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 ТзОВ «HQ Print»***

Виконав: студент IV курсу, групи КІ-406

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

_____ Андрій СЦІБАЙЛО
(ім'я та прізвище)

Керівник Олександра МАРЦЮК
(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

Сцібайло Андрію Івановичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: ***Розробка проєкту комп'ютерної мережі ТзОВ «HQ Print»***

керівник роботи Марцюк Олександра Василівна
(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 _____ Андрій СЦІБАЙЛО
(підпис) (ім'я та прізвище)

Керівник роботи _____ Олександра МАРЦЮК
(підпис) ім'я та прізвище)

АНОТАЦІЯ

Сцібайло А.І. Розробка проєкту комп’ютерної мережі ТзОВ «HQ Print»: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. – 88 с.

Роботу присвячено проєктуванню ефективної, безпечної та відмовостійкої мережевої інфраструктури підприємства. У ході виконання досліджено технічні вимоги, підібрано комутаційне обладнання й програмне забезпечення, а також визначено базові засоби мережевого захисту. Створено логічну та фізичну топології, підготовлено інструкції з налаштування серверів, мережевих пристроїв і робочих станцій. Окрему увагу приділено фінансовому обґрунтуванню рішень та дотриманню правил охорони праці.

Ключові слова: комп'ютерна мережа, мережеве обладнання, програмне забезпечення, мережевий захист, VLAN, wi-fi.

Кваліфікаційна робота містить графічну частину на 5 аркушах формату А1 та пояснювальну записку обсягом 88 сторінок.

ABSTRACT

Stsibailo A.I. Development of the computer network project for LLC "HQ Print": qualification work for the educational and professional degree of Professional Junior Bachelor in specialty 123 Computer Engineering. Ternopil: VSP "TFC TNTU", 2026. – 88 p.

The work is dedicated to designing an efficient, secure, and fault-tolerant network infrastructure for the enterprise. In the course of the project, technical requirements were analyzed, switching equipment and software were selected, and basic network protection tools were determined. Logical and physical network topologies were developed, and instructions for configuring servers, network devices, and workstations were prepared. Special attention is paid to the financial justification of the solutions and compliance with occupational health and safety regulations.

Keywords: computer network, network equipment, software, network protection, VLAN, Wi-Fi.

The qualification work contains a graphic part on 5 sheets of A1 format and an explanatory note of 88 pages.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

ACL - список контролю доступу для фільтрації трафіку;

AP - точка бездротового доступу до мережі;

ARP - протокол визначення мережевих адрес;

IEEE 802.3ab - стандарт Gigabit Ethernet для кабелю UTP cat. 5e;

IEEE 802.3ac – специфікація для підтримки VLAN (802.1Q) та пріоритезації трафіку (802.1p);

IEEE 802.3u - специфікація Fast Ethernet (100 Мбіт/с);

IEEE 802.3z - специфікація Gigabit Ethernet (1000 Мбіт/с);

ISO - Міжнародна організація зі стандартизації;

ITU - Міжнародний союз електрозв'язку;

MIB - структурована база даних для керування мережевими пристроями;

SNA - системна мережева архітектура;

SNMP - прикладний протокол для моніторингу та адміністрування мережі;

SOHO - сегмент малих та домашніх офісів;

TCP/IP - базовий стек мережевих протоколів для інтеграції гетерогенних систем;

UTP - неекранована вита пара;

VLAN - віртуальна локальна мережа, що логічно ізолює пристрої в окремий широкомовний домен;

WDM - технологія спектрального ущільнення оптичних каналів зв'язку;

ЛМ - локальна мережа;

MAC-адреса - унікальний 48-бітний апаратний ідентифікатор пристрою;

ОС - операційна система;

ПК - персональний комп'ютер.

ВСТУП

Локальна обчислювальна мережа є сукупністю обчислювальних засобів і мережевого обладнання, що об'єднані єдиним середовищем передавання даних для спільного виконання завдань [1].

Інтеграція такої інфраструктури в діяльність сучасного підприємства обумовлена кількома ключовими чинниками. По-перше, це оптимізує внутрішні комунікації, забезпечуючи оперативний обмін інформацією між підрозділами та співробітниками в режимі реального часу. По-друге, досягається суттєва економія матеріальних ресурсів і часу завдяки організації колективного доступу до мережевих периферійних пристроїв, що зменшує витрати на закупівлю зайвого обладнання. По-третє, підвищується рівень захисту даних за допомогою впровадження політик автентифікації користувачів та гнучкого розмежування прав доступу до корпоративних ресурсів. Зрештою, це приводить до зростання загальної продуктивності праці, адже персонал отримує можливість ефективно взаємодіяти у спільному інформаційному просторі.

Таким чином, розгортання локальних мереж є необхідною умовою для підвищення ефективності координації робочих процесів, оптимізації витрат, захисту конфіденційної інформації та максимізації продуктивності компанії.

Метою цієї кваліфікаційної роботи є проєктування локальної комп’ютерної мережі відповідно до умов технічного завдання, узгодженого між замовником та виконавцем.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Даний проєкт передбачає створення локальної обчислювальної мережі (ЛОМ), спроєктованої під специфічні потреби видавництва ТзОВ «HQ Print» з урахуванням узгоджених техніко-експлуатаційних вимог та запланованого бюджету. В основу інженерного задуму покладено розробку інфраструктури, що відповідає сучасним стандартам продуктивності та інформаційної безпеки.

До ключових завдань, поставлених перед мережевою системою, належать:

- Надійність комунікацій: гарантування безперебійного обміну даними між усіма робочими вузлами підприємства.

- Багаторівневий захист: впровадження активних механізмів фільтрації трафіку для ізоляції внутрішніх сегментів від зовнішніх кіберзагроз.

- Ресурсна консолідація: створення єдиного інформаційного простору для спільного використання мережевих активів та централізованого керування серверами.

- Автоматизація керування: підтримка динамічної адресації та конфігурації підключених пристроїв.

- Гібридна архітектура доступу: забезпечення рівноцінної можливості роботи як через стаціонарні дротові лінії, так і через сегменти бездротового Wi-Fi зв'язку.

- Безпека периметра: інтеграція комплексних рішень для моніторингу та захисту кожного мережевого вузла.

Розроблена інфраструктура оптимізована для бізнес-процесів «HQ Print», проте використані принципи сегментування, вибір обладнання Cisco та серверні рішення на базі FreeBSD формують універсальну базу.

Це дозволяє легко масштабувати або адаптувати архітектуру проєкту для інших підприємств поліграфічної та видавничої галузей зі схожими обсягами комунікаційного навантаження та вимогами до стабільності мережі.

1.1.2 Призначення розробки

Основною метою цього проєкту є створення надійної та масштабованої локальної обчислювальної мережі для ТзОВ «HQ Print», яка забезпечить високу ефективність внутрішніх комунікацій, стабільний вихід у мережу Інтернет та централізовану архітектуру зберігання корпоративної інформації. Проєктування здійснюється з урахуванням сучасних стандартів мережевої інженерії для повної відповідності технічному завданню та очікуванням замовника.

Для досягнення поставленої мети в межах проєкту реалізуються такі ключові завдання:

- Побудова цілісного інформаційного простору: Об’єднання всіх сегментів мережі (дротових та бездротових підключень) у єдину інфраструктуру, що надає персоналу безперебійний доступ до спільних ресурсів та корпоративних баз даних.

- Оптимізація витрат: Виконання всіх етапів -від проєктування та вибору апаратних засобів до монтажу та налагодження -в межах суворо визначеного замовником бюджету без шкоди для якості системи.

- Багаторівневий захист: Впровадження інтегрованих засобів кібербезпеки для захисту периметра мережі, що гарантує безпеку як стаціонарних робочих станцій, так і мобільних пристроїв від зовнішніх несанкціонованих втручань.

- Периферійна інтеграція: Забезпечення можливості спільного використання офісної техніки (принтерів, сканерів та промислових друкарських пристроїв) усіма авторизованими користувачами мережі.

- Забезпечення цілісності даних: Створення централізованої системи управління інформацією на базі відмовостійких сховищ, що гарантує захист від втрати даних та можливість їх швидкого відновлення у разі виникнення технічних збоїв.

Реалізація цих завдань дозволить ТзОВ «HQ Print» підвищити продуктивність робочих процесів та забезпечити надійну технічну базу для подальшого зростання видавничої компанії.

1.1.3 Вимоги до апаратного та програмного забезпечення

Проєктування інфраструктури для ТзОВ «HQ Print» базується на інтеграції сучасних апаратних засобів та надійного програмного забезпечення, що забезпечують безперебійне функціонування мережі. Вимоги до комплектуючих сформовані з урахуванням потреби у високій пропускній здатності, безпеці та можливості майбутнього масштабування.

Апаратні вимоги

- Активне мережеве обладнання є ключовим фактором продуктивності системи. До нього висуваються такі вимоги:

- Комутаційна інфраструктура: Використання інтелектуальних комутаторів рівня L3 та L2+ з підтримкою протоколу Spanning Tree (STP) для запобігання логічним петлям у мережі. Всі порти доступу повинні підтримувати швидкість 1 Гбіт/с для забезпечення стабільної передачі «важких» графічних макетів.

- Серверний сегмент: Впровадження спеціалізованих платформ для розділення ролей сервера-шлюзу (безпека периметра та NAT) та сервера зберігання даних (файловий архів).

Бездротова інфраструктура: Інтеграція точок доступу стандарту IEEE 802.11ac (або новішого), що гарантують високу швидкість передачі даних та підтримку технології безшовного роумінгу.

Програмні вимоги

- Коректна робота мережі залежить від гармонійного поєднання серверного та клієнтського програмного забезпечення:

- Серверна ОС: Вибір операційної системи (на прикладі FreeBSD) має базуватися на стабільності ядра та наявності інструментів для глибокого налаштування безпеки (IPFW) і мережевих служб.

- Сумісність клієнтського середовища: Всі обрані ОС для робочих станцій (Windows, Linux) повинні забезпечувати повну підтримку стека TCP/IP та коректно взаємодіяти з корпоративними ресурсами через VLAN.

Прикладне забезпечення: Програмні продукти, що використовуються в робочому процесі, повинні бути протестовані на сумісність із мережевими протоколами та не містити вразливих компонентів, що можуть загрожувати цілісності мережі.

Ретельний підбір обладнання та софту відповідно до цих вимог мінімізує ризики виникнення технічних простоїв та забезпечує відповідність інфраструктури високим стандартам поліграфічного підприємства.

1.1.4 Вимоги до документації

Якісна документація є невід'ємною частиною життєвого циклу мережі, забезпечуючи можливість її ефективного адміністрування, масштабування та технічної підтримки. Процес документування має бути безперервним: від етапу формування технічного завдання до остаточного введення системи в експлуатацію. Будь-які подальші модернізації апаратної бази чи зміни програмних конфігурацій повинні фіксуватися в актуальній версії технічного паспорта мережі.

Для мінімізації ризиків виникнення критичних збоїв проект передбачає впровадження системи постійного моніторингу та аналізу статистичних показників трафіку. Це дозволяє здійснювати проактивне адміністрування, виявляючи потенційні «вузькі місця» або ознаки перевантаження сегментів ще до моменту виходу системи з ладу.

Мінімальний комплект технічної документації, необхідний для подальшого супроводу мережі ТзОВ «HQ Print», включає такі компоненти:

- Структурні схеми: актуальні креслення логічної топології та фізичної топології (розміщення вузлів, комутаційних шаф та кабельних трас).

- Адресний план: зведені таблиці розподілу IP-адрес для всіх сегментів мережі, включаючи статичні адреси серверів, комутаторів та точок доступу.

- Регламенти налаштування: детальні інструкції щодо конфігурації мережевих вузлів (Cisco CLI) та хостів, що дозволяє швидко відновити параметри у разі заміни обладнання.

- Технічні паспорти вузлів: таблиці параметрів конфігурації для кожного клієнтського пристрою із зазначенням апаратних характеристик та переліку встановленого програмного забезпечення. Візрець технічного паспорту наведено на рисунку 1.1

- Звітність з тестування: протоколи вимірювань фізичних параметрів кабельних ліній та акт введення об’єкта в експлуатацію.

Дотримання цих вимог дозволяє перетворити мережу на керовану та прозору систему, де кожен елемент є ідентифікованим, а будь-яке втручання - прогнозованим та безпечним для бізнес-процесів підприємства.

Документовані відомості про конфігурацію обладнання, схеми підключення та параметри функціонування мережевих вузлів дають змогу оперативно локалізувати й усувати несправності, скорочують час відновлення працездатності мережі після аварійних ситуацій та забезпечують ефективне адміністрування інформаційної інфраструктури ТзОВ «HQ Print» протягом усього терміну її експлуатації.

Паспорт мережевого вузла: _____

Назва	Параметр	Значення
Загальні дані	Назва вузла	
	Тип пристрою	
	Локація / Відділ	
	Відповідальна особа	
Технічні дані	MAC-адреса	
	CPU / RAM / Storage	
Мережа	IP-адреса	
	Маска / Шлюз	
	Порт комутатора	
ПЗ	Операційна система	
	Прикладне ПЗ	

Журнал обслуговування та змін

Дата	Опис проведених робіт	Виконавець	Статус

Рисунок 1.1 – Взірець розробленого технічного паспорту вузла

1.1.5 Техніко-економічні показники

Основними техніко-економічними параметрами побудови мережевої інфраструктури ТзОВ «HQ Print» є наступні характеристики, що відображають технологічний рівень рішення та його фінансову ефективність:

- Пропускна здатність: Використання стандарту 1000BASE-T для дротового сегмента гарантує швидкість передачі даних до 1 Гбіт/с. Це забезпечує стабільну роботу з «важкими» графічними макетами та великими обсягами даних без затримок.

- Бездротова продуктивність: Впровадження точок доступу стандарту 802.11ac дозволяє отримати високу щільність підключень та ефективну пропускну здатність у Wi-Fi середовищі, що є критичним для мобільних користувачів.

- Логічна архітектура: Мережа базується на гібридній топології з сегментуванням на рівні віртуальних локальних мереж (VLAN). Такий підхід мінімізує широкомовний трафік та оптимізує маршрутизацію між підрозділами.

- Стекова модель: Застосування протоколів сімейства TCP/IP забезпечує універсальну сумісність із будь-яким сучасним мережевим обладнанням, клієнтськими пристроями та хмарними сервісами.

