу в зоні дихання працівників.

- Контроль за станом акумуляторних батарей. У серверній кімнаті встановлено датчики температури та газоаналізатори для контролю можливого виділення водню від ДБЖ. Проводиться регулярний регламентний огляд стійок з акумуляторами (раз на 6 місяців) для виявлення деформацій корпусів чи слідів витоку електроліту.

- Вологе прибирання та очищення повітря. У приміщеннях щодня проводиться вологе прибирання для усунення пилу. Додатково в робочих зонах встановлено HEPA-фільтри та мийки повітря, які ефективно вловлюють дрібні частки ЛОС та тонеру.

- Засоби індивідуального захисту (ЗІЗ). Хоча для звичайної роботи в офісі ЗІЗ не використовуються, для інженерів, які обслуговують принтери (заміна картриджів, чищення валів) або ДБЖ, передбачено наявність респіраторів класу FFP2/FFP3, захисних окулярів та нітрилових рукавичок для захисту шкіри та дихальних шляхів.

- Система пожежної безпеки. У серверній кімнаті передбачено автоматичне пожежне сповіщення та газове пожежогасіння, що дозволяє швидко локалізувати займання без пошкодження обладнання. Регулярно проводяться перевірки справності датчиків та навчання персоналу діям у разі надзвичайної ситуації.

5.3 Медико-профілактичні заходи в ТОВ «Внутрішні інженерні системи»

Специфіка професійних ризиків

Праця ІТ-інженерів, розробників та системних адміністраторів у ТОВ «Внутрішні інженерні системи» належить до категорії робіт з високим нервово-емоційним та зоровим напруженням. Згідно з НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями», така діяльність супроводжується рядом специфічних факторів ризику.

Основними шкідливими виробничими факторами є гіподинамія (тривале статичне положення тіла), напруження зорового аналізатора, монотонність праці та високий рівень стресу при вирішенні нештатних ситуацій (аварії в мережі, кібератаки). Наслідками цього можуть стати захворювання опорно-рухового апарату (остеохондроз, сколіоз), «комп'ютерний зоровий синдром» (синдром сухого ока, спазм акомодації, короткозорість), а також тунельний синдром зап'ястка (через постійну роботу з мишею та клавіатурою).

Медичні огляди та контроль здоров'я

Основою медико-профілактичної роботи в ТОВ «Внутрішні інженерні системи» є своєчасний моніторинг стану здоров'я співробітників. Відповідно до Наказу МОЗ України № 246, усі працівники, які працюють за персональними комп'ютерами більше 50% робочого часу, підлягають:

- Попередньому медичному огляду під час прийняття на роботу для визначення придатності до виконання обов'язків за станом здоров'я.

- Періодичним медичним оглядам (не рідше одного разу на рік). До складу медичної комісії обов'язково входять лікар-невропатолог та офтальмолог.
- Такий підхід дозволяє виявити ранні ознаки професійних захворювань і вчасно направити працівника на профілактичне лікування чи коригування зору.

Організація режиму праці та відпочинку

Для профілактики перевтоми та зниження напруженості праці розроблено раціональний режим роботи. Згідно з санітарними нормами, тривалість безперервної роботи за екраном монітора не повинна перевищувати 2 години.

У компанії запроваджено наступний графік перерв:

- Мікропаузи тривалістю 1–2 хвилини кожну годину роботи для зняття локального м'язового напруження.
- Регламентовані перерви по 15 хвилин кожні дві години. Працівникам наполегливо рекомендується покидати робоче місце, провітрювати приміщення та виконувати комплекси вправ виробничої гімнастики.
- Окремим елементом профілактики є гімнастика для очей (фокусування погляду на віддалених об'єктах за вікном, часте моргання для відновлення слізної плівки).
- Обідня перерва тривалістю 30–60 хвилин у середині робочого дня. Вона дає змогу відновити енергію, збалансувати харчування та зменшити втому.
- Кавова пауза тривалістю 5–10 хвилин у першій половині дня. Це сприяє короткому відпочинку, неформальному спілкуванню між колегами та підвищенню концентрації.

Ергономіка робочих місць

Медико-профілактичні заходи були б неефективними без належного інженерно-ергономічного облаштування робочого простору:

- Робочі столи мають достатню площу для зручного розміщення обладнання та документів. Висота столів (близько 72-75 см) та наявність простору для ніг дозволяють підтримувати правильну поставу.

-Використовуються спеціалізовані ергономічні крісла з можливістю регулювання висоти сидіння, кута нахилу спинки та наявністю поперекового валика і підлокітників. Це кардинально знижує статичне навантаження на хребет.

