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

бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі для ТзОВ експертФан "ЧудоОстрів"**

Виконав: студент VI курсу, групи КІб-602

Спеціальності **123 Комп'ютерна інженерія**

(шифр і назва спеціальності)

_____ Андрій ГАЙДУКЕВИЧ

(ім'я та прізвище)

Керівник _____ Андрій ЛЯПАНДРА

(ім'я та прізвище)

Рецензент _____ _____

(ім'я та прізвище)

Тернопіль – 2025

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
"31" березня 2025 року

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

Гайдукевичу Андрію Михайловичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі для ТзОВ експертФан "ЧудоОстрів"**

керівник роботи Ляпандра Андрій Степанович
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 28.03.2025р № 4/9-166а.

2. Строк подання студентом роботи: 13 червня 2025 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;
- модель мережі
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
Охорона праці, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	08.05	
2	Збір і узагальнення інформації	20.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	10.06	
9	Оформлення проекту	14.06	
10	Погодження нормоконтролю	17.06	
11	Попередній захист роботи	21.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 01 квітня 2025 року

Студент _____ Андрій ГАЙДУКЕВИЧ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Андрій ЛЯПАНДРА
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Гайдукевич А.І. Розробка проєкту компютерної мережі для ТзОВ експертФан "ЧудоОстрів": кваліфікаційна робота на здобуття освітнього ступеня бакалавр за спеціальністю «123 – Комп'ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2025. 109 с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі ТзОВ експертФан "ЧудоОстрів" згідно стандартів та вимог замовника. В проектованій мережі використано сучасні стандарти Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac та Ethernet IEEE 802.3q. При цьому реалізовано розподіл мережі на віртуальні підмережі, планування та розподіл адресного простору. Розроблено інструкції з інсталяції та налаштування сервера, VPN-шлюзу, шлюзу доступу до мережі Інтернет, віртуальних підмереж та засобів захисту мережі. Створень віртуальну модель мережі в програмі Cisco Packet Tracert.

Ключові слова: комп'ютерна мережа, сервер, точка доступу, VPN, маршрутизатор, комутатор, віртуальна мережа, VLAN, Cisco Packet Tracert

ANNOTATION

Gaidukevich A.I. Development of a computer network project for LLC expertFan "ChudoOstriv": qualification work for obtaining a bachelor's degree in the specialty "123 - Computer Engineering". Ternopil: VSP "TFK TNTU", 2025. 109 p.

The qualification work involves the development of a computer network project for LLC expertFan "ChudoOstriv" according to the standards and requirements of the customer. The designed network uses modern Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac and Ethernet IEEE 802.3q standards. At the same time, the network is divided into virtual subnetworks, planning and allocation of address space are implemented. Instructions for installing and configuring a server, VPN gateway, Internet access gateway, virtual subnets and network security tools have been developed. A virtual network model was created in the Cisco Packet Tracert program.

Keywords: computer network, server, access point, VPN, router, switch, virtual network, VLAN, Cisco Packet Tracert

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DNS (Domain Name System) – сервер доменних імен.

FTP (File Transfer Protocol) – протокол передачі файлів.

HTTP (Hypertext Transfer Protocol) – протокол передачі гіпертексту.

IEEE 802.3ab – стандарт Gigabit Ethernet на витій парі UTP 5e, 6.

IEEE 802.3z – стандарт Gigabit Ethernet на оптоволоконному кабелі.

IEEE 802.3ac – стандарт, що пребачає збільшення максимального розміру фрейму до 1522 байт, яке дозволяє зберігати інформації про VLAN стандарту IEEE 802.1Q та пріоритету стандарту IEEE 802.1p.

IEEE 802.3u - стандарт Fast Ethernet 100Мбіт/с.

IP (Internet Protocol) – Інтернет-протокол;

IPSec (Internet Protocol Security) – це набір протоколів, які забезпечують безпеку даних, що передаються по IP-мережах.

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

SNMP (Simple Network Management Protocol) – простий протокол мережевого управління. Протокол мережевого адміністрування.

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

VPN (Virtual Private Network) – узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри

WAP (Wireless Access Points) – безпровідні точки доступу

ОС – операційна система.

ПК – персональний комп’ютер.

ВСТУП

У сучасному світі інформаційні технології відіграють ключову роль у функціонуванні та розвитку будь-якого підприємства, незалежно від його розміру та сфери діяльності. Ефективність бізнес-процесів, швидкість обміну інформацією, якість обслуговування клієнтів та безпека даних безпосередньо залежать від надійності та функціональності IT-інфраструктури. В умовах стрімкого розвитку цифрових технологій та зростаючої конкуренції, створення сучасної, масштабованої та безпечної комп'ютерної мережі стає не просто перевагою, а життєвою необхідністю для забезпечення стабільного функціонування та подальшого розвитку.

ТзОВ "ЕкспертФан "ЧудоОстрів" – це національна мережа дитячих магазинів, що динамічно розвивається та налічує понад 40 магазинів у більш ніж 25 містах України. У Тернополі присутні три магазини, склад та головний офіс Тернопільської філії мережі магазинів. Для такого розгалуженого підприємства, з його великим обсягом товарообігу, численними транзакціями та необхідністю ефективного управління складами, логістикою та взаємодією з клієнтами, наявність надійної мережевої інфраструктури є критично важливою.

Саме тому актуальність даної дипломної роботи полягає у розробці проекту комп'ютерної мережі для підприємства ТзОВ "ЕкспертФан "ЧудоОстрів" у м. Тернопіль. Метою проекту є створення оптимізованої, надійної та безпечної мережевої інфраструктури, яка відповідатиме сучасним вимогам, забезпечить ефективну взаємодію всіх підрозділів (включаючи головний офіс та роздрібні точки продажу), автоматизацію ключових бізнес-процесів (таких як облік товарів, продажі, взаємодія з клієнтами) та можливість подальшого масштабування відповідно до зростання мережі магазинів.

У процесі роботи будуть проаналізовані потреби підприємства, розроблені топологія мережі, архітектура її компонентів, а також визначені ключові параметри для забезпечення продуктивності, безпеки та відмовостійкості.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

У кваліфікаційній роботі необхідно розробити проєкт корпоративної комп'ютерної мережі для для ТзОВ "ЕкспертФан", що є власником торгової марки "Чудо Острів" (з урахуванням головного офісу та роздрібних торгових точок).

Основне призначення проєкту полягає у створенні єдиної, централізованої та безпечної інформаційно-телекомунікаційної інфраструктури для ТзОВ "ЕкспертФан "ЧудоОстрів". Ця мережа забезпечить надійний та швидкий обмін даними між усіма ключовими підрозділами компанії: центральним офісом (м. Харків, вул. Академіка Павлова, 144Б) та мережею з понад 40 роздрібних магазинів "ЧудоОстрів", розташованих у понад 25 містах України.

Мережа підтримуватиме безперебійне функціонування критично важливих корпоративних систем, таких як ERP-система (для управління запасами, продажами та фінансами), CRM-система (для ведення клієнтської бази та програм лояльності), системи відеоспостереження в магазинах та на складах, а також IP-телефонія. Вона надасть співробітникам безпечний доступ до інтернету та внутрішніх мережевих ресурсів, а також забезпечить функціонування платформи для онлайн-продажів та взаємодії з клієнтами через веб-сайт та мобільні додатки.

Кінцевими цілями розробки цієї мережі є: підвищення операційної ефективності та продуктивності праці співробітників за рахунок автоматизації бізнес-процесів, централізованого управління даними та прискорення комунікацій; зниження ризиків втрати інформації та посилення рівня кібербезпеки; оптимізація витрат на підтримку IT-інфраструктури за рахунок ефективного використання ресурсів.

1.1.2 Призначення розробки

Призначення розробки нової комп'ютерної мережі для ТзОВ "ЕкспертФан "ЧудоОстрів" полягає у створенні надійної, масштабованої та безпечної інформаційно-телекомунікаційної інфраструктури, яка забезпечить ефективне функціонування всіх бізнес-процесів розгалуженої мережі дитячих магазинів.

Ця розробка покликана вирішити наступні ключові завдання та досягти таких цілей:

- створити єдине інформаційне середовище, яке дозволить ефективно управляти даними з усіх магазинів та головного офісу. Це включає централізований облік товарів, контроль за продажами, управління залишками, консолідацію фінансових звітів та даних про клієнтів;

- забезпечити швидкий та безперебійний доступ до корпоративних систем (таких як ERP, CRM) для всіх співробітників, незалежно від їхнього місцезнаходження. Це прискорить обробку замовлень, оптимізує логістичні процеси та зменшить час на виконання рутинних операцій, що безпосередньо вплине на продуктивність праці та якість обслуговування клієнтів;

- забезпечити надійний зв'язок між головним офісом та роздрібними точками продажу, а також між співробітниками всередині підрозділів. Це включає підтримку IP-телефонії, електронної пошти та інших засобів комунікації, що сприятиме оперативному обміну інформацією та прийняттю рішень;

- захистити конфіденційні корпоративні та клієнтські дані від несанкціонованого доступу, кібератак та втрат. Розробка передбачає впровадження сучасних протоколів безпеки, систем розмежування прав доступу, резервного копіювання та відновлення даних. Це критично важливо для збереження довіри клієнтів та дотримання законодавчих вимог.

- побудувати гнучку мережеву архітектуру, яка дозволить легко інтегрувати нові магазини, склади, відділи або додаткові IT-сервіси в майбутньому. Це забезпечить безперервний розвиток компанії без необхідності повної перебудови IT-інфраструктури при кожному розширенні.

1.1.3 Вимоги до апаратного і програмного забезпечення

При виборі апаратного та програмного забезпечення слід керуватися наступними принципами:

- надійність та відмовостійкість. Усі критично важливі компоненти повинні мати механізми резервування (наприклад, RAID для сховищ, джерела безперебійного живлення);
- масштабованість. Можливість легкого розширення мережі та її компонентів у міру зростання компанії (збільшення кількості магазинів, співробітників, обсягів даних);
- безпека. Забезпечення багаторівневого захисту від несанкціонованого доступу, шкідливого програмного забезпечення та інших кіберзагроз;
- продуктивність. Забезпечення достатньої пропускної здатності та обчислювальної потужності для підтримки всіх корпоративних додатків та сервісів без затримок;
- керованість. Наявність інструментів для централізованого моніторингу, конфігурування та управління мережевими пристроями та серверами;
- сумісність. Забезпечення сумісності між різними апаратними та програмними компонентами;
- енергоефективність. Оптимізація споживання електроенергії обладнанням.

В мережі ТзОВ "ЕкспертФан "ЧудоОстрів" необхідно передбачити встановлення сервера, який буде використовуватись для хостингу корпоративних ERP/CRM систем, баз даних (SQL Server), файлових ресурсів, контролера домену (Active Directory) та сервера резервного копіювання.

Для з'єднання головного офісу з Інтернетом, забезпечення зв'язку між центральним офісом та віддаленими магазинами через VPN-тунелі необхідно передбачити використання маршрутизаторів (по одному на кожен магазин). Основні вимоги до маршрутизаторів:

- підтримка протоколів маршрутизації (OSPF/BGP),

- підтримка функцій VPN (IPsec/SSL VPN);
- підтримка функцій міжмережевого екрану (Firewall) та QoS;
- пропускна здатність для центрального каналу зв'язку – 1-10 Гбіт/с.

Оскільки маршрутизація між підмережами магазинів буде здійснюватись засобами маршрутизаторів то в мережі використовуються лише комутатори рівня доступу, які призначені для підключення робочих станцій, POS-терміналів, та Wi-Fi точок доступу. До цих комутаторів встановлюються наступні вимоги:

- керовані (для централізованого управління та безпеки);
- підтримка PoE/PoE+ для живлення IP-пристроїв;
- підтримка VLANs, QoS, швидкість портів 1 Гбіт/с.

Для забезпечення бездротового доступу для співробітників та, можливо, гостьового Wi-Fi у магазинах передбачено точки доступу Wi-Fi (Wireless Access Points - WAP). Дані пристрої повинні підтримувати стандарти Wi-Fi 6 (802.11ac) або новіших, підтримка кількох SSID, централізоване управління (контролер Wi-Fi), функція ізоляції клієнтів, підтримка PoE.

Для забезпечення фізичного зв'язку між усіма мережевими пристроями та кінцевими точками використовуються кабелі структурованої кабельної системи. В мережі ТзОВ "ЕкспертФан "ЧудоОстрів" кабельна система повинна бути на базі скрученої пари категорії Cat 6/6a для горизонтальної розводки, оптоволоконні кабелі (Multi-mode або Single-mode) для магістральних з'єднань та міжбудівельних прокладок. Також слід використатии патч-панелі, комутаційні шафи.

1.1.4 Вимоги до документації

Документація повинна бути вичерпною, актуальною, зрозумілою та доступною для всіх зацікавлених сторін.