- Фінансова дисципліна: Загальний бюджет проєкту, що включає закупівлю активного обладнання (Cisco), пасивних компонентів СКС, монтажні роботи та налаштування, складатиме до 580 000 грн. Ця сума є гранично допустимою та узгодженою з керівництвом підприємства.

Дані показники свідчать про те, що розроблене рішення відповідає принципам оптимального поєднання продуктивності та економічної доцільності, забезпечуючи надійну технічну базу для розвитку видавничої діяльності компанії.

Архітектура мережі передбачає можливість підключення додаткових робочих станцій, мережевого обладнання та серверних ресурсів без необхідності суттєвої перебудови існуючої кабельної системи або зміни логічної структури. Це забезпечує довгострокову експлуатаційну ефективність проєкту, знижує витрати на подальшу модернізацію та створює надійну основу для розвитку інформаційної інфраструктури ТзОВ «HQ Print».

1.1.6 Стадії та етапи розробки

Процес створення мережевої інфраструктури ТзОВ «HQ Print» базується на послідовному проходженні ключових стадій, що забезпечують керованість проєкту на кожному етапі -від початкового аналізу до передачі системи в експлуатацію.

Розподіл робіт систематизовано в таблицю 1.1.

Таблиця 1.1 –Етапи проектування мережі для ТзОВ «HQ Print»

№ п.п.	Етап	Опис діяльності на етапі
1	Аналіз вимог замовника	Формування технічного завдання, визначення кількості робочих місць та потреб у продуктивності.
2	Узгодження та планування	Інспекція приміщень, проєктування кабельних маршрутів та зон розміщення серверної шафи.
3	Вибір обладнання	Підбір активного (Cisco) та пасивного обладнання відповідно до бюджету та вимог надійності.
4	Розробка логічної топології	Створення схеми адресації (VLAN) та визначення принципів маршрутизації трафіку
5	Проєктування фізичної топології	Візуалізація розташування мережевих точок та вузлів доступу на плані приміщень.
6	Монтаж кабельної системи	Фізичне прокладання ліній UTP Cat 6 та встановлення настінних роз'ємів.
7	Інсталяція обладнання	Монтаж серверного пулу та комутаторів у 24U шафу, кросування ліній.
8	Налаштування служб	Конфігурація протоколів TCP/IP, сервісів DHCP, NAT та налаштування політик безпеки (IPFW).
9	Тестування та налагодження	Фізична верифікація ліній, тестування цілісності пакетів, оптимізація швидкості.
10	Фінальна документація	Підготовка паспортів вузлів, інструкцій для адміністраторів та актів здачі робіт.

1.1.7 Порядок контролю та прийому

Фінальним етапом реалізації проєкту є комплексне приймально-здавальне випробування, що підтверджує відповідність побудованої інфраструктури технічному завданню та стандартам якості. Процедура контролю включає перевірку фізичних, логічних та експлуатаційних характеристик мережі ТзОВ «HQ Print».

Навежемо технічні критерії оцінки. Під час тестування здійснюється верифікація критичних параметрів, що безпосередньо впливають на продуктивність:

- Швидкість та пропускна здатність: вимірювання швидкості передачі даних у сегментах 1 Гбіт/с та перевірка стабільності з'єднання між ключовими вузлами.

- Аналіз трафіку: моніторинг обсягів даних, що проходять через порти комутаторів, та виявлення навантаження на ядро мережі.

- Цілісність передачі: виявлення відсотка помилкових кадрів (CRC-помилок), що виникають через неякісний монтаж або електромагнітні перешкоди.

- Стабільність служб: перевірка коректності роботи сервісів DHCP, DNS та міжмережевого екрана IPFW на сервері FreeBSD.

Детальніше опишу інструментарій та методологію. Діагностика проводиться у два етапи:

- Фізичний рівень: сертифікація кабельних ліній Cat 6 за допомогою професійного кабельного тестера (виявлення обривів, коротких замикань та перехресних перешкод).

- Мережевий рівень: використання програмних аналізаторів протоколів та інструментів адміністрування Cisco CLI для зняття статистики стану портів і навантаження на інтерфейси в реальному часі.

Результати всіх тестів документуються у протоколах вимірювань. На основі цих даних складається та підписується Акт введення мережі в експлуатацію, який фіксує перехід системи на стадію поточної експлуатації. Разом з актом замовнику передається повний комплект виконавчої документації, включаючи паспорти вузлів та інструкції з адміністрування, що гарантує прозорість функціонування інфраструктури та можливість її подальшого масштабування силами IT-відділу підприємства

1.2 Постановка задачі на розробку проекту. Характеристика підприємства

Об'єктом дослідження та безпосереднім предметом даної кваліфікаційної роботи є проєктування локальної обчислювальної мережі для ТзОВ "HQ Print". Процес виконання цього завдання включає формування детального технічного завдання з урахуванням усіх потреб компанії, а також вивчення архітектурного планування будівлі для визначення оптимальних шляхів прокладання кабельних магістралей та місць монтажу обладнання. Керуючись результатами аналізу, обирається найбільш доцільна топологія та технологія побудови структурованої кабельної системи (СКС). Наступним кроком стає підбір активних і пасивних мережевих пристроїв з огляду на технічні вимоги та баланс показників ціни й якості. Фінальними стадіями роботи є інсталяція мережі, налаштування комутаційного обладнання, серверних систем та програмних служб.

Основні напрямки діяльності ТзОВ «HQ Print»:

Поліграфічне виробництво: випуск друкованої продукції як малими, так і великими серійними накладами.

Реалізація виробів через партнерські торгові точки та мережеві онлайн-платформи.

Надання інформаційно-консультаційних послуг.

Проведення презентаційної та виставкової роботи, включаючи виготовлення відповідних матеріалів та сувенірної продукції.

Розробка індивідуальних рекламних проєктів та подарункових наборів.

Підприємство розміщується в окремій будівлі, значну частину якої займає друкарський цех. Загальна висота споруди (без урахування даху) становить 5,2 метри. У виробничому приміщенні встановлена масштабна друкарсько-пакувальна лінія, при цьому висота стелі в цій зоні сягає майже 5 метрів. Офісний блок розташований у лівому крилі будівлі на рівні першого поверху, під яким знаходиться цокольне приміщення, що використовується як складська зона та укриття.

Детальний розподіл робочих зон та підрозділів компанії відображений на кресленні «План приміщень». До основних підрозділів підприємства належать:

1. Виробничий відділ (друкарський цех).
2. Підрозділ додрукової підготовки (препрес).
3. Відділи маркетингу та менеджменту.
4. Бухгалтерія.
5. Відділ редагування та коректури.
6. Служба головного інженера та технолога виробництва.
7. Приймальна (офіс-менеджер).
8. Кабінет директора.
9. Відділи дизайну та верстки.
10. Ізольована серверна кімната.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Для забезпечення високої продуктивності, керованості та безпеки проектованої локальної обчислювальної мережі підприємства обрано логічну архітектуру з розподілом на віртуальні локальні мережі (VLAN) на базі стандарту тегування трафіку IEEE 802.1Q. Вибір такого логічного типу мережі обумовлений необхідністю локалізації широкомовного трафіку, оптимізації смуги пропускання та підвищення загального рівня захисту конфіденційних даних. Основним інструментом для реалізації міжмережевої взаємодії та забезпечення високошвидкісного обміну пакетами між створеними віртуальними сегментами виступає комутатор третього рівня (Layer 3), що дозволяє виконувати маршрутизацію трафіку на апаратному швидкодіючому рівні ядра мережі.

Процес логічної організації інфраструктури базується на принципі функціональної сегментації, яка передбачає поділ мережевих вузлів на підмережі з урахуванням технологічної доцільності, ієрархічної структури друкарні та суворих вимог до безпеки інформації. Сформована схема сегментування робочих станцій та мережевого обладнання представлена у таблиці Б.1 додатка Б. Технічні параметри безпосереднього налаштування віртуальних мереж, розподілу адресного простору та закріплення ідентифікаторів VLAN на комутаторах, серверних платформах і бездротових пристроях систематизовано у таблиці Б.2 додатка Б. Зазначені метрики є фундаментальною основою для практичної конфігурації обладнання, оскільки вони чітко регламентують характер інформаційних потоків у межах підприємства і становлять ядро технічної документації мережевого проєкту.

2.2 Розробка схеми фізичного розташування кабелів та вузлів:

2.2.1 Типи кабельних з'єднань та їх прокладка

Проєктування трас прокладання горизонтальних та вертикальних кабельних сегментів структурованої кабельної системи (СКС) виконано у суворій відповідності до міжнародних стандартів (зокрема ISO/IEC 11801 та TIA/EIA-568), а також з урахуванням архітектурних особливостей плану приміщень видавництва та специфічних технічних вимог замовника. Розроблені в межах проєкту креслення «Логічна топологія» та «Фізична топологія» комплексно відображають усі мережеві вузли, комутаційні центри, а також схеми їх підключення та інтеграції в єдиний захищений інформаційний простір підприємства.

Як базове фізичне середовище передачі даних для провідного сегмента мережі обрано неекрановану виту пару категорії 6 (UTP Cat 6). Вибір цього типу кабелю обґрунтований його здатністю стабільно підтримувати швидкість передачі даних до 1 Гбіт/с на відстанях до 100 метрів, а також високим експлуатаційним потенціалом для перспективного переходу на стандарт 10GBASE-T (10 Гбіт/с) без необхідності капітальної реструктуризації кабельних трас, що забезпечує оптимальний баланс вартості та продуктивності інфраструктури.

Фізична топологія провідної частини мережі видавництва реалізована за архітектурою розширеної зірки (Hierarchical Star). Такий підхід передбачає зведення робочих станцій та периферійних комутаторів доступу до центрального комутаційного вузла ядра, що гарантує високу відмовостійкість мережі, простоту масштабування шляхом додавання нових ліній, а також легкість локалізації та усунення можливих несправностей. Базовий приклад побудови та організації такої топологічної структури наведено на рисунку 2.1.

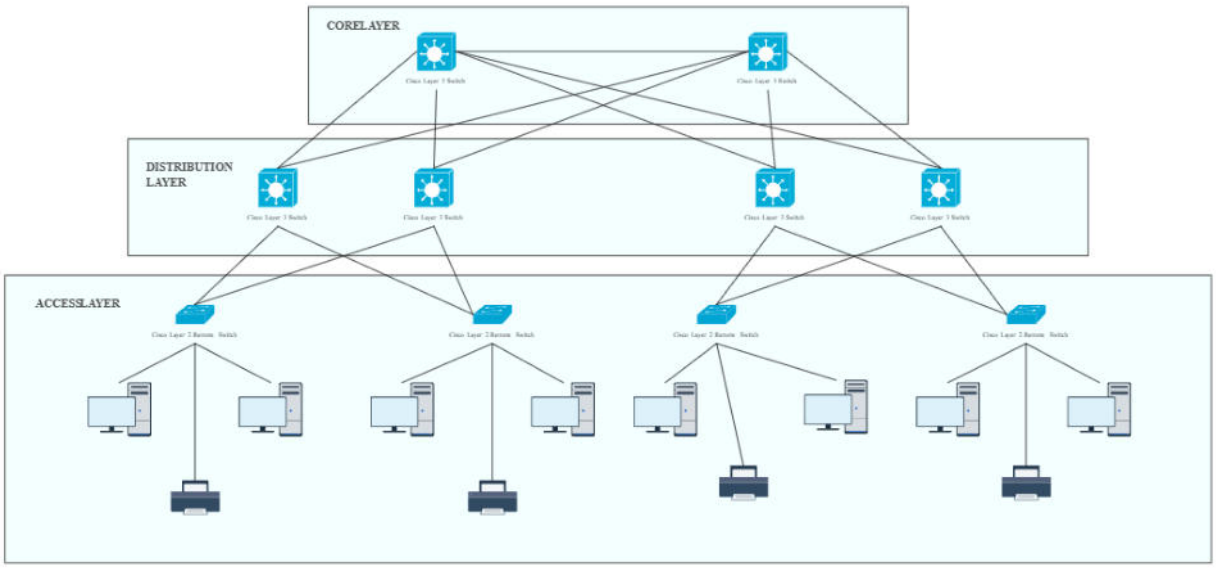

Рисунок 2.1 – Ієрархічна мережева топологія

Інтеграція бездротових сегментів у структуру локальної мережі видавництва зумовлює її гібридний архітектурний вигляд, який поєднує в собі класичну розширену зірку для стаціонарних дротових підключень та елементи комірчастої топології (Mesh) для взаємодії точок доступу у бездротових зонах. Таке технологічне поєднання гарантує максимальну мобільність персоналу в межах офісу при збереженні високої пропускної здатності та надійності магістральних каналів зв'язку.

Практична реалізація горизонтальної підсистеми СКС виконується за чітко регламентованою схемою. Кабельні лінії прокладаються від інформаційних мережевих розеток робочих місць користувачів, проходяться всередині захисних пластикових кабельних каналів (коробів), гофрованих труб або металевих лотків і заводяться до комутаційних шаф. Усередині шаф кабелі розшиваються на крос-панелях (патч-панелях), після чого комутація з портами активного мережевого обладнання Cisco здійснюється за допомогою гнучких сполучних кабелів (патч-кордів) відповідної довжини.

2.2.2 Будова вузлів та необхідність їх застосування

Локальна обчислювальна мережа, розроблена для забезпечення виробничих та адміністративних процесів друкарні, має чітку ієрархічну структуру та складається з таких ключових апаратних вузлів:

- Абонентські розетки (Пасивне обладнання): Представлені настінними та інтегрованими в кабель-канали мережевими розетками RJ-45. Вони призначені для безпосереднього фізичного підключення робочих станцій менеджерів, бухгалтерів, дизайнерів, а також мережевих принтерів і промислового друкарського обладнання до горизонтальної підсистеми СКС.

- Комутатори доступу робочих груп (SW_4, SW_5): В ролі периферійних комутаторів відділів використовуються керовані комутатори Другого рівня Cisco Business 250-24T-4X. Вони забезпечують агрегацію клієнтських підключень у межах своїх технологічних зон (наприклад, відділу менеджменту та виробничого цеху), здійснюють локальну комутацію трафіку на рівні L2 та підтримують технологію віртуальних мереж (VLAN).