-Монітори встановлені таким чином, щоб верхній край екрану знаходився на рівні очей, а відстань до дисплея становила 60-70 см. Дисплеї мають матове покриття для уникнення відблисків, що знижує втому очей.

Заходи загального оздоровлення та перша допомога

Керівництво ТОВ «Внутрішні інженерні системи» підтримує концепцію корпоративного здоров'я (Well-being). В офісі облаштовано зону відпочинку (кімнату релаксації), де співробітники можуть змінити обстановку під час перерв. Компанія забезпечує працівників полісами добровільного медичного страхування (ДМС), які покривають курси масажу та вітамінотерапії.Для надання першої долікарської допомоги у разі раптового погіршення самопочуття, порізів чи травм, у доступних місцях на кожному поверсі розміщено медичні аптечки.

ДОДАТКИ

Додаток А. План розміщення обладнання головного комутаційного вузла

Головний комутаційний вузол підприємства розміщується в окремому приміщенні або виділеній зоні серверної кімнати з обмеженим доступом. У вузлі встановлюється серверна стійка, у якій розміщуються маршрутизатор, головний керований комутатор, комутатори доступу, два сервери, мережеве сховище, джерело безперебійного живлення, патч-панелі, кабель-організатори та допоміжне монтажне обладнання. Компонування виконується так, щоб забезпечити зручність обслуговування, вентиляцію, безпечне прокладання кабелів і раціональне використання простору.

У верхній частині стійки доцільно розміщувати патч-панелі та кабель-організатори, нижче — активне мережеве обладнання ядра мережі, ще нижче — два сервери, мережеве сховище та ДБЖ. Такий підхід відповідає принципам сервісної доцільності, полегшує обслуговування й не порушує вимог до охолодження та доступу до вузлів.

Додаток Б. Характеристики та перелік активного комутаційного обладнання

Характеристики активного комутаційного обладнання мережі зображена в таблиці Б.1

Таблиця Б.1 – Перелік активного комутаційного обладнання

1	2	3	4
Найменування	Кількість	Короткі характеристики	Призначення
MikroTik CRS326-24G-2S+RM	1	24 × Gigabit Ethernet, 2 × SFP+, кероване комутування, VLAN, STP, LACP, QoS	Головний комутатор ядра мережі
MikroTik CRS326-24G-2S+IN	2	24 × Gigabit Ethernet, 2 × SFP+, кероване комутування, VLAN, STP, LACP	Комутатори доступу для сегментів мережі
MikroTik RB4011iGS+RM	1	10 × Gigabit Ethernet, 1 × SFP+, NAT, firewall, DHCP, VPN	Маршрутизація та підключення до провайдера

Продовження таблиці Б.1

1	2	3	4
MikroTik cAP ax	2	Wi-Fi 6, 802.11ax, dual band, PoE, централізоване керування	Бездротовий доступ користувачів
MikroTik CSS610-8G-2S+IN	1	8 × Gigabit Ethernet, 2 × SFP+, кероване комутування	Допоміжне комутаційне обладнання

Усі наведені моделі є реальними зразками обладнання, придатними для побудови мережі малого або середнього підприємства. Остаточна комплектація може змінюватися залежно від бюджету, наявності обладнання та вимог до пропускної здатності.

Додаток В. Характеристики серверів

Під час опрацювання попередніх розділів було визначено саме два сервери, тому в додатку навмисно наведено лише дві серверні одиниці. Такий підхід узгоджується з прийнятою архітектурою мережі та не суперечить рішенню про централізоване зберігання даних і резервне копіювання. Усі зазначені пристрої зображені в таблиці В.1

Таблиця В.1 – Перелік серверного обладнання

Найменування	Кількість	Короткі характеристики	Призначення
Dell PowerEdge R750xs	1	1U сервер, Intel Xeon, 64 GB RAM, RAID-контролер, можливість гарячої заміни дисків	Основний сервер служб домену, файлів і віртуалізації
Synology DiskStation DS923+	1	4-bay NAS, AMD Ryzen, 4–32 GB RAM, підтримка RAID 0/1/5/6/10	Мережеве сховище та резервне копіювання

Додаток Г. Приклади конфігурацій та серверних скриптів

Тексти для програмування активного комутаційного обладнання та серверні скрипти

У цьому додатку наведено умовні приклади конфігурацій. Оскільки налаштування мережі можуть містити комерційну таємницю, усі IP-адреси, паролі, імена хостів та параметри доступу подаються у знеособленому вигляді.