За результатами проектування та впровадження комп'ютерної мережі ТзОВ "ЕкспертФан "ЧудоОстрів" має бути розроблений та наданий наступний комплект документації:

- технічне Завдання (ТЗ) – повний опис цілей, завдань, функціональних та нефункціональних вимог до проектованої мережі;

- пояснювальна записка, яка містить загальний опис архітектурних рішень, обґрунтування вибору технологій та обладнання;

- логічна топологія мережі – схема, що відображає логічну структуру мережі, сегментацію VLAN, IP-адресацію, маршрутизацію, розташування серверів та ключових мережевих сервісів;

- фізична топологія мережі – схема розташування мережевого обладнання (сервери, маршрутизатори, комутатори, точки доступу) та прокладки кабельних трас у головному офісі та типовому магазині;

- схема адресації – детальний план IP-адресації (IPv4/) для всіх сегментів мережі, VLAN ID, діапазони DHCP;

- специфікація обладнання та програмного забезпечення – детальний перелік усього необхідного апаратного забезпечення (з моделями, характеристиками, кількістю) та ліцензійного програмного забезпечення;

- план розміщення обладнання – схеми розміщення серверних шаф, комутаторів, точок доступу та іншого обладнання в приміщеннях.

- інструкції з інсталяції та первинного налаштування – покрокові інструкції для розгортання та базового налаштування всіх компонентів мережі;

- журнал обліку обладнання – перелік встановленого обладнання із серійними номерами, датами встановлення, гарантійними термінами.

1.1.5 Техніко-економічні показники

Проєктована локальна мережа ТзОВ "ЕкспертФан "ЧудоОстрів" повинна відповідати наступним ключовим техніко-економічним характеристикам:

- основний провідний сегмент реалізовано за стандартом Gigabit Ethernet (IEEE 802.3ab).

- розрахована на обслуговування 48 робочих станцій;

- використовує кабель "вита пара" категорії 6 як середовище передачі даних;

- захищені шифровані канали з’єднання між окремим магазинами через загальнодоступні ресурси Інтернет;

- загальна вартість мережі не перевищує 700 тис. грн.

1.1.6 Стадії та етапи розробки

Нижче представлені основні стадії та етапи, які будуть реалізовані під час проектування та впровадження мережі для ТзОВ "ЕкспертФан "ЧудоОстрів".

Перша стадія – це передпроектне обстеження та формування вимог. Ця стадія є фундаментом усього проєкту. Її мета – зібрати максимально повну інформацію про поточні потреби та цілі підприємства, а також визначити технічні та організаційні обмеження.

Друга стадія – це власне проектування мережі. На цій стадії відбувається розробка детальних технічних рішень на основі затвердженого технічного завдання. Ця стадія складається із трьох етапів.

Перший етап – розробка архітектури мережі, що включає:

- вибір топології мережі (зірка, ієрархічна, mesh) з урахуванням розподіленої структури "ЧудоОстрова";

- визначення логічної структури (сегментація VLANs, план IP-адресації).

- розробка моделі взаємодії між головним офісом та віддаленими магазинами (VPN-з'єднання, централізований доступ).

Другий етап – підбір апаратного та програмного забезпечення, що включає:

- вибір конкретних моделей серверів, маршрутизаторів, комутаторів, міжмережевих екранів, точок доступу Wi-Fi, робочих станцій, POS-терміналів та периферійного обладнання;

- вибір операційних систем, мережевих сервісів, прикладного та захисного програмного забезпечення;

- обґрунтування вибору з огляду на вимоги до продуктивності, надійності, безпеки та бюджету.

Третій етап – це розробка детальних проектних рішень та документації , що включає:

- створення детальних логічних та фізичних схем мережі;
- розробка плану кабельної системи (розводка, розміщення розеток, серверних шаф);
- формування специфікації обладнання та програмного забезпечення (BoM – Bill of Materials);
- підготовка інструкцій з конфігурування ключових мережевих пристроїв та серверів.

На третій стадія здійснюється впровадження (інсталяція та налаштування) мережі. Це стадія безпосередньої реалізації проекту, яку можна розділити на три етапи.

На першому етапі здійснюється закупівля та постачання обладнання. Оформлення замовлень, контроль за поставками необхідного обладнання та ліцензійного ПЗ.

На другому етапі виконується монтаж та інсталяція обладнання.

Третій етап – це базове налаштування та конфігурація мережі, що включає:

- інсталяцію операційних систем на сервери та робочі станції;
- базове налаштування мережевого обладнання (IP-адресація, VLANs, маршрутизація);
- налаштування основних мережевих служб (DNS, DHCP, Active Directory);
- встановлення та налаштування корпоративного програмного забезпечення (ERP, CRM, POS).

Четверта стадія розробки проєкту мережі ТзОВ "ЕкспертФан "ЧудоОстрів" – це тестування та її оптимізація. На цій стадії відбувається перевірка функціональності та продуктивності розгорнутої мережі і складається із трьох етапів.

На першому етапі тестування та оптимізація мережі виконується функціональне тестуванняє

На другому етапі здійснюється тестування продуктивності та навантаження мережі

Третій етап – оптимізація та доробки, включає:

- внесення коректив у налаштування обладнання та ПЗ;
- тонке налаштування продуктивності та безпеки.

П’ята стадія розробки проєкту мережі ТзОВ "ЕкспертФан "ЧудоОстрів" включає процес введення в експлуатацію та навчання. Це завершальна стадія перед передачею системи замовнику.

Шоста стадія розробки проєкту мережі ТзОВ "ЕкспертФан "ЧудоОстрів" – це підтримка та супровід (постексплуатація). Хоча ця стадія виходить за межі безпосереднього проектування та впровадження, вона є критично важливою для довгострокової ефективності мережі.

1.1.7 Порядок контролю та прийому

Метою контролю та прийому є забезпечення відповідності розробленої та впровадженої мережі всім вимогам Технічного завдання, стандартам якості та очікуванням замовника – ТзОВ "ЕкспертФан "ЧудоОстрів".

Контроль за ходом виконання робіт здійснюється на наступних ключових етапах:

- контроль на стадії передпроектного обстеження та формування вимог, визначає повноту та коректність зібраних вихідних даних, адекватність сформованих вимог, повнота розробленого технічного завдання..
- контроль на стадії проектування мережі. На цьому етапі перевірється відповідність архітектури мережі та обраних рішень вимогам ТЗ, обґрунтованість вибору апаратного та програмного забезпечення, повнота та коректність проектної документації;

- контроль на стадії впровадження. На цьому етапі здійснюється перевірка дотримання графіка робіт, якості монтажних робіт, коректності інсталяції та базового налаштування обладнання та програмного забезпечення. Процес контролю полягає у подачі регулярних звітів виконавця про хід робіт. Результатом даного етапу є проміжні акти виконаних робіт (за етапами монтажу/інсталяції) або звіт про готовність до тестування.

Приймання системи в експлуатацію здійснюється після завершення всіх робіт з проектування, впровадження та тестування.

На етапі тестування та оптимізації здійснюється перевірка функціональності та продуктивність мережі, відповідність реалізованого функціоналу вимогам ТЗ, відсутність критичних помилок. При цьому проводяться комплексні тестування. Виконавець здійснює всі види тестування, передбачені ТЗ (функціональне, навантажувальне, безпеки, відмовостійкості).

Представники замовника (ІТ-спеціалісти, кінцеві користувачі) беруть участь у процесі приймально-здавальних випробувань (ПЗВ) згідно з програмою та методикою випробувань.

Усі результати тестування фіксуються у протоколах, виявлені недоліки вносяться до переліку виявлених зауважень та недоліків.

Виконавець усуває виявлені недоліки у встановлені терміни.

Результатом етапу тестування та впровадження мережі будуть протоколи успішних приймально-здавальних випробувань та Акт усунення зауважень (за наявності).

На етапі передачі документації та навчання перевіряється повнота, актуальність та якість розробленої експлуатаційної документації, ефективність проведеного навчання персоналу замовника.

Повний комплекту документації, передбаченої розділом "Вимоги до документації" передається замовнику.

Після успішного завершення всіх попередніх етапів та усунення всіх виявлених недоліків, виконавець надає систему замовнику для фінального приймання. Замовник підтверджує готовність системи до експлуатації.

Результатом цього процесу буде підписаний обома сторонами Акт приймання-передачі комп'ютерної мережі ТзОВ "ЕкспертФан "ЧудоОстрів" в промислову експлуатацію. З моменту підписання цього акту система вважається прийнятою, і починається термін гарантійного обслуговування.

1.2 Опис задачі та характеристика підприємства ТзОВ "ЕкспертФан "ЧудоОстрів"

ТзОВ "ЕкспертФан "ЧудоОстрів" є національною мережею дитячих магазинів, що динамічно розвивається та спеціалізується на роздрібній торгівлі товарами для дітей. Компанія веде свою історію з відкриття першого магазину в Харкові у 2011 році і на сьогоднішній день налічує понад 40 магазинів, розташованих у понад 25 містах України. У Тернополі розташовано головний офіс Тернопільської філії із головним магазином та три магазини-філії розташовані в різних мікрорайонах міста.

Основна діяльність компанії включає:

- роздрібну торгівля широким асортиментом товарів для дітей: іграшки для дівчат, хлопців та немовлят, спортивні товари, дитячий транспорт, дитячі меблі та інші супутні товари;
- у деяких магазинах пропонуються оригінальні та сучасні стрижки для маленьких відвідувачів.
- організація акцій, промо-заходів та дитячих свят для залучення клієнтів та підвищення їхньої лояльності.

Як вже повідомлялось підприємство складається з центрального офісу та трьох філій, розташованих у різних районах міста Тернополя.

У центральному офісі зосереджені адміністративні, фінансові, маркетингові та логістичні підрозділи. Кількість співробітників 35 осіб. Використовується для обробки замовлень, управління запасами, ведення бухгалтерського обліку, маркетингових кампаній та загального управління діяльністю підприємства. Крім цього в будівлі центрального офісу розташовано головний магазин та

складські приміщення. План приміщення головного офісу представлено на додатку А.

Крім головного магазину в різних мікрорайонах Тернополя розташовано три магазини-філії. Кожна філія є повноцінним роздрібним магазином з власним штатом продавців-консультантів, касирів та адміністраторів. Плани приміщення головного офісу представлено на додатку А.

Поточна ІТ-інфраструктура характеризуватися фрагментованістю, відсутністю єдиних стандартів, застарілим обладнанням та відстутністю локального мережевого з’єднання. Це призводить до таких проблем, як: ускладнений обмін даними між головним офісом та магазинами, повільна робота облікових систем, ризики втрати або неактуальності даних, низький рівень інформаційної безпеки, високі витрати на адміністрування та обмежені можливості для швидкого впровадження нових сервісів та технологій.

На підприємстві планується впровадження низка інформаційних систем для ефективного функціонування, яких необхідне з’єднання всіх пристроїв в локальну мережу із централізованим керування зі сервера, таких як:

- система обліку та управління торгівлею (Парус), яка буде використовуватись для обліку товару, складських операцій, управління продажами, ведення клієнтської бази, формування звітів;
- POS-терміналів для здійснення розрахунків з покупцями;
- системи відеоспостереження для забезпечення безпеки у філіях та центральному офісі;
- CRM-система lля управління взаємовідносинами з клієнтами.

Враховуючи всі ці фактори виникла необхідність створення єдиною корпоративної мережі для ТзОВ "ЕкспертФан "ЧудоОстрів" у місті Тернопіль.

Метою даного проекту є розробка проекту сучасної, надійної, масштабованої та безпечної комп'ютерної мережі для ТзОВ "ЕкспертФан "ЧудоОстрів".

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Аналіз та обґрунтування вибору топології та технології мережі

Цей підрозділ кваліфікаційної роботи присвячений детальному аналізу та обґрунтуванню вибору оптимальної топології та технологій для побудови комп'ютерної мережі підприємства ТзОВ "ЕкспертФан "ЧудоОстрів" з урахуванням його поточної структури, потреб та перспектив розвитку.

Розглянемо найпоширеніші топології та їх придатність для даної проектованої мережі.

Технологія шина (Bus) полягає у під’єднанні до єдиного кабеля послідовно всіх пристроїв. Її основна перевага – простота реалізації, мінімальна кількість кабелю для невеликих мереж. Проте дана тополоогія вирізняється низькою надійність (вихід з ладу кабелю виводить з ладу всю мережу), складністю діагностики, низькою масштабованістю, наявністю великої кількості колізії.

Дана топологія для "ЕкспертФан "ЧудоОстрів" не підходить, оскільки підприємство має розподілену структуру та високі вимоги до надійності, що суперечить основним характеристикам шинної топології.

Топологія кільце (Ring) полягає у послідовному під’єднанн всіх мережевих пристроїв, при чому останній з’єднується із першим в коло. Основні переваги даної топології полягають у рівномірному розподілі навантаження, можливості передачі даних в одному або двох напрямках. Серед недоліків слід відзначити високу вразливість (обрив кабелю чи вихід з ладу одного вузла порушує роботу всієї мережі, якщо немає дублювання), складність додавання нових пристроїв.

Недолік високої вразливості можна усунути запровадженням топології подвійного кільця (Dual Ring), але при цьому виникають недоліки високої вартості обладнання та складності впровадження та налаштування.

Для "ЕкспертФан "ЧудоОстрів" топологія кільце не підходить, тому що вона і може бути відмовостійкою при подвійному кільці, для такої структури як "ЕкспертФан "ЧудоОстрів" є занадто складною та неефективною.