- Центральний комутатор ядра мережі (SW_6): Виступає головним інтегруючим вузлом усієї інфраструктури, для чого обрано високопродуктивний комутатор Третього рівня Cisco Business 350-24X. Він об'єднує периферійні комутатори, бездротові точки доступу AP_1, AP_2 та серверний пул. Завдяки підтримці маршрутизації на апаратному рівні (L3), SW_6 здійснює високошвидкісний обмін пакетами між різними VLAN-сегментами компанії.

- серверна платформа FreeBSD (S_1, S_2): Апаратні сервери архітектури x86-64, що виконують критично важливі системні та прикладні функції. Сервер S_1 функціонує як корпоративне сховище даних на базі FTP-демона ProFTPD з відмовостійким дисковим масивом для зберігання важких макетів друку. Сервер S_2 виконує роль прикордонного інтернет-шлюзу,

забезпечуючи захист периметра (IPFW), динамічну адресацію (DHCP) та трансляцію мережевих адрес (NAT).

Організація центрального комутаційного вузла

Головний комутаційний вузол мережі, який містить центральний L3-комутатор ядра SW_6 та серверні платформи S_1 і S_2, розташований у спеціалізованому приміщенні серверної кімнати. Для компактного та безпечного розміщення обладнання використано телекомунікаційну монтажну шафу підлогового типу заввишки 24U стандарту 19 дюймів.

Для даного проєкту обрано шафу українського виробника моделі ШС-24U, загальний вигляд якої представлено на рисунку 2.2.

Рисунок 2.2 – Загальний вигляд комутаційної шафи

Усередині шафи, окрім активного обладнання, інтегровано елементи забезпечення працездатності та захисту:

Патч-панель (19", 1U): Для консолідації та впорядкування магістральних кабельних ліній;

Джерело безперебійного живлення (UPS): Для захисту серверів та комутатора ядра від стрибків напруги та забезпечення автономної роботи системи у разі аварійного відключення електромережі.

Проміжні вузли представлені периферійними комутаторами SW_4 та SW_5, які територіально винесені у відповідні робочі зони підприємства. З метою оптимізації бюджету проєкту та враховуючи невелику кількість портів, у цих приміщеннях не передбачено встановлення окремих громіздких підлогових чи настінних шаф і додаткових крос-панелей.

Комутатори Cisco Business 250 серії мають компактне виконання та низький рівень шуму, що дозволяє, залежно від архітектурних умов та побажань замовника, виконувати їх монтаж настінним способом за допомогою комплектних кронштейнів, розміщувати безпосередньо на технічних поверхнях або маскувати всередині захисних ніш (за фальш-стелею чи під фальш-підлогою).

2.3 Обґрунтування вибору комунікаційного обладнання

У даному підрозділі наведено технічне та функціональне обґрунтування вибору обладнання, що використовується для побудови локальної мережі ТзОВ «HQ Print».

Центральним елементом мережі є комутатор ядра, який забезпечує маршрутизацію між сегментами та агрегацію трафіку. Згідно з затвердженою специфікацією, обрано керований комутатор третього рівня (L3) Cisco Catalyst C9200L-24T-4G-E. Цей пристрій забезпечує високу продуктивність, підтримку розширених функцій безпеки та надійну роботу всього інформаційного середовища компанії.

Для структурних підрозділів (робочих груп) обрано комутатори рівня доступу (L2) Cisco Catalyst C1000-16T-2G-L. Ці 16-портові пристрої оптимально підходять для локалізації трафіку в межах окремих відділів, що дозволяє зменшити навантаження на ядро мережі та забезпечити стабільний зв'язок для робочих станцій. Комутатори монтуються безпосередньо у відповідних зонах, що відповідає вимогам архітектури мережі.

Порівняльний аналіз технічних характеристик зазначених пристроїв наведено у таблицях В.1 та В.2 додатка В.

Для забезпечення роботи серверних служб обрано дві платформи Dell PowerEdge T40: Файловий сервер (S_1): призначений для централізованого зберігання даних та забезпечення доступу до макетів друку та Серверний шлюз (S_2): відповідає за підключення до мережі Інтернет, безпеку (IPFW) та розподіл мережевих адрес.

Рисунок 2.3 – Внутрішня будова сервера Dell PowerEdge T40

Сервер Dell PowerEdge T40 є оптимальним для офісного середовища завдяки високій надійності, використанню процесорів Intel Xeon, підтримці великого обсягу оперативної пам'яті та енергоефективності. Його внутрішня будова представлена на рисунку 2.3.

Для організації бездротового сегмента обрано дві точки доступу Cisco Business 140AC. Вони забезпечують високошвидкісний доступ для мобільних пристроїв, підтримуючи стандарти безшовного покриття та безпеки мережі. Зовнішній вигляд точки доступу представлено на рисунку 2.4.

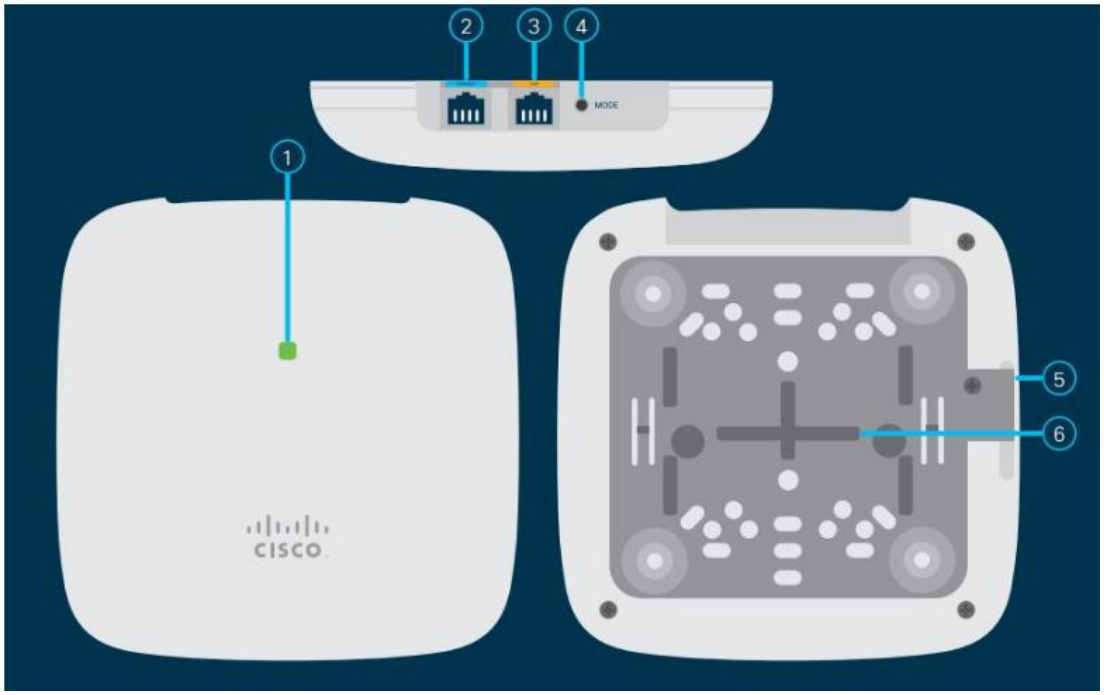

Рисунок 2.4 – Бездротова точка доступу Cisco Business 140AC

1. Світлодіодний індикатор - відображає поточний робочий статус та стан підключення.

2. Консольний порт RJ-45 - інтерфейс для сервісного налаштування та технічної діагностики.

3. Порт PoE-In - забезпечує одночасну передачу даних та живлення пристрою.

4. Кнопка reset - використовується для скидання налаштувань або перемикання режимів.

5. Отвір для гвинта безпеки - призначений для фіксації пристрою від несанкціонованого зняття.

6. Монтажний кронштейн - забезпечує жорстке кріплення точки доступу до поверхні.

Для забезпечення надійності живлення всього активного обладнання використовується джерело безперебійного живлення APC Smart-UPS 2200VA, що дозволяє уникнути перебоїв у роботі під час стрибків напруги. Всі серверні компоненти та комутатор ядра розміщені в телекомунікаційній шафі 24U, яка забезпечує компактне та безпечне розташування обладнання в серверній кімнаті.

Загальний перелік використаного обладнання, що відповідає кошторису проєкту, наведено у підсумковій таблиці 2.1.

Таблиця 2.1 – Перелік обладнання та технічних засобів

№ п/п	Найменування технічних засобів та обладнання	Од. вим.	К-сть	Ціна за одиницю, грн.	Вартість разом, грн.
1	2	3	4	5	6
1	Мережевий керований комутатор третього рівня (L3) Cisco Catalyst C9200L-24T-4G-E	шт.	1	52000	52000
2	Комутатор рівня доступу (L2) Cisco Catalyst C1000-16T-2G-L	шт.	5	19500	97500
3	Бездротова двохдіапазонна точка доступу Cisco Business 140AC	шт.	2	5500	11000
4	Мережеве сховище даних (файловий сервер) Dell PowerEdge T40	шт.	1	46700	46700
5	Серверний шлюз доступу до мережі Інтернет Dell PowerEdge T40	шт.	1	43500	43500

Продовження таблиці 2.1

1	2	3	4	5	6
6	Джерело безперебійного живлення APC Smart-UPS 2200VA	шт.	1	15600	15600
7	Телекомунікаційна шафа 24U для монтажу обладнання в серверній	шт.	1	10350	10350
8	Комутаційна патч-панель на 24 порти (категорія 6)	шт.	1	4120	4120
9	Мережева розетка RJ-45 (категорія 6)	шт.	33	130	4290
10	Пластиковий кабель-канал (короб) для магістралей	м.	175	50	8750
11	Мережевий кабель «вита пара» UTP cat. 6	м.	610	24	14640
12	Комутаційний шнур (патч-корд) cat. 6	шт.	50	34	1700
	ЗАГАЛЬНА СУМА	-	-	-	310 150

2.4 Особливіості монтажу мережі

Для забезпечення високої надійності, стабільності функціонування та якості передачі даних у локальній мережі друкарні монтаж кабельної інфраструктури здійснюється згідно з суворими міжнародними стандартами СКС. Вибір неекранованої витої пари категорії 6 (UTP Cat 6) у якості фізичного середовища передачі даних вимагає безкомпромісного дотримання технологічних регламентів під час прокладання трас, оскільки саме на фізичному рівні найчастіше виникають збої через неякісний монтаж або ігнорування електромагнітних впливів.

Надійний електричний контакт у всіх точках з’єднання гарантується використанням виключно професійних конекторів RJ-45, які повністю сумісні з технічними параметрами кабелю шостої категорії. Процес обтиснення контактів виконується суто спеціалізованим інструментом (кримпером), що дозволяє досягти необхідного зусилля фіксації та запобігти окисленню жил, що в майбутньому могло б спричинити втрату пакетів або зниження швидкості мережевого обміну. Для запобігання неконтрольованому затуханню сигналу, яке є критичним для високошвидкісних мереж 1 Гбіт/с,

довжина кожного постійного сегмента кабельної лінії між кінцевою мережевою розеткою та портом патч-панелі в серверній шафі не повинна перевищувати 90 метрів. Цей показник розрахований з урахуванням допустимих втрат сигналу та запасів для підключення абонентських патч-кордів.

З метою забезпечення захисту від випадкових механічних пошкоджень, критичних перегинів та надмірного натягу кабельні лінії акуратно укладаються в захисні короби, кабельні лотки або гофровані труби, що прокладені згідно з планом приміщень видавництва. Важливою умовою є надійна фіксація кабелів кріпильними елементами через рівномірні інтервали, що виключає «провисання» трас та їх пошкодження в процесі експлуатації. Категорично забороняється використання будь-яких кустарних методів, зокрема саморобних скруток чи неякісних перехідників, оскільки такі рішення призводять до порушення цілісності витих пар, зміни їхнього кроку скручування та, як наслідок, появи значних електромагнітних наводок і спотворень даних. Усі розгалуження, зміни напрямку ліній та виходи до кінцевих вузлів реалізуються виключно через сертифіковані патч-панелі та настінні розетки, що забезпечує легкість подальшого масштабування та адміністрування системи.

Окрему увагу в проєкті приділено питанням електромагнітної сумісності (EMC). Оскільки кабелі передачі даних є чутливими до зовнішніх перешкод, кабель UTP Cat 6 прокладається на відстані щонайменше 50 сантиметрів від силових електричних мереж з напругою 220 В. У місцях, де паралельне прокладання є неминучим, використовуються спеціальні розділові екрани або окремі заземлені металеві лотки, що повністю нівелює вплив електромагнітних полів, які створюються силовими кабелями при високому навантаженні. Дотримання цих монтажних стандартів є фундаментальною запорукою цілісності інформаційних потоків, стабільної роботи серверного обладнання Cisco та довговічності всієї мережевої інфраструктури

видавництва, що дозволяє уникнути виникнення «вузьких місць» на фізичному рівні мережі протягом багатьох років експлуатації.

2.5 Обґрунтування вибору програмного забезпечення

Ефективність функціонування локальної обчислювальної мережі ТзОВ «HQ Print» залежить від коректного вибору та налаштування програмного стека. Увесь програмний комплекс, задіяний у межах проєкту, розділено на три функціональні категорії: спеціалізовані серверні операційні системи, ОС для робочих станцій та прикладне ПЗ для вирішення бізнес-задач.

Серверне програмне забезпечення

Для забезпечення стабільної роботи мережевої інфраструктури в ролі серверної ОС обрано FreeBSD 14.1. Вибір цієї операційної системи зумовлений її високою відмовостійкістю, ефективним керуванням пам'яттю та вбудованим інструментарієм для побудови безпечних мережевих сервісів:

Інтернет-шлюз та мережеві сервіси (S_2): Для динамічного розподілу адресного простору в локальній мережі розгорнуто службу isc-dhcp-server. Захист периметра від несанкціонованого доступу та фільтрацію вхідного/вихідного трафіку забезпечує потужний штатний міжмережевий екран IPFW (IP Firewall). Його гнучка архітектура дозволяє створювати складні правила фільтрації пакетів на канальному, мережевому та транспортному рівнях.