Г.1 Приклад базової конфігурації комутатора ядра

Configure terminal

hostname SW-CORE

vlan10

name OFFICE

vlan 20

name TECH

vlan 30

name WIFI

vlan 40

name SECURITY

vlan60

nameSERVERS

interface range gigabitEthernet 1/0/1-24

```
switchport mode access
switchport access vlan 10
spanning-tree portfast
interface gigabitEthernet 1/0/25
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,60
end
write memory
```

Г.2 Приклад базової конфігурації маршрутизатора

```
interface wan1
ip address dhcp
interface lan1
ip address 192.168.60.1 255.255.255.0
ip nat inside
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
ip nat inside source list 1 interface wan1 overload
```

Г.3 Серверний скрипт резервного копіювання

```
#!/bin/bash

SRC="/srv/data"

DST="/backup/$(date +%F)"

mkdir -p "$DST"

rsync -a --delete "$SRC/" "$DST/"
```

Г.4 Серверний скрипт моніторингу служб

```
#!/bin/bash

services=(nginx samba ssh)

for s in "${services[@]}"; do

  systemctl is-active --quiet "$s" || echo "$s is down" | mail -s "Alert" admin@example.com

done
```

Висновок до додатків

Подані додатки узагальнюють практичну частину проєкту комп'ютерної мережі підприємства, демонструють принцип розташування обладнання, реальний склад активної та серверної інфраструктури і приклади умовних конфігурацій для її програмування. Наведені дані мають навчальний і проєктний характер та можуть бути уточнені залежно від остаточного технічного рішення.

ВИСНОВКИ

На основі аналізу специфіки діяльності ТОВ «Внутрішні інженерні системи», сформованих вимог технічного завдання та виконаних етапів розробки технічного і робочого проєктів, можна зробити такі висновки:

- Ефективність архітектурного рішення: У ході виконання кваліфікаційної роботи було успішно розроблено проєкт сучасної локальної комп'ютерної мережі за логічною топологією «Ієрархічна зірка». Поділ мережі на 6 ізольованих віртуальних підмереж (VLAN) дозволив логічно сегментувати структуру підприємства відповідно до його підрозділів (FIN, TECH, SECURITY, SERVERS, WIFI). Це забезпечило високий рівень безпеки корпоративних даних, оптимізацію мережевого трафіку та мінімізацію широкомовного шторму всередині мережі.
- Обґрунтованість апаратного забезпечення: Обране мережеве обладнання компанії MikroTik (маршрутизатор RB4011iGS+RM, центральний комутатор CRS326-24G-2S+RM та PoE-комутатор CRS318-16P-2S+OUT) продемонструвало оптимальний баланс між продуктивністю, функціональністю та економічною доцільністю для підприємства з 18 робочими станціями. Розрахунки портів та бюджету PoE підтвердили наявність значного експлуатаційного та технічного резерву (вільними залишаються 17 портів на ядрі та понад 200 Вт потужності PoE), що гарантує легку масштабованість мережі при подальшому розширенні офісу чи модернізації систем відеоспостереження.
- Надійність фізичної інфраструктури: Проєктування структурованої кабельної системи (СКС) на базі неекранованої витої пари категорії Cat.6 та кабельних лотків виробництва DKC забезпечило стабільну передачу даних на швидкості до 1 Гбіт/с. Централізований монтаж обладнання в окремій серверній

шафі із застосуванням джерел безперебійного живлення (UPS) створив надійні умови для безперервного функціонування критичних вузлів у режимі 24/7.

- Гнучкість програмного середовища: Застосування гібридного програмного підходу — використання операційної системи Windows 11 Pro на робочих станціях (для максимальної сумісності з інженерним ПЗ: AutoCAD, Revit, АВК-5) та вільно розповсюджуваної Ubuntu Server 24.04 LTS разом із Synology DSM на серверах — дозволило суттєво оптимізувати витрати на придбання ліцензій без компромісів щодо стабільності, безпеки й керованості інфраструктури.

Комплексна безпека та моніторинг: Впровадження інструкцій із захисту та щоденного моніторингу, налаштування міжмережевого екрана (Firewall), NAT-шлюзу на базі RouterOS, а також автоматизованого резервного копіювання на базі мережевого сховища Synology DS923+ звело до мінімуму ризики втрати комерційної та інженерної інформації внаслідок збоїв чи несанкціонованого доступу.