Топологія зірка (Star) полягає у з’єднанні всіх кінцевих мережевих пристроїв до єдиного центру в якому може бути встановлено комутатор або концентратор. Основні переваги топології полягають у високій надійність (вихід з ладу одного вузла не впливає на інші), легкості додавання нових пристроїв (масштабованості), простій діагностиці, централізованому управлінні. Основні недоліки – це висока залежність від центрального пристрою (комутатора/хаба) та велика витрата кабелю для великих мереж.

Для проектованої мережі "ЕкспертФан "ЧудоОстрів" цілком підходить для локальних мереж у межах головного офісу та кожної окремої філії. Забезпечує необхідну надійність та керованість на рівні підрозділу.

Деревовидна (Tree) топологія або ієрархічна розширена зірка полягає у з’єднанні декількох центральних пристроїв окремих зірок у ієрархічну структуру, що дозволяє поділи мережу на окремі підрозділи з’єднучи їх із комутуючими пристроями вищого рівня, такими як коіматори рівня розподілу та комутатори рівня ядра мережі. Дана топологія поєднаю переваги шини та зірки, легко масштабується, забезпечує централізоване управління для частин мережі. Основними недоліками є залежність від кореневого пристрою, складність прокладання кабелю для великих мереж.

Для проектованої мережі "ЕкспертФан "ЧудоОстрів" підходить як основна логічна топологія для об'єднання локальних мереж філій та центрального офісу. Дозволяє ієрархічно організувати мережу з центральним офісом як коренем та філіями як гілками.

Топологія сітка (Mesh) полягає у безпосередньому з’єднанні всіх кінцевих пристроїв на пряму. При цьому створюється складна сітка мережевих з’єднань. Основними перевагами даної топології є максимальна відмовостійкість (багато шляхів між будь-якими двома вузлами) та висока пропускна здатність. Серед недоліків слід відзначити дуже високу вартість реалізації (велика кількість кабелю та портів) та складність управління.

Для проектованої мережі "ЕкспертФан "ЧудоОстрів" повна сітчаста топологія є надмірною та економічно невиправданою для зв'язку між філіями.

Однак принципи часткової сітчастої топології (наприклад, дублювання каналів між ключовими вузлами) можуть бути використані для підвищення надійності.

На основі аналізу, для ТзОВ "ЕкспертФан "ЧудоОстрів" буде застосовано ієрархічну (деревоподібну) топологію мережі з елементами зірки.

На рівні локальних мереж (LAN) центрального офісу та кожної філії буде використана топологія "Зірка". Кожен комп'ютер, POS-термінал та камера відеоспостереження буде підключений до центрального комутатора (або групи комутаторів) в межах свого приміщення. Це забезпечить:

- легкість розширення (додавання нових робочих місць);
- просту діагностику (вихід з ладу одного кабелю чи пристрою не впливає на інші);
- централізоване управління трафіком та безпекою на рівні підрозділу.

На рівні глобальної мережі (WAN) між центральним офісом та філіями буде реалізована логічна топологія "Дерево" (або "Зірка" у контексті WAN). Центральний офіс виступатиме головним вузлом, до якого підключатимуться всі філії. Це дасть змогу:

- централізовано керувати доступом до корпоративних ресурсів (сервери, бази даних);
- ефективно маршрутизувати трафік між філіями через центральний офіс;
- спростити впровадження єдиної політики безпеки та QoS;
- забезпечити ефективну взаємодію між усіма підрозділами.

Для підвищення надійності між центральним офісом та філіями можуть бути розглянуті варіанти резервування каналів зв'язку, що є елементом часткової сітчастої топології.

При виборі мережевої технології ключовими факторами є необхідна швидкість передачі даних для абонентів та обрана топологія мережі. Оскільки технічне завдання вимагає забезпечення швидкості не менше 1 Гбіт/с і передбачає топологію "розширена зірка", технологія Gigabit Ethernet є найбільш відповідною цим критеріям. Вона ефективно задовольняє ці вимоги, пропонуючи достатню продуктивність для даної архітектури.

Технологія Gigabit Ethernet підтримує передачу даних через три основні типи кабелів: одномодове оптичне волокно, багатомодове оптичне волокно та кручена пара.

Стандарти IEEE 802.3, що регламентують Gigabit Ethernet, поділяються на дві основні групи:

- IEEE 802.3z – для оптоволоконних з'єднань (також відомий як 1000BASE-X);
- IEEE 802.3ab – для з'єднань на крученій парі.

Оптоволоконні стандарти (IEEE 802.3z / 1000BASE-X) призначені для передачі даних по оптоволоконному кабелю і включає кілька специфікацій:

- 1000BASE-SX (Short Wavelength): Використовує багатомодове оптичне волокно та короткохвильові лазери (850 нм). Ідеально підходить для коротких відстаней (зазвичай до 550 метрів), що робить його оптимальним для мереж у межах однієї будівлі або кампусу.
- 1000BASE-LX (Long Wavelength): Працює як з одномодовим, так і з багатомодовим оптичним волокном, використовуючи довгохвильові лазери (1300 нм). Забезпечує передачу даних на значно більші відстані: до 5 км на одномодовому волокні та до 550 метрів на багатомодовому. Це робить його придатним для міжбудівельних з'єднань у місті або для магістральних каналів.
- 1000BASE-LH (Long Haul): Це розширення 1000BASE-LX, розроблене для передачі даних на ще більші відстані по одномодовому оптичному волокну, досягаючи 10 км і більше, завдяки використанню вдосконалених технологій передачі.
- 1000BASE-CX: Хоча менш поширений, цей стандарт використовує мідні збалансовані кабелі для дуже коротких з'єднань (до 25 метрів), зазвичай усередині серверних стійок або між близько розташованими пристроями.

Стандарт IEEE 802.3ab, відомий як 1000BASE-T, призначений для передачі даних по мідній крученій парі (наприклад, кабелі Категорії 5e, 6 або вище). Він забезпечує швидкість 1 Гбіт/с на відстань до 100 метрів.

1000BASE-T є надзвичайно популярним вибором для більшості локальних мереж завдяки своїй економічності та можливості використовувати вже існуючу кабельну інфраструктуру.

Враховуючи потреби підприємства, розміри приміщень та керуючись принципом економічної доцільності, для дротового сегменту мережі було обрано специфікацію 1000BASE-T. Це рішення дозволить створити швидку та надійну локальну мережу з оптимальними витратами.

Відповідно до обраної технології буде використовуватися структурована кабельна система (СКС) на базі кабелю кручена пара (UTP) категорії 6, який забезпечує кращі характеристики та запас для майбутнього (наприклад, 10 Gigabit Ethernet на коротких відстанях) ніж категорія 5e. Для серверних та магістральних з'єднань вирішено використати оптичне волокно для більшої відстані та пропускної здатності.

Як вже зазначалося в розділі 1.1.3, запланована мережа матиме як кабельне з’єднання, так і безпровідні сегменти.

Сучасні безпровідні мережі переважно використовують електромагнітні (радіо) хвилі для передачі інформації. Хоча існують технології на основі інфрачервоного та лазерного випромінювання, їх використання обмежене через високу чутливість до механічних перешкод, які можуть блокувати сигнал. Серед радіохвильових технологій найпоширенішими є Bluetooth, Wi-Fi та WiMAX [3].

Bluetooth стала однією з перших технологій для бездротової передачі даних на невеликі відстані. Вона регламентується стандартом IEEE 802.15 і переважно використовується для побудови персональних мереж (PAN). Bluetooth забезпечує зв'язок на короткі відстані (10-100 м) у неліцензованому частотному діапазоні 2,4 ГГц [3].

Ця технологія ідеально підходить для підключення комп'ютерів, мобільних пристроїв та периферійного обладнання (наприклад, бездротових мишей, клавіатур, гарнітур). Bluetooth підтримує як з'єднання "точка-точка" (між двома пристроями), так і "точка-кілька точок" (один пристрій з кількома). Дві

або більше пристроїв, що використовують один канал, утворюють так звану пікомережу (piconet).

Для мережі ТзОВ "ЕкспертФан "ЧудоОстрів" технологія Bluetooth буде використовуватися лише для підключення індивідуальних периферійних пристроїв до робочих станцій або мобільних терміналів збору даних, але не для основної мережевої інфраструктури, оскільки її пропускна здатність та радіус дії недостатні для корпоративних потреб [3].

На відміну від Bluetooth, технологія Wi-Fi (Wireless Fidelity) широко використовується для побудови локальних бездротових мереж (WLAN). Вона регулюється набором стандартів IEEE 802.11.

Для розповсюдження радіохвиль у Wi-Fi можуть використовуватися кілька частотних діапазонів: 2,4 ГГц, 5 ГГц або 6 ГГц. Кожен діапазон має свої особливості та набір каналів [3]:

- 2,4 ГГц – використовує три непересічні канали шириною 20 МГц кожен. Цей діапазон більш схильний до перешкод через його поширеність;
- 5 ГГц – пропонує 33 канали, з яких 19 не перетинаються. Кожен канал має ширину 40 МГц. Цей діапазон забезпечує вищу швидкість та менше перешкод порівняно з 2,4 ГГц;
- 6 ГГц – найновіший діапазон (доступний зі стандартом Wi-Fi 6E), що пропонує 59 каналів різної ширини, включаючи 14 додаткових каналів шириною 80 МГц та сім шириною 160 МГц. Цей діапазон забезпечує найбільшу пропускну здатність та мінімальні перешкоди.

Важливо зазначити, що чим більше каналів і чим більша їхня ширина, тим менше буде взаємних перешкод при одночасній роботі кількох бездротових мереж у сусідніх зонах.

Для ТзОВ "ЕкспертФан "ЧудоОстрів" з урахуванням сучасних вимог до швидкості та кількості одночасних підключень, а також для забезпечення майбутнього розширення, доцільно використовувати обладнання, що підтримує стандарти IEEE 802.11ac (Wi-Fi 5). Це гарантує високу пропускну здатність для торгових операцій, відеоспостереження та інших корпоративних потреб, а також

забезпечує надійне підключення для численних мобільних пристроїв та гостьової мережі.

Ядром мережі Wi-Fi є точка доступу (Access Point). Вона зазвичай підключається до провідної мережевої інфраструктури та забезпечує передачу радіосигналу, створюючи зону Wi-Fi (або хот-спот). Точка доступу складається з приймача, передавача, інтерфейсу для підключення до дротової мережі та програмного забезпечення для обробки даних. Для підключення пристрій з бездротовим адаптером повинен знаходитися в зоні дії точки доступу. Якщо пристрій потрапляє в радіус дії кількох Wi-Fi зон, він автоматично підключається до точки доступу з найсильнішим сигналом, забезпечуючи роумінг.

Пропонується використовувати точки доступу, що підтримують обидва діапазони 2,4 ГГц та 5 ГГц, для забезпечення оптимальної продуктивності та стабільності зв'язку в умовах можливих радіоперешкод.

Для проектованої мережі ТзОВ "ЕкспертФан "ЧудоОстрів" технологія Wi-Fi (стандарти IEEE 802.11ac) буде ключовою для забезпечення бездротового доступу в центральному офісі та кожній філії. Це дозволить:

- підключення мобільних робочих місць (ноутбуки, планшети);
- використання бездротових терміналів збору даних для інвентаризації та обліку товару;
- організацію гостьової Wi-Fi мережі для відвідувачів магазинів (з відповідними заходами безпеки та ізоляцією від корпоративної мережі);
- гнучкість у розміщенні пристроїв, де прокладання кабелю є недоцільним або неможливим.

Для безпечного ізольованого з’єднання окремих магазинів-філій із центральним офісом слід використати технологію глобальних мереж (WAN) VPN (Virtual Private Network). Дана технологія є ключовою для об'єднання географічно розподілених філій. VPN створює зашифрований тунель через загальнодоступну мережу Інтернет, забезпечуючи безпечний та конфіденційний обмін даними між центральним офісом та філіями. Це набагато економічніше, ніж виділені канали зв'язку.

Для проектованої мережі ТзОВ "ЕкспертФан "ЧудоОстрів" буде використано IPsec VPN (Internet Protocol Security Virtual Private Network) у режимі "site-to-site" між маршрутизаторами центрального офісу та кожної філії. Це забезпечить надійне шифрування та автентифікацію трафіку [6].

Для доступу до VPN-з'єднань, хмарних сервісів, електронної пошти та загального доступу до Інтернету необхідне Інтернет-з'єднання. Для цього у центральному офісі та кожній філії буде забезпечено високошвидкісне широкосмугове Інтернет-з'єднання (оптичне волокно), бажано від різних провайдерів для резервування. Для центрального офісу рекомендується швидкість не менше 1-2 Гбіт/с, для філій – 1 Гбіт/с.