Корпоративне сховище даних (S_1): Для організації безпечного файлового обміну та зберігання критично важливих макетів друку використано FTP-сервер ProFTPD. Це програмне забезпечення обрано через можливість гнучкого налаштування прав доступу, підтримку зашифрованих з’єднань (FTPS) та високу стабільність роботи під великим навантаженням.

Програмне забезпечення робочих станцій

Архітектура мережі друкарні розроблена як агностична до типу операційної системи клієнтських вузлів, оскільки ключовим критерієм є повна підтримка стека протоколів TCP/IP. Це забезпечує гнучкість при виборі робочого середовища для персоналу:

Рекомендовано використання ОС Microsoft Windows 10/11 для забезпечення повної сумісності зі спеціалізованим дизайнерським ПЗ та офісними пакетами.

Для адміністративних та технічних задач допускається використання дистрибутивів Linux (Ubuntu 22.04 LTS та вище), що гарантує високий рівень безпеки та безкоштовність ліцензування.

Вимоги до прикладного програмного забезпечення

Усі прикладні програми, що встановлюються на кінцеві робочі станції, проходять попередню оцінку на предмет інформаційної безпеки. Ключовою вимогою до корпоративного софту є відсутність неперевірених шпигунських модулів та рекламних компонентів (adware), здатних скомпрометувати конфіденційність макетів друку або стати вектором для кібератак. Пріоритет надається перевіреному ліцензійному ПЗ, яке отримує регулярні оновлення безпеки, що дозволяє мінімізувати ризики проникнення шкідливого коду в інформаційний простір друкарні.

2.6 Тестування та налагодження локальної мережі

Після завершення монтажних робіт та початкового налаштування активного обладнання Cisco, мережева інфраструктура ТзОВ «HQ Print» проходить комплексний етап тестування. Цей процес розділений на три рівні: фізичний, мережевий (IP) та прикладний, що дозволяє гарантувати стабільність роботи друкарні.

1. Тестування фізичного рівня (L1)

На початковому етапі проводиться повна верифікація кабельних ліній за допомогою професійного кабельного тестера (або сертифікатора). Тестування дозволяє виявити помилки монтажу: розриви жил, порушення схеми обтиснення (T568B), замикання або перехрещення пар. Кожна лінія СКС перевіряється на відповідність категорії 6, що забезпечує підтримку швидкості 1 Гбіт/с без втрат пакетів через наведення чи надмірне загасання.

2. Тестування протокольного рівня (L3)

Після фізичної комутації проводиться перевірка логічної зв'язності між сегментами VLAN. Для цього застосовуються базові діагностичні інструменти ОС FreeBSD та клієнтських систем:

- ping: використовується для швидкої перевірки наявності зв'язку між комутатором ядра SW_6, серверами S_1/S_2 та робочими станціями.

- tracert (або traceroute): дозволяє простежити шлях проходження пакетів через L3-комутатор ядра, що критично важливо для виявлення петель або помилок у таблицях маршрутизації між віртуальними підмережами.

- arp -a: використовується для перевірки відображення IP-адрес на MAC-адреси мережевих інтерфейсів Cisco.

3. Розширена діагностика та оптимізація

Оскільки мережа побудована на обладнанні Cisco, для глибокого налагодження використовуються специфічні інструменти:

Cisco CLI (Command Line Interface): через консольний порт проводиться моніторинг стану портів (команди show interface, show vlan brief), що дозволяє переконатися у правильному розподілі трафіку по сегментах.

Утиліти Linux/FreeBSD: для перевірки навантаження на інтернет-шлюз S_2 застосовуються системні монітори (top, netstat -i), а для аналізу проходження пакетів і виявлення конфліктів у мережі -консольний аналізатор tcpdump.

Крім того, проводиться перевірка стабільності бездротового сегмента: точок доступу Cisco Business 140AC на предмет зони покриття, рівня сигналу

(RSSI) та відсутності інтерференції з іншими мережами в радіусі дії. Лише після успішного проходження всіх етапів перевірки, де час відгуку (latency) стабільно не перевищує 1-2 мс у локальному сегменті, мережа вважається готовою до введення в експлуатацію.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з інсталяції і налаштування програмного забезпечення серверів

3.1.1 Інструкція з налаштування служби автоконфігурації хостів DHCP

Динамічне призначення мережевих параметрів для робочих станцій, оргтехніки та бездротових пристроїв друкарні реалізується за допомогою протоколу DHCP (Dynamic Host Configuration Protocol). Використання цієї служби дозволяє автоматизувати процес розгортання мережі, уникнути конфліктів IP-адрес та мінімізувати ручне втручання системного адміністратора [20].

У рамках архітектури проєктується централізований DHCP-сервер на базі демона ISC-DHCPD, який функціонує під керуванням операційної системи FreeBSD на сервері шлюзу S_2. Оскільки сервер фізично підключений до інтерфейсу em0 ядра мережі, а клієнти розподілені по різних віртуальних мережах (VLAN 101 – VLAN 111), взаємодія між ними забезпечується за допомогою технології DHCP Relay (запити ретранслюються центральним комутатором Cisco Catalyst на IP-адресу сервера 192.168.1.254).

1. Інсталяція програмного забезпечення

Встановлення пакета DHCP-сервера у FreeBSD виконується з офіційних репозиторіїв за допомогою штатного менеджера пакунків pkg. Для цього в консолі з правами суперкористувача (root) виконується команда:

Bash

```
pkg install isc-dhcp44-server
```

Під час інсталяції система автоматично розгортає необхідні залежності та створює базові директорії для зберігання конфігураційних файлів і бази даних виданих адрес (leases).

2. Конфігурування служби DHCP

Основним файлом налаштувань є /usr/local/etc/dhcpd.conf. У ньому визначаються глобальні параметри мережі (адреси DNS, час оренди), пули динамічних адрес для кожного сегмента друкарні, а також статичні прив’язки для критично важливого обладнання.

Приклад налаштування конфігураційного файлу для адміністративного сегмента (VLAN 101) та фіксованої адреси окремого хоста має такий вигляд:

```
# Глобальні параметри для всієї мережі друкарні
option domain-name "printing.local";
option domain-name-servers 8.8.8.8, 1.1.1.1;
default-lease-time 7200;
max-lease-time 86400;
authoritative;
log-facility local7;
# Опис підмережі керування та локального інтерфейсу сервера
subnet 192.168.1.0 netmask 255.255.255.0
# Конфігурація пулу адрес для підмережі адміністрації (VLAN 101)
subnet 192.168.101.0 netmask 255.255.255.0 {
   range 192.168.101.50 192.168.101.200;
   option routers 192.168.101.1;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.101.255;
}
# Резервування статичної IP-адреси за MAC-адресою для станції верстки
host design_station_1 {
```

```
    hardware ethernet 00:11:22:33:44:55;
    fixed-address 192.168.101.10;
}
```

Інтерпретація основних директив конфігурації:

- option domain-name та option domain-name-servers -задають суфікс локального домену друкарні та IP-адреси глобальних DNS-серверів, які передаватимуться клієнтам;
- default-lease-time і max-lease-time -визначають базовий (2 години) та максимальний (24 години) час оренди мережевих налаштувань пристроєм;
- log-facility -вказує категорію системного журналу (syslog) для реєстрації подій роботи сервера, що спрощує моніторинг та пошук несправностей;
- subnet ... netmask -оголошує межі конкретного мережевого сегмента. Всередині блоку директива range виділяє діапазон для динамічних клієнтів, а option routers вказує адресу шлюзу за замовчуванням (у нашому випадку -це інтерфейс SVI комутатора Cisco у відповідному VLAN);

- host -унікальний ідентифікатор пристрою, де за допомогою параметра hardware ethernet вказується фізична MAC-адреса мережевої карти, а через fixed-address -постійна IP-адреса, яка закріплюється за цим пристроєм назавжди.

3. Інтеграція в автозавантаження та запуск служби

Для автоматичного старту DHCP-сервера під час завантаження FreeBSD, а також для додаткового захисту процесу шляхом його ізоляції в обмеженому середовищі (chroot), необхідно внести відповідні директиви до конфігураційного файлу системи /etc/rc.conf:

Plaintext

```
dhcpd_enable="YES"
```

dhcpd_ifaces="em0"

dhcpd_conf="/usr/local/etc/dhcpd.conf"

dhcpd_chrootdir="/var/db/dhcpd"

dhcpd_flags="-q"

Параметр dhcpd_ifaces="em0" чітко вказує службі прослуховувати лише внутрішній мережевий інтерфейс. Значення dhcpd_chrootdir переносить корінь виконання процесу у безпечний каталог /var/db/dhcpd, що унеможливлює доступ зловмисника до критичних файлів ОС у разі компрометації служби. Права доступу на файли всередині chroot обмежуються системною маскою (umask 022), яка дозволяє читання конфігурацій усім, але запис -виключно власнику процесу dhcpd.

Керування життєвим циклом служби здійснюється стандартними системними скриптами. Запуск сервера виконується командою:

Bash

/usr/local/etc/rc.d/isc-dhcpd start

Перевірка поточного стану працездатності демона:

Bash

/usr/local/etc/rc.d/isc-dhcpd status

У разі успішного ініціалізації система поверне повідомлення із зазначенням ідентифікатора процесу: dhcpd is running as pid [номер_піда]. Якщо служба переходить у стан dhcpd is not running, це свідчить про наявність синтаксичних помилок у файлі конфігурації.

4. Моніторинг роботи та діагностика

Контроль за процесом взаємодії клієнтів із сервером здійснюється через аналіз файлу системного журналу /var/log/messages. Процес видачі динамічної адреси складається з чотирьох стандартних стадій (схема DORA) і фіксується у логах наступним чином:

Plaintext

dhcpd[3412]: DHCPDISCOVER from 00:11:22:33:44:55 via 192.168.101.1

dhcpd[3412]: DHCPOFFER on 192.168.101.50 to 00:11:22:33:44:55 via 192.168.101.1

dhcpd[3412]: DHCPREQUEST for 192.168.101.50 from 00:11:22:33:44:55 via 192.168.101.1

dhcpd[3412]: DHCPACK on 192.168.101.50 to 00:11:22:33:44:55 via 192.168.101.1

У випадках, коли запит надходить від вузла з фіксованою адресою, сервер миттєво зіставляє MAC-адресу із записом у блоці host і здійснює пряму видачу конфігурації:

Plaintext

dhcpd[3412]: DHCPREQUEST for 192.168.101.10 from 00:11:22:33:44:55 via 192.168.101.1

dhcpd[3412]: DHCPACK on 192.168.101.10 to 00:11:22:33:44:55 via 192.168.101.1

Аналіз наведених записів дозволяє адміністратору друкарні в реальному часі відслідковувати підключення нових пристроїв, контролювати навантаження на пули адрес та оперативно реагувати на потенційні аномалії у локальній мережі.

3.1.2 Інструкції з налаштування програмної маршрутизації та міжмережевого екрану

Програмна маршрутизація та захист периметра мережі у цьому проєкті реалізуються на базі серверної платформи Gateway (S_2) під керуванням операційної системи FreeBSD. Основним інструментом для керування трафіком, фільтрації пакетів та трансляції мережевих адрес виступає вбудований системний сервіс ipfw (IP Firewall) у зв'язці з демоном natd.

Процес конфігурування шлюзу безпеки виконується в кілька послідовних етапів:

1. Конфігурування мережевих інтерфейсів

Для забезпечення маршрутизації сервер оснащений кількома мережевими адаптерами. Внутрішній інтерфейс em0 підключається до центрального комутатора ядра мережі (SW_6), а зовнішній інтерфейс em2 забезпечує зв'язок із обладнанням інтернет-провайдера.

Активація внутрішнього інтерфейсу та призначення йому IP-адреси з підмережі керування інфраструктурою здійснюється командою:

Bash

ifconfig em0 inet 192.168.1.254/24 up

2. Створення правил фільтрації трафіку та трансляції адрес (NAT)

Для реалізації механізму маскування внутрішніх IP-адрес (класу Private IP) у реальну публічну адресу провайдера, трафік необхідно перенаправляти через утиліту natd, яка прив'язується до зовнішнього інтерфейсу em2.

Завантаження базового набору правил та увімкнення форвардингу пакетів на рівні ядра ОС виконується за допомогою таких системних команд:

Bash

Увімкнення пересилання IP-пакетів між різними підмережами

sysctl net.inet.ip.forwarding=1

Конфігурування правила NAT: трансляція здійснюється через зовнішній інтерфейс em2

ipfw add 100 divert natd ip from any to any via em2

Дозвіл проходження будь-якого вихідного трафіку через зовнішній інтерфейс

ipfw add 200 pass ip from any to any out via em2

Дозвіл проходження всього локального трафіку всередині корпоративної мережі

ipfw add 300 pass ip from any to any via em0

Запуск системної служби natd для забезпечення трансляції адрес

/etc/rc.d/natd start

3. Налаштування політики безпеки та обмеження доступу

Для захисту внутрішніх ресурсів друкарні та безпосередньо самого сервера від зовнішніх кібератак, на інтерфейсі em2 розгортається політика обмеженого доступу. Наприклад, для заборони несанкціонованих спроб підключення з глобальної мережі Інтернет до веб-сервісів самого маршрутизатора (порт 80), застосовується таке правило фільтрації:

Bash

Заборона вхідних TCP-підключень на 80-й порт з боку Інтернету

ipfw add 400 deny tcp from any to me dst-port 80 in via em2

Розроблена послідовність конфігураційних дій дозволяє розгорнути відмовостійкий шлюз із базовим рівнем захисту інформаційного периметра. Завдяки модульній структурі ipfw, системний адміністратор підприємства має можливість гнучко масштабувати правила фаєрвола, додаючи обмеження для окремих VLAN або впроваджуючи списки доступу (ACL) відповідно до корпоративної політики безпеки.

3.1.3 Інструкції з налаштування файлового серверу

Для забезпечення централізованого обміну макетами, цифровими відбитками та іншою технологічною документацією між відділами друкарні, на базі серверної платформи S_1 розгортається файловий сервер. З метою забезпечення безпеки та розмежування прав доступу, базою для сервісу обрано захищений демон ProFTPD із розширенням FTPS (FTP over TLS), який функціонує під керуванням операційної системи FreeBSD.

Класичний протокол FTP передає автентифікаційні дані та вміст файлів у відкритому вигляді (Plain Text), що створює ризики перехоплення комерційної інформації у локальній мережі. Інтеграція криптографічного протоколу TLS (Transport Layer Security) дозволяє повністю зашифрувати як

канал керування (порт 21), так і динамічний канал передачі даних, гарантуючи конфіденційність інформаційного периметра підприємства.