Таким чином, створений проєкт комп'ютерної мережі повністю відповідає вимогам сучасних інформаційних технологій, вирішує завдання швидкого обміну великими обсягами графічних даних для ТОВ «Внутрішні інженерні системи» і є економічно виправданою інвестицією, яка підвищить загальну продуктивність праці персоналу та забезпечить стабільність бізнес-процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. ОСНОВИ ОХОРОНИ ПРАЦІ / С. В. СУКАЧ, А. В. КОЛОСЮК, В. П. КОЛОСЮК, В. А. ГЛИВА. – М: Кременчук, 2020. – 256 с.

2. ДСН 3.3.6.039-99. Державні санітарні норми виробничої загальної та локальної вібрації. Режим доступу: URL: https://ecolog-ua.com/news/yaki-pokaznyky-potrebuyut-kontrolyu-vibraciyi-v-szz. Дата доступу: 29.05.2026.

3. ДСН 3.3.6.037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку. Режим доступу: URL: https://dnaop.com/html/1642/doc-%D0%94%D0%A1%D0%9D_3.3.6.037-99. Дата доступу: 28.05.2026.

4. Інструкція з охорони праці під час монтажу кабельних мереж. Режим доступу: URL: https://dnaop.com/html/31931/doc-instrukcijaz-ohoroni-pracipid-chas-montazhu-kabelynih-merezh. Дата доступу: 29.05.2026.

5. Комп'ютерний кабель Одескабель 8х0,54 КПВ-ВП(250) мідь. [електронний ресурс] - Режим доступу: URL: https://epicentrk.ua/shop/kabel-kompyuternyy-odeskabel-kpv-vp-250-4-2-0-54-odeskabel-6-kat-u-utp.html. Дата доступу: 17.04.2026.

6. Комутатор TP-LINK SG5428X 24xGE, 4xSFP+, Керований L3. - Режим доступу: URL: https://tp-link.com.ua/komutator-tp-link-sg5428x-24xge-4xsfp-kerovanyil3/?srsltid=AfmBOor4GxNam2J7VD9zCEXtupRjKY8kviIpzIDvgAkaL9Gq9uSvqJzj. Дата доступу: 18.04.2026

7. Маршрутизатор MikroTik Режим доступу: URL: RB4011iGS+RMhttps://rozetka.com.ua/ua/mikrotik_rb4011igs_rm/p65685753/?gad_source=1&gad_campaignid=23838481152&gbraid=0AAAADlXhI6VfPmbwmbq

8UbuntuServer24.04LTS Режимдоступу:URL:https://en.wikipedia.org/wiki/Ubuntu

9 MikroTik RB4011iGS+RM Режимдоступу:URL: https://comfy.ua/ua/kommutator-lokal-noj-seti-switch-mikrotik-rb4011igs-rm.html?gad_source=1&gad_campaignid=17147029668&gbraid=0AAAAAC-ixwiOw0jR57hRrvZ3asLGwP64B&gclid=CjwKCAjwgO7RBhBKEiwAZNP85ltT60KjaQ5zNXcqFJxBCrB7Nw33hQvmZ2XdvFEQn1Y2-wnyNO_hlxoCbPkQAvD_BwE

10 DKC лотки Режимдоступу:URL https://amperok.com.ua/tm_dks?utm_source=google&utm_medium=cpc&ut_campaign=Search_Elektrika&utm_content=771205433919&utm_term=&gad_source=1&gad_campaignid=22175175573&gbraid=0AAAAACdx31B8IXlzjhsZiMCYWgBpQxWx5&gclid=CjwKCAjwgO7RBhBKEiwAZNP85mon6d2YYbbtsZD0pZohpcqfPgddwIVyy8FL4P8d1t42a-J3mUuiRBoCBiEQAvD_BwE

11 CRS318-16P-2S+OUT Режим доступу: URL https://unisfera-shop.com.ua/mikrotik-crs318-16p-2sout/?gad_source=1&gad_campaignid=23056763741&gbraid=0AAAABArNatlaFAVgeRIst8o3NNjPvayve&gclid=CjwKCAjwgO7RBhBKEiwAZNP85oC2WAPObTaI1KYZUbCMqFoPPyo5yr5xLtcsoX7wpXFLdXFNpnXANxoCwxYQAvD_BwE

12. Комутатор MikroTik CRS326-24G-2S+RM. - Режим доступу: URL https://comfy.ua/ua/kommutator-lokal-noj-seti-switch-mikrotik-crs326-24g-2s-rm.html?gad_source=1&gad_campaignid=17147029668&gbraid=0AAAAAC- Дата доступу: 18.04.2026.