Отже, для проектованої корпоративної мережі ТзОВ "ЕкспертФан "ЧудоОстрів" вибрана ієрархічна топологія (Дерево/Зірка) з використанням технологій Gigabit Ethernet та Wi-Fi для LAN, а також VPN over Internet для WAN, є оптимальним рішенням для ТзОВ "ЕкспертФан "ЧудоОстрів". Такий підхід забезпечує:

- високу надійність, завдяки зіркоподібній структурі локальних мереж та можливоті резервування WAN-каналів;
- масштабованість – легкість додавання нових філій та розширення існуючих LAN;
- продуктивність – застосування Gigabit/10 Gigabit Ethernet та сучасних стандартів Wi-Fi;
- безпеку, завдяки використанню VPN для міжфілійних з'єднань, VLAN для сегментації та комплексу заходів безпеки на рівні мережевого обладнання;
- економічну ефективність, завдяки використанню загальнодоступного Інтернету для WAN-з'єднань замість дорогих виділених ліній, при цьому забезпечуючи необхідний рівень безпеки та функціональності;
- керованість, завдяки використанню керованих комутаторів та централізованого управління VPN-з'єднаннями.

Побудована повна логічна топологія проектованої мережі ТзОВ "ЕкспертФан "ЧудоОстрів" представлена на рисунку додатку Б.

2.2 Вибір кабельного середовища та розташування вузлів мережі

Вибір кабельного середовища є критично важливим для забезпечення надійності, продуктивності та довгострокової перспективи мережевої інфраструктури. Для ТзОВ "ЕкспертФан "ЧудоОстрів" буде використано комбінований підхід, що включає як мідні, так і оптоволоконні кабелі, залежно від призначення сегмента мережі та необхідної відстані передачі.

Основним типом кабелю для локальних мереж буде неекранована кручена пара (UTP) Категорії 6 (Cat 6). Цей вибір є економічно вигідним і водночас відповідає сучасним вимогам до швидкості та надійності. Кабель Cat 6 повністю підтримує стандарт Gigabit Ethernet (1000BASE-T) на відстанях до 100 метрів, що є оптимальним для всіх підключень у центральному офісі та філіях. Крім цього, Cat 6 надає кращі характеристики щодо перехресних перешкод та шуму порівняно з Cat 5e, що забезпечує запас продуктивності та можливість підтримки 10 Gigabit Ethernet на коротких дистанціях у майбутньому.

Кабель Cat 6 буде використовуватися для підключення всіх робочих станцій (комп'ютерів користувачів, касирів, адміністраторів), камер відеоспостереження та точок доступу Wi-Fi, які отримуватимуть живлення за технологією Power over Ethernet (PoE) безпосередньо через цей кабель. Також, Cat 6 буде застосований для з'єднань між мережевими комутаторами на рівні доступу та розподілу в межах одного приміщення.

Для міжфілійного зв'язку (WAN), використовуються послуги інтернет-провайдерів з організацією безпечних VPN-тунелів через загальнодоступну мережу Інтернет, що є найбільш економічно ефективним рішенням для підприємства такого типу.

За результатами всебічного аналізу технічних вимог, відповідності запитам замовника, а також з урахуванням критеріїв вартості та перспектив подальшої модернізації, для побудови локальної мережі було обрано кабель U/UTP Cat.6 4Pr виробництва «Одескабель». Цей кабель має провідники, виконані з мідного м'якого дроту діаметром 0,57 мм, що відповідає стандарту 23

AWG. Кожна жила ізольована поліетиленом, збільшуючи її загальний діаметр до 1,05 мм. Цей кабель повністю відповідає міжнародним стандартам якості та продуктивності, зокрема ISO/IEC 11801:2002, EN 50173-1:2002, ANSI/TIA/EIA-568-B.2-1-2002 та IEC 61156-5:2002 [11].

Важливим компонентом кабельної інфраструктури є конектори, що забезпечують підключення крученої пари до мережевих пристроїв. Для реалізації цього проєкту були обрані конектори ATCOM RJ45 CAT.6 UTP 8P8C, що відповідають стандарту 8P8C (RJ45). Цей вибір гарантує сумісність з кабелем Категорії 6 та високу якість з'єднання.

Для оптимізації кабельної системи та спрощення підключення кінцевих пристроїв, у всіх точках доступу передбачено встановлення мережевих розеток стандарту 8P8C (RJ45). Взаємодія між цими розетками та персональними комп'ютерами здійснюватиметься за допомогою спеціалізованих патч-кордів.

Зважаючи на широкий асортимент готових рішень на сучасному ринку, для потреб мережі ТзОВ "ЕкспертФан "ЧудоОстрів" оптимальним вибором є патч-корди довжиною 1,5 метра. Зокрема, обрано модель 2E CAT6 UTP RJ-45 26AWG, її зовнішній вигляд буде представлено на рисунку 2.1.

Рисунок 2.1 – Патч-корд 2E CAT6 UTP RJ-45 26AWG

Для забезпечення гнучкого підключення кінцевих пристроїв до стаціонарних кабельних ліній мережі, обов'язковим елементом є мережеві розетки. У межах проєкту ТзОВ "ЕкспертФан "ЧудоОстрів" було обрано зовнішню модель Cablexpert RJ45x1 UTP Cat.6 (див. рис. 2.2). Цей вибір обґрунтований високою практичністю та зручністю монтажу даної моделі. Зовнішні розетки

особливо доречні для офісних приміщень, де потрібне швидке та просте підключення обладнання без необхідності прихованої інсталяції в стіни.

Рисунок 2.2 – Мережева розетка Cablexpert RJ45x1 UTP cat.6

Використання однопортових мережевих розеток сприяє створенню не тільки організованого, але й естетично привабливого робочого простору. Їхня повна відповідність Категорії 6 забезпечує ідеальну сумісність з обраною кабельною інфраструктурою та гарантує стабільну підтримку швидкості Gigabit Ethernet.

Мережа магазинів ТзОВ "ЕкспертФан "ЧудоОстрів" розташована в чотирьох різних одноповерхових будівлях займаючи в кожній із них по одному цілому або частині поверху. План відповідних будівель (частин будівель) представлено на додатку А.

Необхідно спланувати розташування окремих вузлів у кожному із приміщень. Продумане розташування вузлів мережі є запорукою її ефективності, керованості та безпеки. Планується ієрархічна структуру з централізацією ключових ресурсів.

В центральному офісі ключовим вузлом стане серверна кімната. Це окреме, захищене приміщення з контрольованим доступом, системою кондиціонування та пожежогасіння, а також надійною системою безперебійного живлення (ДБЖ). У ній розміщуватимуться основні сервери (для ERP-системи, баз даних, файлового сховища, контролера домену, IP-АТС, системи відеоспостереження), комутатор рівня доступу для з’єднання всіх кінцевих пристроїв локальної мережі головного офісу та магазину, а також маршрутизатор/файрвол для виходу в Інтернет та налаштування VPN-тунелів до

філій. З'єднання всередині серверної та до кінцевих пристроїв у відділах буде здійснюватися за допомогою Cat 6 кабелів.

На робочих місцях у відділах (бухгалтерія, продажі, маркетинг, логістика) та у магазині кожен комп'ютер, камера відеонагляду та точка безпровідного доступу будуть підключені до комутатора доступу (Access Switch), розташованого у серверній за допомогою кабелю Cat 6. Для забезпечення бездротового доступу, точки доступу Wi-Fi будуть стратегічно розташовані по центру приміщення головного магазину та підключені до комутатора доступу з підтримкою PoE.

Кожна філія матиме свій комунікаційний вузол, що являтиме собою невелику, захищену комунікаційну шафу або бокс. У ній буде розміщено маршрутизатор/VPN-пристрій для встановлення захищеного VPN-тунелю до центрального офісу та підключення до Інтернету, а також комутатор рівня доступу філії, який розподілятиме мережу всередині магазину. Усі критично важливі пристрої будуть живитися через систему безперебійного живлення (ДБЖ).

Отже, для розміщення активного мережевого обладнання в коджному із магазинів та головному офісі необхідно вибрати комутаційну шафу.

При виборі комутаційної шафи для мережі "ЕкспертФан "ЧудоОстрів" ми керувалися наступними критеріями:

- габарити та ємність (висота в юнитах - U) – визначається кількістю та розмірами активного й пасивного обладнання, яке планується розмістити. Запас по юнитах (зазвичай 20-30%) є обов'язковим для майбутнього розширення;
- конструкція та матеріали. Міцність корпусу (зазвичай сталь), наявність перфорації для вентиляції, можливість встановлення вентиляторних блоків, тип дверей (скляні або металеві, перфоровані);
- система охолодження. Забезпечення ефективного відведення тепла є критично важливим для стабільної роботи обладнання. Це може бути пасивна вентиляція (перфорація), активна (вентиляторні блоки) або навіть системи кондиціонування для великих серверних;

- безпека. Наявність замків на дверях та бокових панелях для запобігання несанкціонованому доступу до обладнання;

- система кабельного менеджменту. Зручність прокладки та фіксації кабелів всередині шафи для підтримки порядку та полегшення обслуговування;

- ступінь захисту (IP), що залежить від місця встановлення. Для офісних приміщень може бути достатньо базового захисту, тоді як для складських або виробничих зон потрібен вищий ступінь захисту від пилу та вологи.

- виробник та вартість. Вибір надійного виробника, який пропонує оптимальне співвідношення ціни та якості.

На основі зазначених критеріїв та структури мережі, для ТзОВ "ЕкспертФан "ЧудоОстрів" передбачається використання комутаційних шаф Hypernet WMNC-9U-FLAT (див. рис. 2.3).

Рисунок 2.3 – Комутаційна шафа Hypernet WMNC-9U-FLAT

Ця шафа призначена для розміщення ключових мережевих компонентів, зокрема: патч-панелей, комутатора, кабельних організаторів та блоку безперебійного живлення (ДБЖ) APC Back-UPS Pro 1500VA. Останній забезпечить безперервну подачу електроенергії на всі мережеві вузли, захищаючи їх від можливих перебоїв у електромережі.

Для організації та кросування з'єднань у шафі використовуватиметься патч-панель Panduit 19" на 24 порти Категорії 6. Вона легко встановлюється у стандартні серверні шафи/стійки, оснащена конекторами RJ-45 і не потребує спеціальних інструментів для підключення завдяки системі автоматичного прорізання ізоляції. Ця патч-панель постачається з необхідними кріпильними

деталями та хомутами Colring, повністю відповідаючи стандарту EIA/TIA 568 B.2-1.

Усі комутаційні шафи будуть встановлені з дотриманням правил безпеки, забезпечуючи зручний доступ для обслуговування та модернізації. Всередині шаф буде організований належний кабельний менеджмент за допомогою стяжок, органайзерів та спеціальних каналів для уникнення заплутування кабелів та полегшення діагностики. Системи охолодження будуть регулярно моніторитися для запобігання перегріву обладнання.

Робочі місця у філіях, включаючи каси, робоче місце адміністратора та склад, будуть підключені до комутатора філії за допомогою кабелю Cat 6. POS-термінали, комп'ютери та IP-телефони у магазині будуть використовувати ці з'єднання для обміну даними та зв'язку з центральним офісом. Для моніторингу та безпеки, IP-камери відеоспостереження також будуть підключені до мережі (з використанням PoE) та передаватимуть дані на центральний сервер. Точки доступу Wi-Fi будуть розміщені для повного покриття торгових залів та складських приміщень, забезпечуючи бездротовий доступ для співробітників та, за потреби, для відвідувачів.

Вся кабельна інфраструктура буде побудована згідно з принципами структурованої кабельної системи (СКС) за стандартом TIA/EIA-568. Це означає використання патч-панелей, комутаційних шнурів, стандартизованих розеток RJ-45, а також обов'язкове маркування всіх кабелів та портів для легкої ідентифікації та обслуговування.

Кабелі прокладатимуться у пластикових кабель-каналах (коробах) профілем 50×35 мм, трубах або каналах, щоб забезпечити їх захист та зручність обслуговування. Буде суворо дотримуватися максимальних відстаней для Cat 6 (100 м). Обов'язковим елементом буде належне заземлення всього активного мережевого обладнання та комунікаційних шаф.

Короби монтуються вздовж стін або під плінтусами, що забезпечує естетичний вигляд приміщень та надійний захист кабельних ліній від механічних пошкоджень. У випадках, коли це дозволяють конструктивні особливості

будівлі, може бути застосована прихована прокладка кабелів (наприклад, за гіпсокартонними стінами, під фальшстелею або фальшпідлогою) для досягнення максимальної невидимості кабельних трас.

Для протягування кабелю через стінові перегородки необхідно свердлити отвори діаметром 16 мм та використовувати гофровані трубки відповідного діаметру для додаткового захисту кабелю та зручності обслуговування.

Під час монтажу необхідно суворо дотримуватися мінімальних радіусів вигину кабелів, що становить 4-8 зовнішніх діаметрів для крученої пари. Це критично важливо для запобігання пошкодженню провідників та забезпечення стабільної працездатності кабельної системи [3].

Кожен етап прокладання та підключення слід детально документувати, включаючи схеми, розташування розеток та маркування. Цей комплексний підхід до вибору кабельного середовища та розташування вузлів забезпечить створення надійної, продуктивної, безпечної та ефективно керованої мережевої інфраструктури для ТзОВ "ЕкспертФан "ЧудоОстрів".

Детальний план розміщення активного мережевого обладнання та прокладання кабельних систем представлено на додатку В.