1. Інсталяція програмного забезпечення

Встановлення FTP-сервера у FreeBSD може здійснюватися як через систему компіляції портів для гнучкого налаштування модулів, так і за допомогою менеджера бінарних пакунків. Для розгортання служби з підтримкою TLS через порти виконується наступна послідовність дій:

Bash

Перехід до каталогу з портом служби

cd /usr/ports/ftp/proftpd

Конфігурування модулів (обов'язково відмітити пункт з підтримкою MOD_TLS)

make config

Компіляція та встановлення сервера в систему

make install clean

2. Генерація криптографічних сертифікатів OpenSSL

Для ініціалізації захищеного з'єднання сервер повинен мати власний сертифікат безпеки та закритий ключ. Створення виділеного каталогу та генерація самопідписаного сертифіката терміном дії на 1 рік (365 днів) здійснюється за допомогою інструментарію OpenSSL:

Bash

Створення захищеної директорії для збереження ключів

mkdir -p /usr/local/etc/proftpd/ssl

Генерація закритого ключа RSA (2048 біт) та самопідписаного сертифіката

openssl req -new -x509 -days 365 -nodes \

-newkey rsa:2048 \

-out /usr/local/etc/proftpd/ssl/proftpd.cert.pem \

-keyout /usr/local/etc/proftpd/ssl/proftpd.key.pem

Обмеження прав доступу до приватного ключа сервера

chmod 600 /usr/local/etc/proftpd/ssl/proftpd.key.pem

3. Конфігурування модулів безпеки ProFTPD

Головний конфігураційний файл розташований за шляхом /usr/local/etc/proftpd.conf. Для активації шифрування у кінець файла додається директива підключення окремого конфігураційного блоку TLS:

Plaintext

Include /usr/local/etc/proftpd/tls.conf

Безпосереднє налаштування параметрів шифрування, визначення дозволених протоколів та шляхів до сертифікатів виконується у файлі /usr/local/etc/proftpd/tls.conf:

Plaintext

<IfModule mod_tls.c>

Активація модуля шифрування

TLSEngine on

Визначення шляху до журналу реєстрації TLS-підключень

TLSLog /var/log/proftpd/tls.log

Заборона застарілих протоколів, використання лише криптостійких версій

TLSProtocol TLSv1.2 TLSv1.3

Вимкнення обов'язкового запиту сертифікатів від клієнтських станцій

TLSOptions NoCertRequest

Шляхи до згенерованих криптографічних компонентів

TLSCertificateFile /usr/local/etc/proftpd/ssl/proftpd.cert.pem

TLSCertificateKeyFile /usr/local/etc/proftpd/ssl/proftpd.key.pem

Вимкнення обов'язкової верифікації клієнтів

TLSVerifyClient off

Обов'язкове форсування шифрування (клієнти без підтримки TLS не допустяться)

TLSRequired on

</IfModule>

Для створення загального мережевого сховища, куди користувачі зможуть завантажувати файли, в операційній системі створюється окрема директорія з відповідними правами доступу на читання та запис:

Bash

mkdir -p /home/public/files

chmod 777 /home/public/files

4. Активація автозавантаження та запуск демона

Для забезпечення стійкості сервісу до незапланованих перезавантажень серверної платформи, демон додається до підсистеми автозапуску ОС. Для цього у конфігураційний файл /etc/rc.conf вноситься відповідний параметр:

Plaintext

proftpd_enable="YES"

Ініціалізація та запуск служби виконуються в штатному режимі без необхідності перезавантаження операційної системи за допомогою вбудованого системного скрипта:

Bash

/usr/local/etc/rc.d/proftpd start

Для перевірки коректності функціонування та моніторингу сесій системний адміністратор може використовувати локальну утиліту ftptop, а детальний аналіз захищених транзакцій здійснюється шляхом перегляду лог-файла /var/log/proftpd/tls.log. Клієнтські станції підключаються до розгорнутого сервера за допомогою спеціалізованого ПЗ (наприклад, FileZilla) із обов'язковим вибором опції «Явний FTP поверх TLS (Explicit FTP over TLS)».

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування центрального комутатора ядра мережі Cisco Catalyst C9200L

Центральний комутатор SW_6 виконує роль ядра та дистриб'ютора локальної мережі підприємства (Core/Distribution Layer). На нього покладаються завдання агрегації магістральних каналів зв'язку від периферійних комутаторів, забезпечення міжвекторної маршрутизації (Inter-VLAN Routing) на третьому рівні (L3) та перенаправлення DHCP-запитів до центрального сервера.

Налаштування пристрою здійснюється через спеціалізований інтерфейс командного рядка (Cisco IOS XE CLI).

1. Первинна ініціалізація та захист пристрою

На початковому етапі виконується базове конфігурування параметрів безпеки, задається унікальне ім'я хоста в мережевій структурі друкарні та обмежується адміністративний доступ:

Cisco CLI

Перехід до привілейованого режиму та режиму глобальної конфігурації

enable

configure terminal

Призначення ідентифікатора пристрою

hostname SW_CORE_6

Встановлення зашифрованого пароля для доступу до привілейованого режиму

enable secret cisco_secure_pass2026

Вимкнення трансляції невідомих команд у DNS-запити (захист від підвисання консолі)

no ip domain-lookup

Конфігурування безпеки консольного порту та ліній віддаленого доступу VTY

line console 0

exec-timeout 10 0

logging synchronous

exit

line vty 0 4

exec-timeout 15 0

login local

transport input ssh

exit

Створення локального облікового запису адміністратора з максимальними правами

username net_admin privilege 15 secret admin_vlan_secure

2. Створення віртуальних локальних мереж (VLAN)

Відповідно до розробленої топології, логічна структура підприємства розділяється на ізольовані широкомовні домени. Нижче наведено унікальний фрагмент створення базових технологічних та адміністративних підмереж друкарні:

Cisco CLI

Створення технологічного сегмента для серверного обладнання

vlan 10

name Servers_Management

exit

Створення сегмента адміністрації та бухгалтерії

vlan 101

```
 name Administration
exit
# Створення сегмента відділу дизайну та додрукарської підготовки (Prepress)
vlan 102
 name Prepress_Design
exit
# Створення сегмента виробничого цеху (друкарські машини та контролери)
vlan 103
 name Production_Floor
exit
# Створення бездротової мережі для співробітників та гостей
vlan 110
 name Wi-Fi_Corporate
exit
```

3. Активація L3-маршрутизації та налаштування SVI-інтерфейсів

Оскільки Cisco Catalyst C9200L є комутатором третього рівня, він самостійно здійснює апаратну маршрутизацію трафіку між створеними VLAN, що розвантажує програмний шлюз. Для кожної віртуальної мережі створюється віртуальний інтерфейс комутатора (SVI), який виступає основним шлюзом (Default Gateway) для клієнтських станцій у цьому сегменті.

Також на цьому етапі інтегрується механізм DHCP Relay (ip helper-address), який перехоплює широкомовні DHCP-запити з кабінетів і пересилає їх на наш сервер FreeBSD (192.168.1.254):

Cisco CLI

```
# Активація функції маршрутизації IP-пакетів на комутаторі
ip routing
```

```
# Налаштування інтерфейсу для серверної підмережі (керування)
interface Vlan10
 description Gateway to Server Subnet
 ip address 192.168.1.1 255.255.255.0
 no shutdown
exit
# Налаштування шлюзу та ретрансляції DHCP для адміністрації (VLAN 101)
interface Vlan101
 description Gateway for Administration
 ip address 192.168.101.1 255.255.255.0
 ip helper-address 192.168.1.254
 no shutdown
exit
# Налаштування шлюзу та ретрансляції DHCP для дизайнерів (VLAN 102)
interface Vlan102
 description Gateway for Prepress and Design
 ip address 192.168.102.1 255.255.255.0
 ip helper-address 192.168.1.254
 no shutdown
exit
# Налаштування шлюзу для виробничої зони (VLAN 103)
interface Vlan103
 description Gateway for Production Equipment
 ip address 192.168.103.1 255.255.255.0
 ip helper-address 192.168.1.254
 no shutdown
exit
```

4. Конфігурування магістральних (Trunk) та клієнтських портів

Для передачі тегованого трафіку (стандарт IEEE 802.1Q) від центрального комутатора до п'яти периферійних комутаторів робочих груп (SW_1 – SW_5), відповідні фізичні інтерфейси переводяться в режим Trunk. Порти, до яких підключаються сервери S_1 та S_2, виділяються в окремий серверний сегмент:

Cisco CLI

```
# Налаштування портів Gi1/0/1 - Gi1/0/5 як магістральних каналів до SW_1-SW_5
interface range GigabitEthernet1/0/1 - 5
 description Trunk link to Access Switches
 switchport mode trunk
 switchport trunk allowed vlan 10,101-103,110
 negotiation auto
exit
# Налаштування порту Gi1/0/10 для підключення файлового сервера S_1 (FreeBSD)
interface GigabitEthernet1/0/10
 description Connection to File Server S_1
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
exit
# Налаштування порту Gi1/0/11 для підключення інтернет-шлюзу S_2 (FreeBSD)
interface GigabitEthernet1/0/11
 description Connection to NAT/DHCP Gateway S_2
 switchport mode access
 switchport access vlan 10
```

```
 spanning-tree portfast
exit
```

Налаштування порту Gi1/0/12 для прямого підключення точки доступу AP_2 (Зона відпочинку)

```
interface GigabitEthernet1/0/12
 description Connection to Wi-Fi AP_2 (Recreation Zone)
 switchport mode access
 switchport access vlan 110
 spanning-tree portfast
 no shutdown
exit
```

Примітка: Команда spanning-tree portfast мінімізує час ініціалізації порту при підключенні серверів, переводячи його в стан пересилання в обхід стандартних затримок протоколу STP.

5. Налаштування маршруту за замовчуванням (Static Route)

Для того, щоб весь трафік, адресований у глобальну мережу Інтернет із будь-якого внутрішнього VLAN друкарні, коректно пересилався на програмний шлюз безпеки S_2, на комутаторі ядра задається статичний маршрут за замовчуванням (Default Route):

Cisco CLI

Статичний маршрут: увесь нелокальний трафік направляється на внутрішній IP шлюзу FreeBSD

```
ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

6. Перевірка конфігурації та збереження змін

Після завершення введення основних параметрів виконується верифікація працездатності створених інтерфейсів та збереження поточної конфігурації з оперативної пам'яті (Running-Config) в енергонезалежну пам'ять пристрою (NVRAM):

Cisco CLI

Перевірка статусу віртуальних інтерфейсів та таблиці маршрутизації

do show ip interface brief | exclude unassigned

do show ip route

Збереження поточної конфігурації системи в NVRAM

write memory

3.2.2 Інструкції з налаштування комутаторів рівня достопу робочих груп

Комутатори рівня доступу (Access Layer) SW_1 – SW_5 призначені для безпосереднього підключення кінцевого обладнання користувачів (робочих станцій, принтерів, точок доступу) до інформаційної інфраструктури друкарні. На відміну від комутатора ядра, ці пристрої працюють на другому рівні моделі OSI (L2). Їхнє головне завдання -маркування (тегування) трафіку клієнтів, ізоляція портів та забезпечення базової безпеки на рівні фізичних підключень.

Конфігурування локального комутатора адміністративного відділу SW_1 виконується через інтерфейс командного рядка Cisco IOS CLI за наступним алгоритмом.

1. Адміністративне налаштування та безпека терміналу

Першочергово встановлюється мережеве ім'я пристрою, обмежуються права доступу до консолі та активується криптографічний протокол SSH для віддаленого керування системним адміністратором:

Cisco CLI

Вхід у режим глобального конфігурування

enable

configure terminal

Призначення унікального імені пристрою для ідентифікації в топології

hostname SW_ACCESS_1

Встановлення пароля на привілейований режим (шифрування Type 8/9)

enable secret cisco_access_pass2026

Створення локального профілю адміністратора

username net_admin privilege 15 secret admin_access_secure

Конфігурування ліній віддаленого доступу з дозволом лише шифрованого SSH-трафіку

line vty 0 4

login local

transport input ssh

exec-timeout 10 0

exit

2. Оголошення віртуальних мереж (VLAN)

Для того, щоб комутатор другого рівня міг коректно обробляти теговані пакети, інформація про використовувані VLAN повинна бути внесена до його локальної бази даних (файлу vlan.dat):

Cisco CLI

Реєстрація віртуальної мережі адміністративного персоналу

vlan 101

name Administration

exit

Реєстрація віртуальної мережі корпоративного Wi-Fi

vlan 110

name Wi-Fi_Corporate

exit

3. Налаштування магістрального порту (Uplink / Trunk)

Для передачі трафіку всіх відділів до комутатора ядра SW_6, виділений гігабітний порт (наприклад, GigabitEthernet0/16) переводиться в режим Trunk. Через цей лінк проходитимуть пакети з тегами стандарту IEEE 802.1Q:

Cisco CLI

Перехід до конфігурування аплінк-інтерфейсу

interface GigabitEthernet0/16

description Uplink trunk connection to SW_CORE_6

switchport mode trunk

switchport trunk allowed vlan 101,110

negotiation auto

no shutdown

exit

4. Конфігурування клієнтських портів доступу (Access Ports)

Порти з 1 по 10 виділяються для дротового підключення комп'ютерів адміністрації та мережевих принтерів. Вони переводяться в режим access і жорстко закріплюються за VLAN 101.

Для захисту від утворення мережевих петель та прискорення роботи портів інтегруються технології PortFast та BPDU Guard:

Cisco CLI

Пакетне налаштування робочих портів користувачів

interface range GigabitEthernet0/1 - 10

description End-user PC and Printer Ports

switchport mode access

switchport access vlan 101

Прискорення активації порту в обхід стандартних затримок STP

spanning-tree portfast

Захист периметра: негайне вимкнення порту в разі підключення стороннього комутатора

spanning-tree bpduguard enable

```
 no shutdown
exit
```

5. Налаштування інтерфейсу керування (In-band Management) та шлюзу

Щоб системний адміністратор міг підключатися до комутатора через SSH з будь-якої точки мережі друкарні, пристрою призначається статична IP-адреса у віртуальному інтерфейсі керування (SVI) та вказується маршрут до шлюзу за замовчуванням (який розгорнутий на L3-комутаторі ядра):