2.3 Обґрунтування вибору комунікаційного обладнання

Проєктування локальної комп'ютерної мережі для ТзОВ "ЕкспертФан "ЧудоОстрів" вимагає ретельного підбору активного мережевого обладнання, адже воно формує основу всієї інфраструктури. Правильний вибір компонентів є ключовим для забезпечення високої продуктивності, надійності, безпеки та масштабованості системи.

Для мережі ТзОВ "ЕкспертФан "ЧудоОстрів" було обрано обладнання від провідного виробника Cisco. Це рішення гарантує корпоративний рівень якості, надійності та підтримки, що є вкрай важливим для стабільної роботи комерційного підприємства.

Відповідно до розробленої топології мережі (представленої у Додатку Б), інфраструктура ТзОВ "ЕкспертФан "ЧудоОстрів" включатиме наступне активне мережеве обладнання:

- три комутатори робочих груп – ці пристрої забезпечать підключення кінцевих користувачів та пристроїв (комп'ютерів, IP-камер відеоспостереження) у центральному офісі/магазині та філіях;

- три маршрутизатори – будуть відповідати за маршрутизацію трафіку між локальними мережами філій і центральним офісом, здійснювати маршрутизацію між віртуальними підмережами, а також за організацію безпечних VPN-тунелів через мережу Інтернет;

- шість бездротових точок доступу – забезпечать покриття Wi-Fi в торгових залах, надаючи безпровідний доступ для мобільних пристроїв, POS-терміналів та співробітників.

Комутатори робочих груп є ключовими вузлами доступу до мережі, відіграючи центральну роль у своїх сегментах. Вони збирають трафік від кінцевих пристроїв – таких як робочі станції, камери віднонагляду та інші периферійні пристрої – і направляють його до спільних ресурсів або головного комутатора чи маршрутизатора. Для мережі ТзОВ "ЕкспертФан "ЧудоОстрів" передбачено шість таких комутаторів.

Вибір цих пристроїв ґрунтується на двох основних вимогах: достатня кількість портів і відповідна пропускна здатність. Враховуючи необхідність гарантованої пропускної здатності 1 Гбіт/с для кожного користувача, всі порти комутаторів робочих груп повинні підтримувати стандарт Gigabit Ethernet. Цей стандарт забезпечує номінальну швидкість передачі даних 1 Гбіт/с на кожен порт, що є ключовим для сучасних вимог до пропускної здатності.

Для визначення необхідної кількості портів та технічних характеристик комутаторів робочих груп (рівня доступу), ми орієнтуємося на найбільший сегмент мережі. Згідно зі схемою логічної топології (представленої у додатку Б), максимальне навантаження припадає на комутатор головного офісу/магазину, до якого підключається 22 кінцеві вузли (хости). Отже, цей комутатор повинен мати

мінімум 23 порти: 22 для підключення кінцевих вузлів та 1 для висхідного (uplink) підключення до маршрутизатора.

Проте, відповідності портів стандарту Gigabit Ethernet недостатньо для ефективної обробки всього мережевого трафіку. Сам комутатор повинен мати достатню внутрішню комутаційну спроможність (switching capacity або backplane bandwidth). Цей показник відображає здатність комутатора одночасно обробляти дані, які надходять та відправляються з усіх підключених до нього портів, запобігаючи вузьким місцям і забезпечуючи повну дуплексну передачу.

Для визначення мінімально необхідної внутрішньої пропускної здатності комутатора, ми розраховуємо сумарні потреби всіх користувачів найзавантаженішого сегмента. Оскільки кожен користувач може одночасно передавати та приймати дані (повнодуплексна передача), розрахунок виконується наступним чином [2]:

$$\text{Внутрішня комутаційна спроможність} = N \times S \times 2 \qquad (2.1)$$

де: N – кількість портів комутатора, S – швидкість порту (1 Гбіт/с). Множник 2 вказує на повнодуплексний режим роботи, де передача та прийом даних можуть відбуватися одночасно.

Для сегменту з 22 вузлами внутрішня комутаційна спроможність становить:

$$22 \text{ вузли} \times 1 \text{ Гбіт/с} \times 2 = 44 \text{ Гбіт/с}$$

Для забезпечення необхідної внутрішньої комутаційної спроможності у 44 Гбіт/с, а також відповідності вимогам мережі (Gigabit Ethernet порти, підтримка PoE для точок доступу та IP-камер, керованість), вирішено вибрати комутатор Cisco Catalyst 2960L-24PS-LL, зовнішній вигляд якого представлено на рисунку 2.4.

Рисунок 2.4 – Комутатор Cisco Catalyst 2960L-24PS-LL

Обраний керований комутатор другого рівня (L2) гарантує швидке з'єднання для всіх користувачів завдяки підтримці Gigabit Ethernet на кожному порту, а також формує стабільні магістральні з'єднання через виділені аплінк-порти. Це дозволяє ефективно обробляти весь мережевий трафік без затримок.

Комутатор оснащений 24 LAN-інтерфейсами Gigabit Ethernet (RJ-45, 10/100/1000 Мбіт/с), що забезпечує високошвидкісне підключення для всіх кінцевих вузлів сегмента. Додатково, для надійного та високошвидкісного зв'язку з маршрутизатором мережі або іншими мережевими пристроями, він має чотири виділені аплінк-порти Gigabit Ethernet (SFP, 1000 Мбіт/с) для з’єднання оптоволоконним кабелем. Ці порти формують ключові магістральні з'єднання, що є критично важливим для загальної стабільності та продуктивності мережі.

З комутаційною пропускною здатністю 56 Гбіт/с, цей пристрій значно перевершує мінімальні розрахункові потреби мережі, які становлять 44 Гбіт/с. Такий запас продуктивності забезпечує високу ефективність передачі даних та запобігає перевантаженням навіть у пікові періоди. Повний перелік характеристик комутатора представлено в Таблиці 2.1.

Таблиця 2.1 – Технінчі характеристики Cisco Catalyst 2960L-24PS-LL [16]

Характеристика	Значення
Тип пристрою	Комутатор другого рівня L2
Порти LAN	24 x 10/100/1000 Мбіт/с PoE+
Порти Uplink	4 x 10G SFP+,
Пропускна здатність	56 Гбіт/с
Швидкість обробки пакетів	46,67 млн пакетів/сек
Буфер пам’яті	512 Мб
Підтримка VLAN	8192
Розмір, мм	440 x 265 x 445
Вага, кг	3,46
Підтримка PoE	IEEE 802.3af/at (PoE+)

Наступним важливим етапом у виборі активного мережевого обладнання є маршрутизатор. Він відіграє ключову роль, виступаючи шлюзом для доступу локальної мережі до Інтернету та забезпечуючи маршрутизацію трафіку між віртуальними підмережами (VLAN).

Враховуючи, що з'єднання з інтернет-провайдером буде реалізовано за допомогою оптоволокна, маршрутизатор обов'язково повинен бути оснащений оптичним SFP-слотом. Це забезпечить пряме, високошвидкісне та надійне підключення до волоконно-оптичного каналу провайдера. Важливо зазначити, що підключення комутатора робочої групи до маршрутизатора також здійснюватиметься за допомогою оптоволоконного кабелю, що підкреслює необхідність підтримки оптичних інтерфейсів на маршрутизаторі.

Ще однією ключовою вимогою до вибору моделі маршрутизатора є підтримка стеку протоколів IPSec та технології VPN для створення віртуальних захищених каналів з’єднання між магазинами-філіями і головним офісом.

З урахуванням цих вимог, було прийнято рішення обрати маршрутизатор Cisco ISR4321/K9. Його зовнішній вигляд представлений на рисунку 2.5

Рисунок 2.5 – Зовнішній вигляд маршрутизатора Cisco ISR4221/K9

Цей маршрутизатор оснащений двома SFP-портами та двома Gigabit Ethernet LAN-портами (RJ-45). Для подальшого розширення можливостей він має два додаткові слоти для інтерфейсних модулів NIM, в які ланується встановлення SFP-модулів для підключення комутатора через оптоволоконний кабель.

Маршрутизатор Cisco ISR4321/K9 вирізняється високою продуктивністю, забезпечуючи швидкість передачі даних до 10 Гбіт/с. Для ефективної роботи він обладнаний 4 ГБ оперативної пам'яті, яку можна розширити до 16 ГБ, та має 4 ГБ вбудованої флеш-пам'яті для зберігання операційних систем та конфігураційних файлів. Ключові технічних характеристик у таблиці 2.2.

Таблиця 2.2 – Технічні характеристик Cisco ISR4221/K9 [17]

Характеристика	Значення
1	2
Серія продукту	4000
Модель продукту	4321
Кількість вбудованих портів GE SFP	2
Кількість вбудованих портів RJ-45 GE	2
Кількість слотів NIM розширення	2
Розмір	43,7 x 32,2 x 25,4 мм
Вага	3,22 кг
Живлення	230 В

Цей маршрутизатор забезпечує комплексну підтримку VPN-сервісів, що є критично важливим для організації безпечного міжфілійного зв'язку. Він також підтримує широкий спектр мережевих протоколів, необхідних для гнучкої та оптимізованої маршрутизації, включаючи:

- NAT (Network Address Translation) – для ефективного використання IP-адрес та приховування внутрішньої структури мережі;
- RIP v1/v2, OSPF, EIGRP, BGP: протоколи динамічної маршрутизації, що дозволяють автоматично обмінюватися інформацією про маршрути та адаптуватися до змін у мережі;
- PBR (Policy-Based Routing) – для маршрутизації трафіку на основі заданих політик, а не лише за адресою призначення;
- PfR (Performance Routing) – для оптимізації маршрутизації на основі продуктивності мережі.

Маршрутизатор Cisco ISR4321/K9 пропонує широкі можливості для реалізації віртуальних приватних мереж (VPN), що є важливим для забезпечення безпечного зв'язку між центральним офісом ТзОВ "ЕкспертФан "ЧудоОстрів" та його філіями, а також для організації віддаленого доступу співробітників.

Цей маршрутизатор підтримує різноманітні технології VPN, які дозволяють створювати зашифровані тунелі для передачі даних через загальнодоступну мережу Інтернет. Основні типи VPN, що можуть бути реалізовані на Cisco ISR4321/K9, включають:

- IPsec VPN (IP Security VPN) – це найбільш поширений і надійний протокол для створення VPN-тунелів "сайт-до-сайту" (site-to-site) між офісами. Cisco ISR4321/K9 ефективно виконує шифрування та дешифрування IPsec-трафіку, використовуючи апаратне прискорення, що забезпечує високу пропускну здатність навіть при інтенсивному обміні даними. Це ідеально підходить для безпечного з'єднання філій в Тернополі та інших містах з центральним офісом, гарантуючи конфіденційність та цілісність даних;
- SSL VPN (Secure Sockets Layer VPN / AnyConnect VPN) – цей тип VPN дозволяє окремим користувачам (наприклад, менеджерам або IT-персоналу, які працюють віддалено) безпечно підключатися до корпоративної мережі з будь-якого місця, використовуючи стандартний веб-браузер або клієнтську програму. Це забезпечує гнучкий та безпечний віддалений доступ;
- DMVPN (Dynamic Multipoint VPN) – ця технологія дозволяє створювати масштабовані та гнучкі VPN-мережі, де кожна філія може динамічно встановлювати VPN-тунелі з будь-якою іншою філією без необхідності створення окремих статичних тунелів до центрального офісу для кожного з'єднання. Це значно спрощує управління великою кількістю філій.

Завдяки потужності маршрутизатора Cisco ISR4321/K9, він не тільки встановлює VPN-тунелі, але й обробляє VPN-шифрування, що є ключовим для підтримки високої пропускної здатності навіть при використанні сильних алгоритмів шифрування. Це означає, що безпека не буде компромісом для продуктивності мережі.

На додаток до основних функцій маршрутизації, Cisco ISR4321/K9 ефективно виконує роль міжмережевого екрана (файрволу). Це дозволяє йому контролювати мережевий трафік за допомогою списків контролю доступу (ACL).

Відповідно до проєкту, бездротовий сегмент мережі ТзОВ "ЕкспертФан "ЧудоОстрів" передбачає розгортання точок доступу TP-LINK EAP225 (див. рис. 2.6). Їх стратегічне розташування в центрі торгівельного залу, забезпечить ефективне покриття Wi-Fi.

Вибір саме цієї моделі зумовлений кількома ключовими факторами. TP-LINK EAP225 пропонує оптимальне співвідношення ціни та функціональності для потреб невеликого офісу, гарантуючи при цьому достатню продуктивність. Крім того, її конструкція забезпечує зручність встановлення як на вертикальні, так і на горизонтальні поверхні, що спрощує монтаж та інтеграцію в інтер'єр приміщення.

Рисунок 2.6 – Точка доступу TP-LINK EAP225

Цей бездротовий пристрій — високоефективна дводіапазонна точка доступу, що працює за стандартом Wi-Fi 5 (802.11ac). Вона забезпечує значну швидкість передачі даних: до 867 Мбіт/с у діапазоні 5 ГГц та 450 Мбіт/с у діапазоні 2.4 ГГц, що дозволяє обслуговувати різноманітні пристрої з різними потребами.

TP-LINK EAP225 оснащена одним Gigabit Ethernet портом (RJ45), який підтримує технологію Power over Ethernet (PoE) за стандартом 802.3af/at. Це означає, що пристрій отримує живлення безпосередньо через мережевий кабель, усуваючи потребу в окремому джерелі живлення. Це значно спрощує розміщення точки доступу та її монтаж. Завдяки своєму елегантному дизайну,

що нагадує світильник, TP-Link EAP225 легко інтегрується в будь-яке офісне середовище, дозволяючи кріпити її на стіну чи підвішувати до стелі.

EAP225 є ідеальним рішенням для середовищ з високою щільністю клієнтів, таких як офіси, готелі або комп'ютерні клуби, забезпечуючи стабільну та високу продуктивність. Вона пропонує оптимальний баланс між можливостями Wi-Fi 5, наявністю гігабітного порту та доступною ціною, що робить її економічно вигідним вибором.

Однією з ключових переваг EAP225 є підтримка аутентифікації користувачів. Це дозволяє адміністраторам ефективно контролювати доступ до бездротової мережі, забезпечуючи високий рівень безпеки даних та запобігаючи несанкціонованому підключенню.

Для забезпечення відеоспостереження у мережі ТзОВ "ЕкспертФан "ЧудоОстрів" було обрано провідну IP-камеру Reolink RLC-1224A (див. рис. 2.7). Ця модель підтримує підключення по крученій парі, що спрощує її інтеграцію в існуючу кабельну інфраструктуру.

Рисунок 2.7 – Камери відеонагляду Reolink RLC-1224A

Камера Reolink RLC-1224A вирізняється високою роздільною здатністю у 12 мегапікселів, забезпечуючи чітке та деталізоване зображення. Вона також оснащена інфрачервоним (ІЧ) підсвічуванням з дальністю до 30 метрів, що гарантує якісний моніторинг навіть у повній темряві. Додатковими перевагами цієї моделі є детекція руху та виявлення людини, що дозволяє точно фіксувати події та мінімізувати помилкові спрацьовування.

Оскільки камера підтримує підключення по крученій парі, вона, також використовує технологію Power over Ethernet (PoE). Це спрощує монтаж,

оскільки камера отримує як дані, так і живлення через один кабель Ethernet, усуваючи потребу в окремій електричній розетці поблизу камери.

На цьому процес вибору мережевого обладнання завершено

2.4 Особливості монтажу мережі

Монтаж комп'ютерної мережі для ТзОВ "ЕкспертФан "ЧудоОстрів" є ключовим етапом, що безпосередньо впливає на її продуктивність, надійність, безпеку та довговічність. Дотримання чітких правил і стандартів під час інсталяції дозволить уникнути проблем у майбутньому та забезпечити стабільну роботу всієї інфраструктури.

Перш ніж розпочати безпосередній монтаж, необхідно провести ретельне планування та підготовку:

- детальне ознайомлення з проєктною документацією – це включає схеми розташування обладнання, траси прокладки кабелів, специфікації компонентів (кабелі Cat.6, розетки, патч-панелі, комутатори, маршрутизатори, точки доступу, камери);
- оцінка умов монтажу, ідентифікація можливих перешкод (електричні кабелі, водопровідні труби), визначення оптимальних шляхів прокладки кабелів та місць встановлення комутаційних шаф та розеток;
- перевірка наявності необхідного інструментарію (кабельні тестери, обтискні кліщі, викрутки, дрилі, засоби безпеки) та комплектація всіх компонентів мережі;
- забезпечення безпечних умов праці для монтажників, використання засобів індивідуального захисту.

Горизонтальна кабельна підсистема, що використовує кабель U/UTP Cat.6, прокладається переважно у пластикових кабель-каналах (коробах) профілем 50×35 мм вздовж стін або під плінтусами. Це забезпечує естетичний вигляд та надійний захист кабелів від механічних пошкоджень та зовнішніх впливів. У місцях, де це можливо (наприклад, за гіпсокартонними стінами, під

фальшстелею/фальшпідлогою), може бути застосована прихована прокладка для досягнення максимальної невидимості трас.

При прокладанні кабелів через стінові перегородки необхідно свердлити отвори діаметром 16 мм. Кабелі в цих місцях обов'язково прокладаються в гофрованих трубках відповідного діаметру для додаткового захисту та полегшення заміни чи обслуговування в майбутньому.

Надзвичайно важливо суворо дотримуватися мінімальних радіусів вигину кабелів – для крученої пари це 4-8 зовнішніх діаметрів кабелю. Нехтування цим правилом може призвести до пошкодження провідників, погіршення цілісності сигналу та, як наслідок, зниження продуктивності або повної відмови сегмента мережі.

Кабелі слід прокладати на максимально можливій відстані від джерел електромагнітних завад, щоб мінімізувати вплив шуму та перешкод на якість передачі даних.

У центральному офісі та філіях встановлюються настінні комутаційні шафи, які забезпечують організоване та захищене розміщення активного та пасивного обладнання. Всередині шаф необхідно організувати ефективний кабельний менеджмент за допомогою стяжок, органайзерів та спеціальних каналів, щоб уникнути сплутування кабелів та полегшити подальше обслуговування. У шафі організовано розміщується наступне обладнання:

- маршрутизатор Cisco ISR4221/K9;
- комутатор рівня доступу Cisco Catalyst 3560CX-12XPD-S;
- комутатор Комутатор Cisco Catalyst 2960L-24PS-LL;
- блок безперебійного живлення APC Back-UPS Pro 1500VA;
- патч-панель Panduit 19" на 24 порти, Категорії 6.
- кабельні організатори для упорядкування кабелів.

У всіх точках підключення кінцевих пристроїв (робочі станції, POS-термінали, IP-телефони) встановлюються однопортові мережеві розетки стандарту 8P8C (RJ45) Категорії 6. Вибір зовнішніх моделей (як-от Cablexpert RJ45x1 UTP Cat.6) спрощує монтаж, особливо в офісних приміщеннях.

Для запобігання електромагнітним наведенням та забезпечення стабільності мережевого сигналу, кабелі даних прокладаються окремо від силових ліній електроживлення.

Кабелі до безпровідних точок доступу проколадається над підвісною стелею у гофрованих трубках діаметру 16 мм.

Монтаж точки доступу TP-LINK EAP225 значно спрощується завдяки підтримці технології Power over Ethernet (PoE) стандарту 802.3af/at. Це дозволяє живити пристрій безпосередньо через мережевий кабель, виключаючи потребу в прокладанні окремих силових кабелів. Точки доступу буде розміщено таким чином, щоб забезпечити оптимальне Wi-Fi покриття у торговельному залі.

Для забезпечення безпеки та відповідності стандартам, усі металеві елементи комутаційної шафи та мережевого обладнання підлягають обов'язковому заземленню.

Додатково, встановлення ДБЖ APC Back-UPS Pro 1500VA гарантує безперебійну подачу живлення на маршрутизатор, головний комутатор та інші критично важливі компоненти в серверній, надійно захищаючи їх від перебоїв в електромережі.

2.5 Обґрунтування вибору програмного забезпечення

Вибір програмного забезпечення є не менш важливим етапом, ніж підбір апаратного забезпечення, адже саме воно визначає функціональність, ефективність, безпеку та зручність використання мережі ТзОВ "ЕкспертФан "ЧудоОстрів".

Для робочих станцій потрібно вибрати операційну систему із вирахо-вуванням підтримки ОС спеціалізованого прикладного програмного забезпечення, яке використовується в роботі співробітники сітки магазинів ТзОВ "ЕкспертФан "ЧудоОстрів", а саме автоматизовану систему управляння магазином, розроблену на основі СКБД MySQL та АСУП “Парус”. Дана система

працює на платформі Windows, тому цей критерій є основним у виборі операційної системи для робочих станцій мережі.

Ще одним критерієм вибору ОС клієнтських хостів є рівень кваліфікації співробітників у використанні відповідної платформи. Кількість працівників, які мають навики роботи у Windows значно переважають інші платформи.

Отже, для робочих станцій та офісних комп'ютерів ТзОВ "ЕкспертФан "ЧудоОстрів" рекомендується використання ліцензійних версій операційних систем Microsoft Windows 10/11 Professional, які мають наступні переваги:

- стабільність та надійність – це перевірені часом платформи, які забезпечують високий рівень стабільності та мінімізують збої в роботі;
- сумісність. Windows має широку підтримку програмного забезпечення та периферійних пристроїв, що є критично важливим для офісних завдань;
- безпека. Професійні версії Windows пропонують розширені функції безпеки, такі як BitLocker для шифрування дисків, Windows Defender для захисту від шкідливого ПЗ, а також можливість інтеграції в домен Active Directory для централізованого управління користувачами та політиками безпеки;
- зручність використання. Інтерфейс Windows є звичним для більшості користувачів, що мінімізує час на навчання та адаптацію.

Для керування IP-камерою Reolink RLC-1224A та зберігання відеозаписів буде використовуватися відповідне програмне забезпечення:

- Reolink Client/NVR Software – безкоштовне програмне забезпечення від Reolink, яке дозволяє переглядати відеопотік, керувати записами та налаштуваннями камери. Це простий варіант для базового моніторингу;
- стороннє VMS з підтримкою ONVIF. Для більш розширених можливостей (наприклад, інтеграції кількох камер різних виробників, розширеного відеоаналізу, централізованого зберігання) може бути розглянуто комерційне VMS, що підтримує стандарт ONVIF (Open Network Video Interface Forum), який підтримує Reolink RLC-1224A. Приклади таких систем: Milestone XProtect Essential+, Genetec Security Center (для великих систем), або Nx Witness.

Для центрального сервера ТзОВ "ЕкспертФан "ЧудоОстрів" пропонується використовувати Microsoft Windows Server 2022 версії.

Windows Server дозволяє розгорнути контролер домену Active Directory, що є основою для централізованого керування користувачами, комп'ютерами, групами безпеки, мережевими ресурсами та застосуванням єдиних політик.

Дана операційна система є надійною платформою для розгортання файлових ресурсів з гнучким керуванням доступом та можливістю налаштування квот.

Windows Server є масштабованою платформою, яка може зростати разом з потребами компанії. Забезпечує бездоганну інтеграцію з Microsoft Office та іншими корпоративними рішеннями.

2.6 Визначення функцій серверів

У структурі інформаційної системи ТзОВ "ЕкспертФан "ЧудоОстрів", сервери відіграють центральну роль, забезпечуючи функціонування критично важливих мережевих сервісів. Їхнє правильне налаштування та розподіл функцій гарантують ефективність, безпеку та надійність роботи всієї IT-інфраструктури.

Для потреб даної мережі передбачається розгортання одного фізичного сервера, який буде виконувати кілька ключових ролей, консолідуючи функціонал для оптимізації ресурсів та спрощення управління. Основні функції цього сервера включатимуть:

- контролер домену (Active Directory Domain Controller);
- файловий сервер;
- DHCP-сервер;
- сервер відеоспостереження (Video Management Software - VMS);
- сервер додатків.

Сервер виконуватиме роль контролера домену Active Directory. Це є основою для централізованого управління мережею, що дозволяє забезпечити:

- єдину аутентифікацію та авторизацію. Керування обліковими записами користувачів та комп'ютерів, що дозволяє їм безпечно входити в мережу та отримувати доступ до ресурсів;

- групові політики (Group Policy) безпеки. Централізоване застосування правил та налаштувань безпеки для всіх користувачів та комп'ютерів у домені, що забезпечує єдність конфігурації та високий рівень контролю;

- управління ресурсами – спрощене надання доступу до спільних папок, принтерів та інших мережевих ресурсів;

- масштабованість – можливість легкого додавання нових користувачів, комп'ютерів та філій у майбутньому.

Файловий сервер буде функціонувати як централізоване сховище даних для всіх співробітників ТзОВ "ЕкспертФан "ЧудоОстрів". Це забезпечить:

- централізоване зберігання – усі робочі документи, проєкти, бази даних та інші важливі файли будуть зберігатися на сервері, що усуває розрізненість даних на окремих робочих станціях;

- налаштування прав доступу до файлів та папок на основі ролей та груп користувачів, гарантуючи конфіденційність та цілісність інформації;

- спрощене централізоване резервне копіювання всіх критично важливих даних, що мінімізує ризики їх втрати внаслідок збоїв або непередбачених ситуацій;

- можливість легкого обміну файлами між співробітниками та відділами.

На сервері також буде розміщено програмне забезпечення для керування відеоспостереженням (VMS). Це забезпечить:

- безперервний запис відеопотоку з IP-камер Reolink RLC-1224A (та інших, якщо їх буде додано) та зберігання його на дисковій підсистемі сервера;

- можливість віддаленого доступу до архіву відео та перегляду відеопотоку в реальному часі для контролю безпеки;

- налаштування реакцій на події (наприклад, детекція руху, виявлення людини) та сповіщень.

Вибір Microsoft SQL Server як сервера баз даних для ТзОВ "ЕкспертФан "ЧудоОстрів" забезпечить міцну, надійну та масштабовану основу для зберігання та управління вашими корпоративними даними. Це рішення пропонує низку ключових переваг, які є критично важливими для сучасного бізнесу.