```
Cisco CLI
# Призначення керуючої адреси для комутатора SW_1
interface Vlan101
 description In-band Management Interface
 ip address 192.168.101.2 255.255.255.0
 no shutdown
exit
# Вказання адреси шлюзу ядра мережі для доступу з інших підмереж
ip default-gateway 192.168.101.1
```

6. Фіналізація змін та збереження параметрів

На завершальному етапі виконується перевірка активності інтерфейсів, після чого робоча конфігурація перезаписується з оперативної пам'яті до енергонезалежної пам'яті NVRAM пристрою:

```
Cisco CLI
# Верифікація таблиці комутації та стану VLAN
do show vlan brief
# Фіксація та збереження конфігураційного файла
write memory
```

Нлаштування інших комутаторів доступу здійснюється за аналогічним принципом, змінюються лише номери портів, ідентифікатори VLAN (наприклад, VLAN 102 для дизайнерів на SW_3, чи VLAN 103 для цеху на

SW_5) та індивідуальні IP-адреси керування пристроїв (192.168.101.3, 192.168.101.4 тощо)

3.2.3 Інструкції з налаштування точок доступу AP_1 та AP_2

Розгортання бездротового сегмента мережі друкарні реалізується на базі двохдіапазонних точок доступу Cisco Business 140AC. Логічно обидва пристрої функціонують у межах одного широкомовного домену -VLAN 110 (Wi-Fi_Corporate), проте мають децентралізоване фізичне підключення для оптимізації кабельної інфраструктури:

AP_1 (відділ менеджменту) підключена до порту Gi0/11 периферійного комутатора робочої групи SW_4;

AP_2 (зона відпочинку) підключена безпосередньо до порту Gi1/0/12 центрального комутатора ядра SW_6.

Для спрощення адміністрування та забезпечення безшовного роумінгу (Seamless Roaming) при переміщенні працівників між зонами, точки доступу об'єднуються в єдиний логічний кластер за архітектурою Primary/Subordinate (майстер-підлеглий). Конфігурування всієї бездротової мережі зводиться до трьох послідовних етапів.

Крок 1. Первинна конфігурація головної точки (AP_1) та запуск контролера

Оскільки AP_1 першою вводиться в експлуатацію, вона ініціалізується як Primary-контролер кластера:

Після фізичного підключення до SW_4 точка автоматично отримує IP-адресу в межах VLAN 110 від DHCP-сервера FreeBSD завдяки ретрансляції ip helper-address.

Точка починає трансляцію тимчасової технологічної мережі CiscoBusiness-Setup. Адміністратор підключається до неї (пароль за

замовчуванням: cisco123) та через браузер переходить за адресою https://ciscobusiness.cisco.

У вікні майстра налаштувань (Setup Wizard) задаються базові параметри:

Адміністратор: Створення профілю wl_admin та пароля доступу до керування;

Регіон: Обов'язково вказується Ukraine (для автоматичного вирівнювання потужності передавачів згідно з нормами законодавства);

Параметри мережі (SSID): Задається назва робочої мережі Printing_Corp_WiFi та сучасний профіль безпеки WPA2/WPA3-Personal із ключем доступу.

Після перезавантаження AP_1 стає активним віртуальним контролером мережі.

Крок 2. Автоматична інтеграція точки зони відпочинку (AP_2)

Завдяки технології Cisco Plug-and-Play, введення в роботу другої точки доступу відбувається повністю в автоматичному режимі:

При підключенні AP_2 до порту ядра SW_6 вона успішно отримує динамічну IP-адресу у тому ж VLAN 110.

За допомогою системних службових протоколів Cisco точка AP_2 виявляє в підмережі активний контролер AP_1 і надсилає запит на авторизацію в кластері.

Віртуальний контролер автоматично перевіряє сумісність прошивок, за потреби оновлює мікропрограму AP_2 та прозоро реплікує на неї всі налаштування корпоративної мережі Printing_Corp_WiFi. Ручне створення SSID на другій точці не потрібне.

Крок 3. Оптимізація радіоресурсу та частотне планування

Для виключення інтерференції (взаємного глушіння) радіосигналів у суміжних зонах покриття, адміністратор виконує фінальне налаштування через веб-інтерфейс кластера:

У меню Wireless Settings > Access Points перевіряється активний статус обох точок.

Для діапазону 2.4 GHz, який є найбільш чутливим до завад, за допомогою механізму RRM (Radio Resource Management) або вручну фіксуються непересічні частотні канали: для AP_1 призначається Канал 1, для AP_2 -Канал 6 (або 11).

Вмикається підтримка протоколів 802.11r/k/v для забезпечення безшовного перемикання мобільних пристроїв та терміналів збору даних між точками AP_1 та AP_2 без обриву мережевих сесій та втрати пакетів.

Впроваджена схема централізованого керування дозволяє динамічно масштабувати бездротовий сегмент друкарні, просто додаючи нові точки доступу в будь-який комутатор, де активовано VLAN 110.

3.3 Інструкція з використання тестових наборів та тестових програм

Надійність функціонування локальної мережі друкарні забезпечується трирівневою системою діагностики: апаратною (L1), мережевою (L3) та системною.

1. Апаратні засоби тестування (Фізичний рівень)

Для перевірки структурованої кабельної системи (UTP Cat 5e/6) застосовується два класи пристроїв:

- Базові кабельні тестери: Використовуються для швидкої перевірки цілісності ліній. Вони визначають правильність розпинування провідників за стандартами T568A/B, виявляють короткі замикання чи обриви (виводячи індикацію «OK» / «PASS»).

- Професійні кабельні аналізатори (Сертифікатори): Здійснюють точну сертифікацію ліній, вимірюючи довжину кабелю, затухання сигналу та рівень

наводок. Це дозволяє уникнути помилок фізичного рівня (CRC errors), які сповільнюють передачу макетів до черги друку.

2. Утиліти діагностики мережевого зв'язку (Мережевий рівень)

Для перевірки маршрутизації між VLAN-сегментами використовуються кросплатформні програмні інструменти:

- Команда ping: Працює за протоколом ICMP. Вона надсилає запити до вузлів (файлового сервера S_1 чи шлюзу S_2), визначаючи доступність пристрою, відсоток втрати пакетів та час затримки (RTT).

- Команди tracert / traceroute: Відображають повний шлях проходження пакетів через проміжні пристрої (включаючи L3-комутатор ядра SW_6).

На робочих станціях Windows використовується команда tracert.

В консолі FreeBSD серверів та комутаторів Cisco -утиліта traceroute. Інструмент дозволяє локалізувати вузол, на якому виникає втрата даних.

3. Інструменти моніторингу ОС FreeBSD (Системний рівень)

Для аудиту серверних ресурсів та контролю служб (ProFTPD, DHCP, NAT) на серверах FreeBSD використовуються вбудовані утиліти:

- Утиліта ps (зокрема ps -aux): Формує статичний зріз активних процесів у системі із зазначенням їх PID, власника та рівня споживання процесора (CPU) й оперативної пам'яті (RAM).

- Утиліта top: Забезпечує динамічний моніторинг стану ОС у реальному часі. Вона відображає загальне завантаження процесора, використання RAM/Swap, дискових операцій (I/O) та інтерактивний список найактивніших процесів.

Впровадження комплексної трирівневої діагностики мінімізує ризики збоїв і гарантує безперебійну роботу всієї проектованої мережі друкарні.

3.4 Інструкція з експлуатації та моніторингу системних ресурсів

Операційна система FreeBSD, на базі якої функціонує серверне обладнання мережі (інтернет-шлюз S_2 та файловий сервер S_1), володіє потужним вбудованим інструментарієм для аналізу продуктивності та аудиту безпеки. Системний моніторинг є обов’язковим елементом експлуатації інфраструктури друкарні, оскільки дозволяє превентивно виявляти аномальне споживання ресурсів, контролювати стабільність мережевих служб (DHCP, NAT, FTP) та запобігати відмовам обладнання.

Для моніторингу поточного стану операційної системи та мережевих інтерфейсів використовуються такі базові утиліти:

- top (Table of Processes): Головний інтерактивний інструмент для моніторингу активності процесора та оперативної пам'яті в режимі реального часу. Утиліта відображає загальну статистику системи (завантаження CPU, обсяг вільної та зайнятої RAM, стан Swap-простору) та динамічний список активних процесів. Адміністратор має можливість сортувати процеси за рівнем утилізації ресурсів (процесорного часу, пам'яті, операцій введення-виведення), відстежувати їхні ідентифікатори (PID), власників (UID) та поточний стан виконання.

- vmstat (Virtual Memory Statistics): Призначена для виведення зведеної інформації про стан віртуальної пам'яті, активність процесів у черзі на виконання, кількість переривань процесора та перемикань контексту. Дозволяє оперативно діагностувати дефіцит оперативної пам'яті (пажинг/свопінг) на серверах.

- iostat (Input/Output Statistics): Спеціалізована утиліта для контролю роботи дискової підсистеми. Вона фіксує швидкість передачі даних (Мбайт/с), кількість операцій читання/запису на секунду (IOPS) та коефіцієнт завантаженості жорстких дисків. Є критично важливою для моніторингу

файлового сервера S_1 під час інтенсивного обміну важкими графічними макетами.

- netstat (Network Statistics): Фундаментальний інструмент мережевого аудиту. Відображає вміст таблиць маршрутизації, інформацію про поточні мережеві з'єднання (TCP/UDP), стан сокетів та детальну статистику пропускної здатності інтерфейсів (кількість переданих/втрачених пакетів, CRC-помилки). Використовується на шлюзі S_2 для контролю завантаження зовнішнього інтернет-каналу.

- systat (System Status Display): Універсальний повноекранний інструмент на базі бібліотеки ncurses. За допомогою внутрішніх команд (наприклад, systat -netstat, systat -iostat, systat -ifstat) дозволяє в межах одного вікна консолі комбінувати та візуалізувати графіки завантаження мережевих інтерфейсів, дисків та процесора.

3.5 Інструкції з налаштування засобів захисту мережі

Забезпечення безпеки інформаційно-комунікаційної інфраструктури друкарні базується на концепції ешелонованого захисту (Defense-in-Depth), що передбачає розгортання взаємопов'язаних технічних та організаційних засобів на всіх рівнях моделі OSI. Ключовим елементом на мережевому рівні є чітка сегментація доменів за допомогою віртуальних локальних мереж (VLAN), які логічно ізолюють адміністрацію, менеджерів, виробничий цех та бездротову мережу, унеможливлюючи несанкціоноване перехоплення внутрішнього трафіку. На клієнтських портах комутаторів доступу активовано захист BPDU Guard для запобігання підключенню стороннього обладнання, а міжмережеву фільтрацію транзитного й зовнішнього пакетопотоку забезпечує комутатор ядра разом із центральним шлюзом під керуванням операційної системи FreeBSD.

Для захисту критичних вузлів мережі впроваджено сувору політику рольового керування доступом (RBAC) на основі принципу найменших привілеїв та використання складних криптостійких паролів, що повністю нівелює загрозу успішного проведення атак методом підбору. Передача всієї чутливої інформації здійснюється виключно через захищені протоколи із шифруванням, такі як SSL/TLS, SSH та HTTPS, що запобігає реалізації атак типу «людина посередині» (MitM) та унеможливлює перехоплення автентифікаційних даних або комерційної таємниці у відкритому вигляді. Проактивний захист робочих станцій підсилюється централізованими антивірусними системами, локальними фаєрволами та системами виявлення вторгнень (IDS/IPS) для аналізу сигнатур мережевих пакетів на предмет аномалій. Усі події безпеки фіксуються системною службою syslog для оперативного розслідування інцидентів, а стабільність інфраструктури підтримується регулярним оновленням мікропрограм комутаторів Cisco та пакетів безпеки FreeBSD у поєднанні з інструктажем персоналу щодо протидії соціальній інженерії.

На центральному інтернет-шлюзі мережі функціонує штатний високопродуктивний міжмережевий екран IPFW, який виконує пакетну фільтрацію на канальному, мережевому та транспортному рівнях моделі OSI. Одним із базових правил безпеки під час налаштування периметра є повна заборона використання застарілого та вразливого протоколу віддаленого керування Telnet, який працює на TCP-порті 23, передає дані у відкритому вигляді й повністю замінений на захищений протокол SSH.

Для автоматичного блокування будь-яких спроб несанкціонованого Telnet-доступу до шлюзу чи транзитом через нього до конфігураційного файлу додається правило:

ipfw add 150 deny tcp from any to any 23.

Впровадження цього правила дозволяє скидати шкідливі пакети від будь-якого відправника без надсилання відповіді, що надійно захищає

інфраструктуру підприємства від сканування ефіру та експлуатації відповідних уразливостей на початковому етапі.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на обчислення собівартості та повної ціни проекту мережі. Також важливим є визначення економічної ефективності розробки для ТзОВ «HQ Print» 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 дані витрат часу по окремих операціях технологічного процесу зводяться у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Час викон. операції, год.
1	2	3	4
1	Аналіз вимог замовника	Керівник проекту	5
2	Узгодження та планування	Інженер	12
3	Вибір обладнання	Технік	8
4	Розробка логічної топології	Технік	16
5	Проєктування фізичної топології	Технік	16
6	Монтаж кабельної системи	Технік	40

Продовження таблиці 4.1

1	2	3	4
7	Інсталяція обладнання	Технік	10
8	Налаштування служб	Інженер	12
9	Тестування та налагодження	Інженер	4
10	Фінальна документація	Інженер	12
Разом		-	135

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для ТзОВ «HQ Print» складає 135 годин, з них 5 годин – керівник проекту, 40 годин – інженер та 90 технік.

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:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Отже, основна заробітна плата для працівників становить:

1. Керівник проекту - $З_{осн1} = 5 \cdot 260 = 1300$ грн.
2. Інженер - $З_{осн2} = 40 \cdot 210 = 8400$ грн.

3. Технік - $З_{осн3} = 90 \cdot 180 = 16200$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 1300+8400+16200 = 25900 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника проекту: $З_{дод1} = 1300 \cdot 0,13 = 169$ грн.
- інженера: $З_{дод2} = 8400 \cdot 0,13 = 1092$ грн.
- техніка: $З_{дод3} = 16200 \cdot 0,13 = 2106$ грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 169 + 1092 + 2106 = 3367 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

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

$$В_{о.п} = 25900 + 3367 = 29267 \text{ грн}$$

Крім того, слід визначити відрахування на соціальні заходи становить 22%. Отже, сума відрахувань на соціальні заходи буде становити:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 29267 \cdot 0,22 = 6438,74 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
1	Керівник проекту	260	5	1300	169	-	-
2	Інженер	210	40	8400	1092	-	-
3	Технік	180	90	16200	2106	-	-
Разом				25900	3367	6438,74	35 705,74

Отже, загальні витрати на оплату праці становлять 35 705,74 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни (формула 4.5):

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

де q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi} \qquad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування технічних засобів та обладнання	Од. вим.	К-сть	Ціна за одиницю, грн.	Вартість разом, грн.
1	Мережевий керований комутатор третього рівня (L3) Cisco Catalyst C9200L-24T-4G-E	шт.	1	52000	52000
2	Комутатор рівня доступу (L2) Cisco Catalyst C1000-16T-2G-L	шт.	5	19500	97500
3	Бездротова двохдіапазонна точка доступу Cisco Business 140AC	шт.	2	5500	11000
4	Мережеве сховище даних (файловий сервер) Dell PowerEdge T40	шт.	1	46700	46700
5	Серверний шлюз доступу до мережі Інтернет Dell PowerEdge T40	шт.	1	43500	43500
6	Джерело безперебійного живлення APC Smart-UPS 2200VA	шт.	1	15600	15600
7	Телекомунікаційна шафа 24U для монтажу обладнання в серверній	шт.	1	10350	10350
8	Комутаційна патч-панель на 24 порти (категорія 6)	шт.	1	4120	4120
9	Мережева розетка RJ-45 (категорія 6)	шт.	33	130	4290
10	Пластиковий кабель-канал (короб) для магістралей	м.	175	50	8750
11	Мережевий кабель «вита пара» UTP cat. 6	м.	610	24	14640
12	Комутаційний шнур (патч-корд) cat. 6	шт.	50	34	1700
	ЗАГАЛЬНА СУМА	-	-	-	310 150

Загальна сума матеріальних витрат на розробку мережі становить 310 150 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

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

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

Час роботи ПК над даним проектом становить 109 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії для промислових підприємств в робочий час (7-19 год) на момент розрахунку становить – 15,94 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0{,}5 \cdot 120 \cdot 15{,}94 = 956.40 \text{ грн.}$$

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.

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

де $Т_в$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_в = 310150 \cdot 0{,}09 = 27913{,}5 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фонді. Мінімально допустимі строки їх використання 2 роки [19]. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%} \cdot T, \tag{4.9}$$

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

Враховуючи, що ПК працює над даним проектом 109 год., балансова вартість ПК – 33000 грн., тому:

$$A = \frac{33000 \cdot 0{,}04}{150} \cdot 109 = 959{,}4 \text{ грн.}$$

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.

$$Н_в = В_{о.п.} \cdot 0{,}2...0{,}6, \tag{4.10}$$

де $Н_в$ – накладні витрати.

$H_в = 29267 \ \ 0{,}4 = 11706$ грн.

4.8 Складання кошторису витрат та визначення собівартості НДР

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

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

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	29267	7,55
Відрахування на соціальні заходи	6438,74	1,66
Матеріальні витрати	310150	80,06
Витрати на електроенергію	956,40	0,25
Транспортні витрати	27913,50	7,21
Амортизаційні відрахування	959,20	0,25
Накладні витрати	11706	3,02
Собівартість	387 391,64	100,00

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

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + Т_в + А + Н_в \qquad (4.11)$$

Отже, собівартість дорівнює: $C_в$= 387 391,64 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

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

де $C_в$ – собівартість виконання НДР;

$P_{рен.}$ – рівень рентабельності, в хв'язку з сучасними реаліями в ІТ-галузі може ствновити 20%

ПДВ – ставка податку на додану вартість.

$Ц$ = 387 391,64 · (1+0,2) · (1+0,2) = 557 843,96 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), можна визначити за формулою 4.13 та термін окупності ($T_{ОК}$), який можна визначити за формулою 4.14.

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

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.

$$ЧТВ = -222\,371{,}57 + \frac{194538{,}1}{(1+0{,}15)} + \frac{194538{,}1}{(1+0{,}15)^2} = 93890{,}75\,\text{грн}$$

Термін окупності визначається за формулою:

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

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

$H_В$ – невідшкодовані витрати на початок року, грн.;

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

$$T_{ОК} = 1 + \frac{53208{,}00}{194538{,}1} = 1{,}3$$

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	387 391,64
2.	Плановий прибуток, грн.	77478,33
3.	Ціна, грн.	557 843,96
4.	Чиста теперішня вартість, грн.	93890,75
5.	Термін окупності, рік	1,3

Загальна вартість розробленої комп'ютерної мережі для ТзОВ «HQ Print» становить 557 843,96 грн. Термін окупності становить 1,3 роки.

Отже загальна вартість розробленої мережі поміщується в граничну межу замовника (580 тис. грн.), має хороший рівень рентабельності та термін окупності і рекомендується до впровадження.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

У сучасних умовах проблемою державної та суспільної значущості стає забезпечення безпеки життєдіяльності населення, збереження головної цінності - її громадян, їх здоров'я та життя. Виходячи з сучасних уявлень, безпека життєдіяльності є багатогранним об'єктом розуміння й сприйняття дійсності, що потребує інтеграції різних стратегій, сфер, аспектів, форм і рівнів пізнання [3].

Дотримання базових засад і положень охорони праці є важливим аспектом організації роботи будь-якого підприємства від малого офісу до промислових гігантів. В даному розділі роботи буде описано питання на яких грунтується безпека праці в ТзОВ "HQ Print".

5.1 Методи та засоби захисту від статичної електрики при обслуговуванні локальної мережі

Статична електрика є фізичним явищем накопичення електричного заряду на поверхні або в об'ємі діелектричних та ізольованих провідних матеріалів, яке виникає внаслідок порушення електричної рівноваги у приповерхневих шарах речовини. З погляду фізики процесів, це явище зумовлене трибоелектричним ефектом - перенесенням електронів при контакті та подальшому роз'єднанні двох поверхонь з різними робочими виходами, що призводить до виникнення різниці потенціалів та формування локальних електричних полів високої напруженості [9].

Основними джерелами статичної електрики в умовах експлуатації мережевої інфраструктури є процеси взаємодії синтетичних матеріалів. До них належать переміщення людей по покриттях із синтетичних полімерів (лінолеум, ковролін), використання одягу зі штучних волокон (поліестер, нейлон), а також рух повітряних мас через фільтруючі елементи

вентиляційних систем, що створює заряд на частинках пилу. Крім того, технологічні операції з розмотування кабелів у полімерній ізоляції, тертя пластикових корпусів обладнання об пакувальні матеріали та робота з некоректно заземленим периферійним обладнанням також провокують генерацію електростатичних зарядів.

У контексті обслуговування локальної мережі ТзОВ «HQ Print», де впроваджено високопродуктивне обладнання Cisco та Dell, ризик виникнення електростатичного розряду (ESD - Electrostatic Discharge) стає критичним фактором. Висока щільність монтажу мікросхем, використання компонентів, виготовлених за технологією КМОН (CMOS) з мініатюрними затворами польових транзисторів, роблять обладнання надзвичайно вразливим до пробою діелектричних шарів під впливом розряду навіть при відносно низькій напрузі. Некерований розряд, що проходить через шини даних або порти комутаторів, може викликати як катастрофічні пошкодження у вигляді повної деградації функціональних вузлів, так і приховані дефекти, що призводять до виникнення випадкових помилок, несистемних перезавантажень або зниження пропускної здатності каналів зв'язку.

Для забезпечення ефективного захисту інженерна система повинна базуватися на концепції створення електростатично безпечної зони (EPA - ESD Protected Area) відповідно до вимог стандарту IEC 61340-5-1. Основою такої зони є зрівнювання потенціалів усіх провідних елементів конструкції [9].

Комутаційні шафи повинні бути оснащені внутрішніми шинами заземлення, з’єднаними з основним контуром заземлення будівлі через провідники з мінімальним індуктивним опором. Усі монтажні роботи, що передбачають відкриття корпусів активних пристроїв, повинні проводитися із застосуванням антистатичних браслетів з послідовним резистором номіналом 1 МОм, що обмежує струм розряду до безпечного значення. Використання спеціалізованих ESD-килимків на поверхні робочих столів, які мають

розсіювальні властивості, дозволяє плавно відводити накопичений заряд з корпусів обладнання на шину заземлення, мінімізуючи амплітуду потенційного імпульсу. Окрім цього, підтримання відносної вологості повітря в діапазоні 40–60% є технологічно обґрунтованим заходом, оскільки підвищення вологості сприяє зростанню поверхневої провідності діелектриків, що забезпечує природне розсіювання зарядів.

5.2 Оцінка шумового навантаження від виробничого та мережевого обладнання на робочих місцях

Оцінка шумового навантаження на підприємстві ТзОВ «HQ Print» потребує диференційованого підходу, оскільки акустичне середовище формується двома якісно різними джерелами: високочастотним шумом мережевого обладнання в серверній кімнаті та широкосмуговим імпульсним шумом від промислового друкарського устаткування у виробничому цеху. Згідно з ДСТУ ISO 9612:2018, ідентифікація та оцінка ризиків повинні базуватися на визначенні еквівалентних рівнів звукового тиску, що дозволяє коректно розподілити заходи з охорони праці для різних категорій персоналу [5].

У серверній кімнаті головним джерелом акустичної емісії є сервери Dell та комутатори Cisco, де шумовими характеристиками володіють переважно системи примусового охолодження. Вентилятори, що працюють на високих обертах, генерують стабільний вузькосмуговий шум у діапазоні високих частот. Хоча абсолютні показники рівня звуку в серверній часто нижчі за виробничі (в середньому 65–75 дБА), постійний вплив навіть такого шуму на системних адміністраторів призводить до сенсорного виснаження та зниження когнітивних функцій. Для нівелювання цього впливу застосовується архітектурна акустична ізоляція: стіни приміщення обробляються звукопоглинальними панелями з базальтового волокна, а

телекомунікаційні шафи оснащуються вібродемпферними прокладками, що запобігають передачі структурного шуму на перекриття будівлі.

Натомість друкарський цех є зоною з високим ризиком акустичного травматизму. Робота друкарських верстатів супроводжується механічними ударами, роботою пневматичних систем та приводних механізмів, що створює імпульсний шум рівнем 85–95 дБА і вище. Такий рівень акустичного тиску є небезпечним для слухового апарату працівників, викликаючи незворотні зміни у внутрішньому вусі при тривалому експонуванні. У цій зоні інженерні методи (наприклад, кожухи на верстатах) не завжди здатні знизити рівень шуму до нормативних 80 дБА, тому використання засобів індивідуального захисту слуху є імперативною вимогою. Вибір навушників повинен базуватися на показниках їхнього коефіцієнта шумозаглушення (SNR) - для цеху ТзОВ «HQ Print» необхідно використовувати пасивні навушники з SNR не менше 30–35 дБА, що дозволяє знизити рівень звукового впливу на барабанну перетинку до безпечних 60 дБА.

Між виробничим цехом та офісними приміщеннями ТзОВ «HQ Print» змонтована багатошарова перегородка, що поєднує каркасну конструкцію з мінераловатним наповненням високої щільності та вібродемпферними прокладками на вузлах кріплення до перекриттів, що забезпечує комплексний акустичний розрив для ефективної звуко- та віброізоляції робочих зон.

Організаційний контроль за станом акустичного середовища передбачає періодичний інструментальний моніторинг за допомогою професійних шумомірів 1-го класу точності. Для виробничої зони необхідно розробити та запровадити графік роботи, що обмежує час безперервного перебування персоналу біля джерел шуму без застосування навушників. Окрім того, важливим є навчання персоналу правилам експлуатації ЗІЗ, оскільки навіть найефективніші навушники втрачають свої захисні властивості при неправильному приляганні амбушурів. Таким чином, інтегрована система захисту на підприємстві поєднує технічні рішення (звукоізоляція серверної) з