Для бездротових точок доступу (ТД) та підключених до них клієнтів (ноутбуків, смартфонів, планшетів) в мережі ТзОВ "ЕкспертФан "ЧудоОстрів" необхідно забезпечити функціонування DHCP-сервера (Dynamic Host Configuration Protocol). Його основне завдання – автоматична видача IP-адрес та інших мережевих налаштувань (маска підмережі, шлюз за замовчуванням, DNS-сервери) пристроям, що підключаються до бездротової мережі.

У випадку проектованої мережі, де вже передбачено сервер під керуванням Microsoft Windows Server з роллю контролера домену Active Directory, найбільш логічним та ефективним рішенням є розгортання на ньому ролі DHCP-сервера.

Крім вже згаданих функцій, сервер ТзОВ "ЕкспертФан "ЧудоОстрів" також може виконувати роль сервера для CRM-системи (Customer Relationship Management). Впровадження CRM-системи є стратегічно важливим для бізнесу, що орієнтований на клієнтів, оскільки вона дозволяє автоматизувати взаємодію з клієнтами, оптимізувати продажі, маркетинг та обслуговування.

Функції сервера CRM-системи:

- централізоване зберігання даних про клієнтів. Сервер буде зберігати всю інформацію про клієнтів, включаючи контактні дані, історію покупок, взаємодії, листування, запити та угоди. Це забезпечує єдиний доступ до даних для всіх відповідних відділів;
- управління продажами. CRM-система дозволяє автоматизувати етапи продажів, від першого контакту до закриття угоди. Сервер підтримує функціонал для відстеження потенційних клієнтів (лідів), управління угодами, прогнозування продажів та формування звітів;
- автоматизація маркетингу. Можливість проведення цільових маркетингових кампаній, розсилок, сегментації клієнтської бази та аналізу ефективності маркетингових активностей;
- підтримка та обслуговування клієнтів. Сервер забезпечує платформу для управління зверненнями клієнтів, відстеження статусів запитів, ведення історії звернень та підвищення якості обслуговування;

- інтеграція з іншими системами. Часто CRM-системи інтегруються з іншими бізнес-додатками, такими як поштові клієнти, ERP-системи, системи обліку, телефонія. Сервер забезпечує необхідні ресурси та доступ для цих інтеграцій;

- звіти та аналітика. Збір та обробка даних для формування різноманітних звітів щодо продажів, ефективності кампаній, задоволеності клієнтів, що є основою для прийняття управлінських рішень.

2.7 Розподіл адресного простору мережевих вузлів

Для ефективної та безпечної адресації пристроїв у корпоративній мережі ТзОВ "ЕкспертФан "ЧудоОстрів" вирішено використовувати приватний адресний простір IPv4 класу C – мережу 192.168.0.0/24. Цей вибір є оптимальним, адже він забезпечує до 254 унікальних IP-адрес, що з великим запасом покриває поточні потреби мережі. Наразі мережа налічує 56 провідних та 28 бездротових кінцевих пристроїв, що становить 84 мережевих адреси.

Для подальшої логічної сегментації, покращення безпеки та оптимізації трафіку, мережу підприємства розділено на десять віртуальних підмереж (VLAN). Ця сегментація виконана відповідно до складу структурних підрозділів мережі магазинів:

- Dir – окрема підмережа керівника ТзОВ "ЕкспертФан "ЧудоОстрів". В підмережу включено лише один пристрій;
- Bug – бухгалтерія ТзОВ "ЕкспертФан "ЧудоОстрів" із 2 комп’ютерів;
- Log – відділ логістики із 2 ПК;
- Man – відділ менеджменту та маркетингу 2 робочих станцій;
- Mag1 – пристрої магазину філії №1, куди входять 1 ПК головного менеджера магазину, 1ПК завідувача складом, 1 ПК у кімнаті працівників. 2 ПК на касах та 2 ПК консультантів. Разом 7 робочих станцій. Крім цього в підмережі потрібно виділити 2 адреси для POS-терміналів та 4 для мобільних планшетів

консультантів в торговому залі. Всього в підмережі необхідно зарезервувати 13 IP-адрес кінцевих вузлів;

- Mag2 – пристрої магазину філії №2, куди входять 1 комп'ютер головного менеджера магазину, 1 – завідувача складом, 1 – у кімнаті працівників. 2 робочих станції на касах та 2 ПК консультантів. Разом 7 вузлів. Крім цього в підмережі потрібно виділити 2 адреси для POS-терміналів та 4 для мобільних планшетів консультантів в торговому залі. Всього в підмережі необхідно зарезервувати 13 IP-адрес;

- Mag3 – пристрої магазину філії №3, куди входять 1 ПК головного менеджера магазину, 1 ПК завідувача складом, 1 – у кімнаті працівників. 2 комп'ютери на касах та 2 ПК консультантів. Разом 7 адрес для кінцевих вузлів. Також в підмережі потрібно виділити 2 адреси для POS-терміналів та 4 для мобільних планшетів консультантів в торговому залі. Отже, разом в підмережі магазину №3 необхідно зарезервувати 13 IP-адрес;

- Mag4 – пристрої магазину в головному офісі, куди входять 1 ПК завідувача складом, 1 ПК у кімнаті працівників. 3 ПК на касах та 2 ПК консультантів. Разом 7 робочих станцій. Крім цього в підмережі потрібно виділити 2 адреси для POS-терміналів та 4 для мобільних планшетів консультантів в торговому залі. Всього в підмережі необхідно зарезервувати 13 IP-адрес кінцевих вузлів;

- Cam – підмережа камер відеоспостереження включає 1 ПК оператора відеоспостереження та 13 IP-камер відеоспотсереження;

- Serv– підмережа сервера корпоративної мережі. Складається лише з одного кінцевого вузла.

Під час виділення діапазонів IP-адрес важливо пам'ятати, що кожна підмережа потребуватиме додаткової IP-адреси для мережевого шлюзу. Ця адреса буде призначена віртуальному інтерфейсу головного комутатора. Отже загальна кількість необхідних IP-адрес для кожної підмережі, враховуючи додаткову адресу шлюзу представлена у таблиці 2.3.

Таблиця 2.3 – Розподіл кількості IP-адрес по VLAN

Назва	Dir	Bug	Log	Man	Mag1	Mag2	Mag3	MagG	Cam	Serv
К-сть IP-адрес	2	3	3	3	14	14	14	14	13	2

Для ефективного та раціонального використання IP-адресного простору мережі ТзОВ "ЕкспертФан "ЧудоОстрів" обрано метод маски змінної довжини (VLSM - Variable Length Subnet Masking). На відміну від традиційного поділу на підмережі (FLSM), VLSM дозволяє асигнувати підмережам маски різної довжини, точно відповідаючи їхнім потребам у кількості IP-адрес. Такий підхід запобігає марнуванню великих блоків адрес для малих підмереж, оптимізує маршрутизацію (дозволяючи агрегацію маршрутів) та підвищує загальну гнучкість мережевого планування.

Ми використовуємо приватний IP-діапазон 192.168.0.0/24, який надає 256 адрес для розподілу. Для кожної віртуальної підмережі необхідно виділити:

- достатню кількість IP-адрес для робочих станцій та інших пристроїв;
- одну додаткову IP-адресу для мережевого шлюзу. Ця адреса буде призначена віртуальному інтерфейсу (SVI - Switched Virtual Interface) головного комутатора, що забезпечуватиме маршрутизацію між VLAN-ами.

З метою запобігання фрагментації адресного простору та забезпечення ефективного розподілу підмереж, насамперед слід відсортувати список підрозділів за спаданням кількості необхідних IP-адрес (включно зі шлюзом). Це дасть змогу оптимально використовувати залишки від виділення великих блоків

Визначення маски підмережі для кожного сегмента базується на знаходженні найменшого цілого числа n, такого, що 2^n буде більшим або рівним необхідній кількості адрес (включаючи мережеву та широкомовну). Після цього довжина маски CIDR розраховується за формулою $32 - n$, де n представляє кількість бітів, відведених для адресації хостів.

Кожен з чотирьох магазинів потребує 14 IP-адрес. Для цього, потрібно маску, яка надає 16 доступних адрес, проте такий діапазон не забезпечує масштабованість мережі в майбутньому. Якщо виникне необхідність розширити мережу

магазину новим кінцевим вузлом такий розподіл не дозволить це зробити. Тому вирішено для дотримання принципу масштабування мережі вибрати маску із 32 доступних адрес, що забезпечить невеликий запас для майбутнього розширення.

Отже, для хостів магазинів слід виділити п’ять бітів, виходячи із математичної залежності $2^5=32$, а для адрес підмереж задишиться 3 біти (всього в октеті 8 біт). Тобто макса підмереж магазинів буде:

11111111.11111111.11111111.11100000,

або в десятковому записі числа: 255.255.255.255.224

Отже, адресу підмережі вузлів в магазині головного офісу MagG можна записати у вигляді 192.168.0.0/27. В таблиці 2.4 представлено інформацію про IP-адресу підмережі MagG, діапазон допустимих адрес для вузлів та бродкест.

Таблиця 2.4 – Розрахунок адресного простору для підмереж

Назва підм.	Необх. к-сть адрес	Обчислення останнього октету	Дост к-ть адрес	Адреса підмережі	Діапазон адрес для вузлів	Широкосму-гова адреса
1	2	3	4	5	6	7
MagG	14	256-32=224	30	192.168.0.0/27	192.168.0.1 – 192.168.0.30	192.168.0.31
Mag1	14	256-32=224	30	192.168.0.32/27	192.168.0.33 –192.168.0.62	192.168.0.63
Mag2	14	256-32=224	30	192.168.0.64/27	192.168.0.65 –192.168.0.94	192.168.0.95
Mag3	14	256-32=224	30	192.168.0.96/27	192.168.0.97 – 192.168.0.126	192.168.0.127
Cam	13	256-32=224	30	192.168.0.128/27	192.168.0.129 – 192.168.0.158	192.168.0.159
Bug	3	256-8=248	6	192.168.0.160 /29	192.168.0.161– 192.168.0.166	192.168.0.167
Log	3	256-8=248	6	192.168.0.168 /29	192.168.0.169– 192.168.0.174	192.168.0.175
Man	3	256-8=248	6	192.168.0.176 /29	192.168.0.177– 192.168.0.182	192.168.0.183
Dir	2	256-4=252	2	192.168.0.184 /30	192.168.0.185– 192.168.0.186	192.168.0.187
Serv	2	256-4=252	2	192.168.0.188 /30	192.168.1.189– 192.168.1.190	192.168.0.191

Для наступної підмережі магазину №1 буде використано наступну вільну адресу після бродкесту попередньої підмережі MagG, тобто 192.168.0.32. Для цієї мережі із вищеописаних міркувань теж буде виділено адресний простір із 30 адрес та маска 255.255.255.255.224. Як бачимо із таблиці 2.4 наступна після останньої адреси діапазону допустимих адрес буде адреса бродкесту 192.168.0.63.

Отже, після неї буде адреса наступної мережі магазину Mag2 – 192.168.0.64/27. Так само для цієї мережі буде виділено адресний простір із 30 адрес та маска 255.255.255.255.224. Як бачимо із таблиці 2.4 наступна після останньої адреси діапазону допустимих адрес буде бродкест 192.168.0.95.

Наступна адреса після бродкесту буде адресою підмережі Mag3. Це буде адреса 192.168.0.96/27. Вона теж містить адресний простір із 30 адрес від 192.168.0.97 до 192.168.0.126, а її бродкест відповідно буде 192.168.0.127.

За подібним принципом розподіляємо адресний простір всіх решту підмереж. Всі результати розподілу представлено у таблиці 2.4.

Для кожної підмережі також необхідно призначити адресу мережевого шлюзу. Шлюз мережі (Gateway) є компонентом будь-якої комп'ютерної мережі, що відіграє важливу роль у маршрутизації трафіку та забезпеченні зв'язку між різними мережами. У контексті мережі ТзОВ "ЕкспертФан "ЧудоОстрів" шлюз забезпечує як внутрішню, так і зовнішню комунікацію.

Шлюз є точкою виходу та входу для мережевого трафіку, що прямує з однієї мережі в іншу, або до мережі Інтернет. Коли пристрій (наприклад, робоча станція або сервер) намагається відправити дані на IP-адресу, яка не належить до його поточної локальної підмережі, він направляє цей трафік на свій шлюз за замовчуванням (Default Gateway). Шлюз, у свою чергу, відповідає за маршрутизацію цих даних до кінцевого пункту призначення.

Для зручності розподілу пропонується виділити останню адресу кожного діапазону адресного простору як шлюз цієї підмережу. Відповдіно адресний простір для кінцевих вузлів буде зменшено на одну адресу. В таблиці 2.5 представлено адреси шлюзів кожної VLAN.