жорсткою регламентацією використання індивідуальних засобів захисту в цеху, що в сукупності забезпечує відповідність стандартам охорони праці та збереження здоров'я працівників

5.3 Організація контролю за станом охорони праці та визначення рівня запиленості повітря в приміщеннях ТзОВ "HQ Print"

Організація системи контролю за станом охорони праці на ТзОВ «HQ Print» регламентується вимогами НПАОП 0.00-1.71-13 і передбачає функціонування багаторівневої системи моніторингу, спрямованої на раннє виявлення виробничих ризиків [5]. Центральним елементом цієї системи є періодичний інструментальний контроль стану повітряного середовища, який на підприємстві суттєво різниться залежно від функціонального призначення приміщень, що вимагає впровадження специфічних інженерних заходів для кожної зони окремо.

У виробничому друкарському цеху головним джерелом запиленості є паперовий пил, що утворюється внаслідок тертя паперового полотна об вали друкарських машин, а також під час процесів різання, обрізки та фальцювання паперу. Такий пил є дрібнодисперсним та володіє високою летючістю, що призводить до його осідання на обладнанні та вдихання персоналом, що значно підвищує ризики розвитку професійних захворювань органів дихання. Для локалізації цієї загрози безпосередньо в зонах різання та друку впроваджуються локальні витяжні системи, оснащені циклонами-пиловловлювачами, які відсікають аерозольні частинки в місці їх генерації. Додатково застосовується загальнообмінна вентиляція з підвищеною кратністю повітрообміну та багаторівневою системою фільтрації, що дозволяє підтримувати концентрацію пилу в межах гранично допустимих значень для промислових приміщень.

В офісній зоні та серверній кімнаті ТзОВ «HQ Print» характер забруднення повітря є принципово іншим, оскільки тут відсутні процеси механічної обробки паперу, тому основним чинником є накопичення побутового та мікроскопічного атмосферного пилу. У серверній кімнаті навіть мінімальні концентрації такого пилу є критичними, адже при осіданні на друкованих платах комутаційного обладнання Cisco та Dell вони діють як теплоізолятори, порушуючи теплообмін та викликаючи перегрів компонентів. Крім того, пил з домішками вологи або металевих частинок може призвести до утворення мікроскопічних струмопровідних містків, що провокує короткі замикання. Для запобігання цьому офісні та серверні приміщення обладнуються системами припливної вентиляції з використанням фільтрів тонкого очищення класу F7, які забезпечують затримання частинок розміром до 0,5 мкм.

Організаційний контроль запиленості здійснюється шляхом регулярного інструментального вимірювання за допомогою портативних лазерних лічильників частинок, результати якого фіксуються у відповідних журналах. Крім інструментального моніторингу, система охорони праці передбачає обов'язкове проведення планових оглядів стану фільтрів вентиляційних установок, перевірку герметичності приміщень та контроль за дотриманням регламенту вологого прибирання, яке є обов’язковим для виробничих та серверних приміщень. Відповідальність за стан охорони праці покладається на призначених посадових осіб, які забезпечують проведення інструктажів, навчання персоналу правилам користування засобами захисту органів дихання у цеху та контролюють цілісність бар'єрних елементів, що розділяють виробничі та офісні зони, забезпечуючи тим самим цілісність інженерної системи захисту всього підприємства.

ВИСНОВКИ

В кваліфікаційній роботі проведено анлаіз технічного завдань та вимог замовника, зроблено аналітичний огляд літератури та існуючих рішень в даному напрямку. Розроблено логічну та фізичну топологію мережі. Вибрано для мережі пасивне та активне комутаційне обладнання, сервери та їх програмне забезпечення.

Особливу увагу звернуто на конфігурування служби DHCP, та проксі-сервера для доступу до мережі Інтернет. Для забезпечення інформації безпеки мережі в цілому сконфігуровано міжмережевий екран ipfw.

Кваліфікаційна робота містить розроблену логічну і фізичну топології мережі, які подано в графічній частині.

В економічній частині роботи зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі.

Останній розділ квалфікаійної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Антонов В. М. Сучасні комп'ютерні мережі: Навч. Посібник. Київ: «МК-Прес». 2015. 480с.

2. Буров Є.В., Митник М.М. Комп’ютерні мережі: навч. посіб.. Львів: Магнолія 2006. 2026. 262с.

3. Грибан В. Г., Фоменко А. Є., Казначеєв Д. Г. Безпека життєдіяльності та охорона праці: підруч. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2022. 3-88 с.

4. Калита Д. М. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: навч. посіб. для студ. вищих закл. освіти. К. : ВПЦ "Київський ун-т", 2023. 326с.

5. В.І. Кошель, Г.П. Сав’юк, Б.С. Дзундза. Основи охорони праці. навчально-методичний посібник для студентів вищих навчальних закладів педагогічного напрямку. Івано-Франківськ: НАІР, 2020. 182 с.

6. Мельник І. Проектування та дослідження комп'ютерних мереж. К.: Університет «Україна», 2020. 362 с.

7. Методичні вказівки для виконання кваліфікаційної роботи із спеціальності 123 ”Компютерна інженерія”/ Тернопіль: ВСП ТФК ТНТУ, 2022.

8. Николайчук Я.М. Проектування спеціалізованих комп'ютерних систем: Навчальний посібник. Тернопіль: ТзОВ "Терно-граф", 2010. 392с.

9. Основи охорони праці : навчальний посібник / Є. Я. Агєєв. — 2-ге вид., стереотипне. — Львів : «Новий Світ-2000», 2026. — 270 с. Джерело.

10. Погорілий С.Д.. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: Підручник К.: ВПЦ "Київський університет, 2018. 138с.

11. Стухляк П.Д., Микитишин А.Г., Митник М.М.. Телекомунікаційні системи та мережі – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.

12. Царьов Р. Ю. Структуровані кабельні системи : навч. посіб. для студентів вищих навчальних закладів. Одеса: ОНАЗ ім. О.С. Попова, 2018. 260 с

13. APC Smart-UPS 2200VA LCD 230V Technical Specifications. URL: https://www.apc.com/shop/ua/uk/products/APC-Smart-UPS-2200VA-LCD-230V/P-SMT2200I (дата звернення: 01.06.2026).

14. Cisco Catalyst 9200L Series Switches Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-ds-cte-en.html (дата звернення: 07.06.2026).

15. Cisco Catalyst 1000 Series Switches Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/datasheet-c78-744246.html (дата звернення: 07.06.2026).

16. Cisco Business 140AC Access Point Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/wireless/business-100-series-access-points/datasheet-c78-742750.html (дата звернення: 07.06.2026).

17. Dell PowerEdge T40 Tower Server Technical Guide. URL: https://www.dell.com/support/manuals/en-us/poweredge-t40/pet40_ts/ (дата звернення: 07.06.2026).

18. FreeBSD 14.2: URL: https://www.freebsd.org/releases/14.2R/schedule//. (дата доступу: 26.05.2026).

19. IPWF на FreeBSD: URL: https://intellect.icu/fajervol-ipfw-vo-freebsd-nastraivaem-s-nulya-primer-prostogo-konfiga-11170/ (дата зверення: 26.05.2025).

20. Амортизація основних засобів. URL: http://www.visnuk.com.ua/ua/pubs/id/3728/ (дата зверненя: 03.06.2026).

ДОДАТКИ

Додаток А. Таблиця IP-адрес

Таблиця А1 – Таблиця IP-адрес

№ п/п	Позначення вузла	Назва кабінету (відділу)	VLAN	Адреса вузла/Маска	Шлюз
1	2	3	4	5	6
1	WS_1	Відділ додрукової підготовки і кольороподілу	101	192.168.101.1/24	192.168.101.254
2	WS_2			192.168.101.2/24	192.168.101.254
3	WS_3			192.168.101.3/24	192.168.101.254
4	WS_4	Виробничий відділ	102	192.168.102.1/24	192.168.102.254
5	WS_5			192.168.102.2/24	192.168.102.254
6	WS_6	Бухгалтерія	103	192.168.103.1/24	192.168.103.254
7	WS_7			192.168.103.2/24	192.168.103.254
8	WS_8			192.168.103.3/24	192.168.103.254
9	WS_9			192.168.103.4/24	192.168.103.254
10	WS_10	Директор	104	192.168.104.1/24	192.168.104.254
11	WS_11	Сист. адмін		192.168.104.2/24	192.168.104.254
12	WS_12	Відділ верстки і дизайну	106	192.168.106.1/24	192.168.106.254
13	WS_13			192.168.106.2/24	192.168.106.254
14	WS_14			192.168.106.3/24	192.168.106.254
15	WS_15			192.168.106.4/24	192.168.106.254
16	WS_16			192.168.106.5/24	192.168.106.254
17	WS_17			192.168.106.6/24	192.168.106.254
18	WS_18			192.168.106.7/24	192.168.106.254
19	WS_19	Менеджери і маркетологи	107	192.168.107.1/24	192.168.107.254
20	WS_20			192.168.107.2/24	192.168.107.254
21	WS_21			192.168.107.3/24	192.168.107.254
22	WS_22			192.168.107.4/24	192.168.107.254
23	WS_23			192.168.107.5/24	192.168.107.254
24	WS_24	Магазин-склад		192.168.107.6/24	192.168.107.254
25	WS_25	Редактори і коректори	108	192.168.108.1/24	192.168.108.254
26	WS_26			192.168.108.2/24	192.168.108.254
27	WS_27			192.168.108.3/24	192.168.108.254
28	WS_28			192.168.108.4/24	192.168.108.254
29	WS_29	Гол. Інженер	109	192.168.109.1/24	192.168.109.254
30	WS_30	Гол. Технолог	109	192.168.109.2/24	192.168.109.254
31	WS_31	Прийомна	110	192.168.110.1/24	192.168.110.254
32	AP_1	Менеджери	107	192.168.107.50/24	192.168.107.254

Продовження таблиці А1

1	2	3	4	5	6
33	AP_2	Кімната відпочинку	111	192.168.111.50/24	192.168.111.254
34	S_1	Серверна	105	192.168.105.252/24	192.168.105.254
35	S_2		105	192.168.105.253/24	192.168.105.254
			-	Надається провайдером	
36	SW_1	Відділ додрукової підготовки і кольороподілу	1	192.168.1.1/24	192.168.1.254
37	SW_2	Бухгалтерія	1	192.168.1.2/24	192.168.1.254
38	SW_3	Відділ верстки і дизайну	1	192.168.1.3/24	192.168.1.254
39	SW_4	Менеджери і маркетологи	1	192.168.1.4/24	192.168.1.254
40	SW_5	Редактори і коректори	1	192.168.1.5/24	192.168.1.254
41	SW_6	Серверна	1	192.168.1.6/24	192.168.1.254

Додаток Б. Дані сегментування локальної мережі

Таблиця Б1 - Таблиця логічної адресації локальної мережі

№ п/п	Позначення вузлів	Робоча група/К-сть вузлів		Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6	7	8
1	WS_1-WS_3, SW_1	-	4	Відділ додрукової підготовки і кольороподілу	-	101	192.168.101.0/24
2	WS_4-WS_5	-	2	Виробничий відділ	-	102	192.168.102.0/24
3	WS_6 – WS_9, SW_2	-	5	Бухгалтерія	-	103	192.168.103.0/24
4	WS_10, WS_11		2	Директор, сист. адміністратор		104	192.168.104.0/24
5	S_1, S_2, SW_6	-	4	Серверна	-	105	192.168.105.0/24
6	WS_12-WS_18, SW_3		7	Відділ верстки і дизайну	-	106	192.168.106.0/24
7	WS_19-WS_24, SW_4, AP_1	-	8	Менеджери і маркетологи	-	107	192.168.107.0/24

Продовження таблиці Б1.

1	2	3	4	5	6	7	8
8	WS_25-WS_28,SW_5	-	5	Редактори і коректори	-	108	192.168.108.0/24
9	WS_29, WS_30	-	2	Гол. Інженер і технолог	-	109	192.168.109.0/24
10	WS_31	-	1	Прийомна	-	110	192.168.110.0/24
11	AP_2			Кімната відпочинку		111	192.168.111.0/24

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Ном. порту	Тип порту	Назва пристрою	Номер порту	Тип порту	Номер VLAN
1	WS_1-WS_3	Eth0	-	SW_1	2-4	Access	101
2	WS_4-WS_5	Eth0	-	SW_1	5-6	Access	102
3	WS_6 – WS_9	Eth0	-	SW_2	2-5	Access	103
4	WS_10-WS_11	Eth0	-	SW_6	1-2	Access	104
5	S_1, S_2	Eth0, Eth0	-	SW_6	3-4	Access	105
6	WS_12-WS_18	Eth0	-	SW_3	2-8	Access	106
7	WS_19-WS_24, AP_1	Eth0	-	SW_4, SW_6	2-7, 5	Access	107
8	WS_25-WS_28,	Eth0	-	SW_5	2-6	Access	108
9	WS_29-WS_30	Eth0	-	SW_6	2-3	Access	109
10	WS_30	Eth0	-	SW_6	4	Access	110
11	SW_1	1	Trunk	SW_6	11	Trunk	-
12	SW_2	1	Trunk	SW_6	12	Trunk	-
13	SW_3	1	Trunk	SW_6	13	Trunk	-
14	SW_4	1	Trunk	SW_6	14	Trunk	-
15	SW_5	1	Trunk	SW_6	15	Trunk	-
16	AP_2	1	Trunk	SW_6	16	Trunk	

Додаток В. Мережеве обладнання

Таблиця В1 – Порівняльна характеристика комутаторів L3

Характеристика	Cisco Catalyst C9200L-24T-4G-E	Allied Telesis x550-28GT	Juniper EX3400-24T
Кількість портів	24	24	24
Порти Uplink	4x1G SFP	4x10G SFP+	4x10G SFP+
Комутаційна здатність	156 Гбіт/с	128 Гбіт/с	88 Гбіт/с
Функції Layer 3	Advanced (OSPF, EIGRP, ISIS)	Standard (Static, RIP, OSPF)	Advanced (OSPF, BGP, IS-IS)
Керування	Web UI, SSH, Cisco DNA	Web, Telnet, SSH, Autonomous Management Framework (AMF)	Junos CLI, Web, J-Web
Особливості	Найкраща екосистема, підтримка StackWise	Висока стійкість до відмов (AMF)	Висока продуктивність на рівні L3

Таблиця В2 – Порівняльна характеристика 8-ми портових комутаторів

	Cisco Catalyst C1000-16T-2G-L	Aruba Instant On 1930 16G	D-Link DGS-1100-16V2
Кількість портів	16	16	16
Порти Uplink	2x1G SFP	2x1G SFP	-
Тип керування	CLI (професійний), Web UI	Cloud Portal, Web UI	Web UI
Підтримка VLAN	Так (до 256)	Так	Так
Функції безпеки	ACL, 802.1X	Basic ACL	Basic ACL
Надійність	Висока (Enterprise)	Середня	Базова

Таблиця В3 – Порівняння апаратних конфігурацій серверів

Сервер	Dell PowerEdge T40 v04	HP ProLiant ML30 Gen10	ARTLINE Business T19
Тип виконання	Tower		
Процесор	Intel Xeon E-2224G	Intel Xeon E-2124	Intel Core i7-9700F
Чіпсет	Intel C246	Intel C246	Intel H370
Пам’ять оперативна	UDIMM ECC DDR4-2666 МГц (4 слоти, 64 ГБ макс.) – 32ГБ		
Рівні RAID	0/1/5/10 - Intel Rapid Storage Technology(RSTe)		
ЖМД	HDD: 2 x 2 ТБ; SSD: 2 x 500 ГБ		
ЛОМ	Gigabit Ethernet		

Таблиця В4 – Порівняльна характеристика точок доступу

Виробник	Cisco Business 140AC	Aruba Instant On AP22	Ubiquiti UniFi U6 Lite
Стандарт Wi-Fi	Wi-Fi 5 (802.11ac Wave 2)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Пропускна здатність	до 1.2 Гбіт/с	до 1.2 Гбіт/с	до 1.2 Гбіт/с
Керування	Web UI / Мобільний додаток	Cloud Portal / Додаток	UniFi Controller
Технологія MU-MIMO	2x2:2	2x2:2	2x2:2
Підтримка Mesh	+	+	+
Призначення	Середній офіс (стабільна робота)	Малий/Середній бізнес	Домашній/Малий офіс