Таблиця 2.5 – Адресний простір віртуальних підмереж та їх шлюзи

Підмережа	Адреса мережі	Діапазон хостів	Адреса шлюзу
MagG	192.168.0.0/27	192.168.0.1 – 192.168.0.29	192.168.0.30
Mag1	192.168.0.32/27	192.168.0.33 – 192.168.0.61	192.168.0.62
Mag2	192.168.0.64/27	192.168.0.65 – 192.168.0.93	192.168.0.94
Mag3	192.168.0.96/27	192.168.0.97 – 192.168.0.125	192.168.0.126
Cam	192.168.0.128/27	192.168.0.129 – 192.168.0.157	192.168.0.158
Bug	192.168.0.160/29	192.168.0.161–192.168.0.165	192.168.0.166
Log	192.168.0.168/29	192.168.0.169–192.168.0.173	192.168.0.174
Man	192.168.0.176/29	192.168.0.177 –192.168.0.181	192.168.0.182
Dir	192.168.0.184/30	192.168.0.185 – 192.168.0.186	192.168.0.187
Serv	192.168.0.188/30	192.168.0.189 – 192.168.0.190	192.168.0.191

Кожна підмережа має власний унікальний IP-діапазон та шлюз, призначений віртуальному інтерфейсу головного комутатора, який забезпечує між-VLAN маршрутизацію. Після розподілу адрес для 10 підмереж, робочий простір займає діапазон до 192.168.0.190. Це дозволяє зберегти вільні 64 IP-адреси (192.168.0.192–192.168.0.255).

Для з’єднання підмереж окремих віддалених магазинів ТзОВ "ЕкспертФан "ЧудоОстрів" буде використано VPN-тунелі через загальнодоступні ресурси Інтрнет. При цьому необхідно створити три VPN-мережі між магазинами №1, №2 та №3 та головним офісом:

- VPN1 – тунель між маршрутизатором R1 магазину №1 та маршрутизатором RG головного офісу (див. додаток Б);
- VPN2 – тунель між маршрутизатором R2 магазину №2 та маршрутизатором RG головного офісу (див. додаток Б);
- VPN3 – тунель між маршрутизатором R2 магазину №2 та маршрутизатором RG головного офісу (див. додаток Б).

Відповідно для підмереж VPN-тунелів теж необхідно виділити адресний простір. З'єднання VPN-тунелі здійснюється за принципом "точка-точка", тому для кожного VPN необхідно виділити по дві IP-адреси:

перша – віддаленого клієнта. Фізично встановлюється на маршрутизаторі віддаленого магазину;

друга – віддаленого сервера. Фізично встановлюється на маршрутизаторі головного офісу;

Для реалізації подібного адресного простору необхідно із останнього октету адреси виділити 2 біти на адресацію хостів – 2^2-2=2 IP-адреси.

Отже, на маску підмережі виділяється 32-2=30 бітів. Відповідно маска буде 255.255.255.252. Адресацію VPN-тунелів представлено в таблиці 2.6.

Таблиця 2.6 – Адресація VPN-тунелів мережі

Назва VPN	Номер віддаленого магазину	IP-адреса підмережі	IP-адреса на клієнтському маршрутизаторі	IP-адреса на маршрутизаторі RG
VPN1	Магазин №1	192.168.0.192/30	192.168.0.193	192.168.0.194
VPN2	Магазин №2	192.168.0.196/30	192.168.0.197	192.168.0.198
VPN3	Магазин №3	192.168.0.200/30	192.168.0.201	192.168.0.202

Після цього розподілу, робочий простір займає діапазон до 192.168.0.203. Це дозволяє зберегти вільні 52 IP-адреси (192.168.1.204–192.168.10.255).

Оскільки, для Wi-Fi підмережі достатньо буде виділити 20 динамічно змінюваних адрес, то найменший блок, що вміщує ці адреси – 32. Кількість бітів для хостів = 5. Маска: 32−5=/32.

Отже, адреса гостьової Wi-Fi-мережі буде 192.168.0.204/27. В діапазон цієї підмережі входить 30 адрес від 192.168.0.205 до 192.168.0.233. Наступна адреса 192.168.1.235 буде бродкестом цієї підмережі. Шлюзом цієї підмережі буде адреса 192.168.0.234.

2.8 Тестування та налагодження мережі

Після завершення монтажу активного та пасивного мережевого обладнання, критично важливим етапом є тестування та налагодження мережі. Цей процес забезпечує, що всі компоненти системи працюють коректно, відповідають проєктним вимогам та забезпечують необхідний рівень продуктивності, надійності та безпеки для ТзОВ "ЕкспертФан "ЧудоОстрів".

Етапи тестування та налагодження включають:

- тестування кабельної інфраструктури;
- початкове налаштування активного обладнання;
- налаштування серверів та сервісів;
- тестування функціональності та продуктивності;
- документування та резервне копіювання.

Тестування кабельної інфраструктури включає:

- перевірка фізичного з'єднання. Використання кабельних тестерів для перевірки цілісності кожного кабельного сегмента. Це дозволяє виявити обриви, короткі замикання, перехресне підключення пар (crossover) або неправильну розкладку жил (розводку по стандартах T568A/B);
- сертифікація кабельної системи. Для важливих сегментів Cat.6 рекомендується використання професійних сертифікаційних тестерів (наприклад, Fluke Networks), які вимірюють такі параметри, як загасання, перехресні наведення (NEXT, FEXT), зворотні втрати, затримку поширення сигналу та інші. Це підтверджує відповідність кабельної системи стандартам Cat.6 та її здатність підтримувати гігабітні швидкості;
- тестування оптичних ліній (для аплінків та WAN). Для оптоволоконних з'єднань проводяться вимірювання рівня потужності сигналу (дБм) за допомогою вимірювача оптичної потужності (OPM) та, за потреби, використання оптичного рефлектометра (OTDR) для виявлення дефектів та точної довжини лінії.

Початкове налаштування активного обладнання включає налаштуування комутаторів та маршрутизаторів.

Налаштування комутаторів включає:

- базове налаштування, таке як локальні паролі, IP-адреси управління (VLAN Interface), таймзона;

- призначення портів доступу (Access Ports) відповідним VLANs для підключення кінцевих пристроїв;

- налаштування транкових портів (Trunk Ports). Конфігурація портів, що з'єднують комутатори з маршрутизатором, для передачі трафіку всіх VLANs за протоколом 802.1Q.

Тестування функціональності та продуктивності:

- перевірка можливості доступу до шлюзів, DNS-серверів, інших пристроїв у своїй та сусідніх підмережах, а також до зовнішніх ресурсів із використанням команд ping та tracert.

- перевірка доступу до спільних папок, принтерів, CRM-системи, Інтернету з різних робочих станцій;

- перевірка якості сигналу та швидкості підключення в різних частинах офісу для Wi-Fi;

- перевірка встановлення та стабільності IPsec VPN-тунелів між магазинами;

- вимірювання пропускної здатності між ключовими вузлами мережі за допомогою спеціалізованих інструментів (наприклад, iPerf) для підтвердження відповідності проєктним швидкостям;

- перевірка функціональності міжмережевого екрана (ACLs) на маршрутизаторі, коректності роботи VPN, антивірусного захисту.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування сервера мережі

Для ефективного керування обліковими записами користувачів у мережі ТзОВ "ЕкспертФан "ЧудоОстрів" буде впроваджена доменна структура на основі служб Active Directory. Це вимагає розгортання доменного контролера на сервері з операційною системою Microsoft Windows Server 2022. Адміністрування цього сервера буде виконуватися за допомогою інтегрованого інструменту Server Manager (див. рис. 3.1).

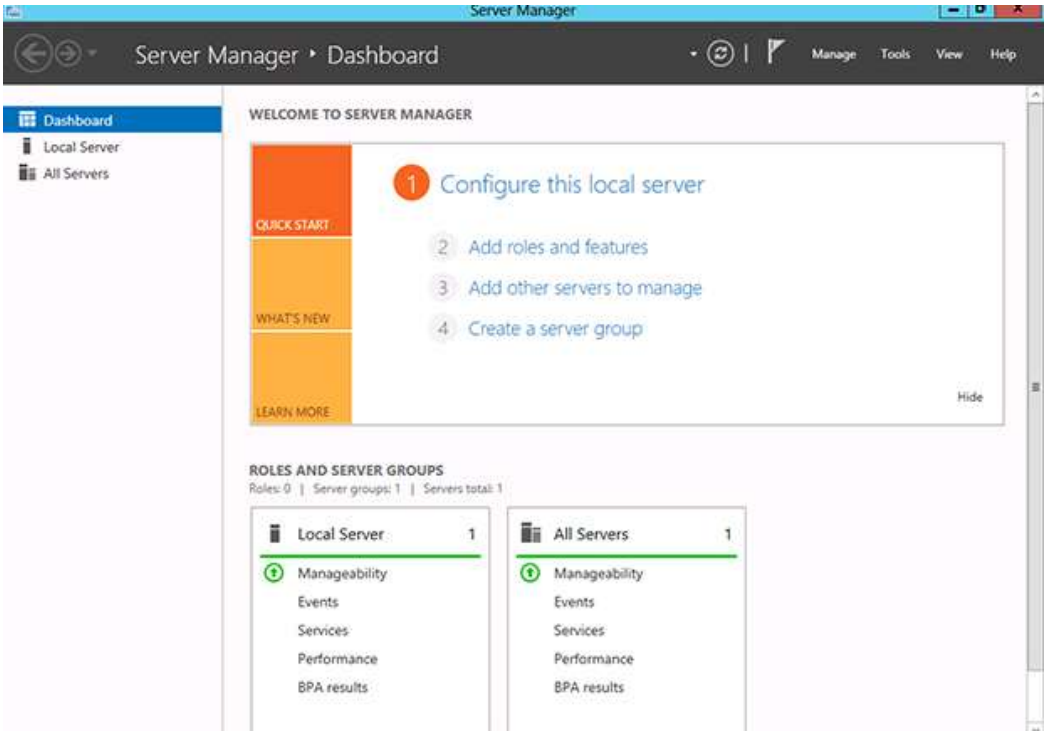


Рисунок 3.1 – Вікно Server Manger

Перед розгортанням служб каталогів Active Directory (AD DS) необхідно виконати ряд підготовчих налаштувань на сервері під керуванням Microsoft Windows Server 2022. Ці кроки забезпечують коректну роботу доменного контролера та його інтеграцію в мережеву інфраструктуру:

- серверу слід присвоїти статичну IP-адресу 192.168.0.189 згідно з планом IP-адрес, представленим в таблиці 2.4;

- в якості основного DNS-сервера вказати IP-адресу самого сервера (127.0.0.1 - Loopback). Це дозволить серверу реєструвати власні записи DNS та забезпечувати функціонування Active Directory Domain Services;

- сервер перейменувати на Serv відповідно до проєктної документації, що спрощує його ідентифікацію в мережі.

Для конфігурації мережевих параметрів сервера слід виконати такі дії:

- у лівій панелі навігації Server Manager (див. рис. 3.1) обрати пункт Local Server;

- у розділі Properties знайти параметр Ethernet та натиснути на посилання поруч з назвою мережевої карти. Це дія відкриє вікно Network Connections;

- у вікні "Network Connections" знайти та клацнути правою кнопкою миші на мережевому адаптері, який підлягає налаштуванню, після чого обрати Properties;

- у діалоговому вікні властивостей мережевого адаптера, у списку компонентів, знайти і виберіть Internet Protocol Version 4 (TCP/IPv4), потім натиснути кнопку Properties;

- у вікні, що відкриється, введіть дані згідно з планом IP-адрес із таблиці 2.4:

  - IP address – 192.168.0.189 (статична IP-адреса сервера);
  - Subnet mask – 255.255.255.252 (маска підмережі);
  - Default gateway – 192.168.0.190 (IP-адреса шлюзу за замовчуванням).
  - Preferred DNS server – 127.0.0.1 (Loopback-адреса, що вказує на сам комп'ютер, оскільки цей сервер буде виконувати функції DNS-сервера для домену Active Directory);
  - Alternate DNS server – 8.8.8.8 (альтернативний публічний DNS-сервер, який використовуватиметься для розв'язання імен в Інтернеті та як резервний, якщо локальний DNS тимчасово недоступний).

Після виконання початкових налаштувань сервера можна перейти до встановлення необхідних ролей DNS-сервера та Active Directory Domain Services

(AD DS). Цей процес здійснюється за допомогою "Майстра додавання ролей та компонентів" у Server Manager. Для цього необхідно виконати наступні кроки:

- у Server Manager (див. рис. 3.1) обрати меню "Manage", а потім пункт Add Roles and Features;
- завантажиться "Майстер додавання ролей та компонентів". На першому кроці Майстра натиснути Next;
- на кроці Installation Type обрати опцію Role-based or feature-based installation і продовжити, натиснувши Next;
- у вікні Server Selection переконатися, що вибрано поточний сервер, і натиснути Next;
- на наступному екрані, у розділі Server Roles, встановити опції DNS Server та Active Directory Domain Services;
- після вибору Active Directory Domain Services з'явиться діалогове вікно Add Features, що пропонує додати необхідні компоненти для AD DS. Підтвердити вибір, натиснувши Add Features;
- у вікні Features натиснути Next;
- на етапі AD DS (Active Directory Domain Services) ознайомитися з представленою інформацією та натиснути Next;
- у вікні Confirmation натиснути Install. Також можна встановити опцію Restart the destination server automatically if required, хоча автоматичне перезавантаження зазвичай потрібне лише після підвищення сервера до доменного контролера.

Після успішного завершення встановлення ролі AD DS у Server Manager з'явиться посилання Promote this server to a domain controller (або відповідне сповіщення у жовтому трикутнику). Необхідно клацнути на це посилання, щоб запустити Майстер конфігурації доменних служб (див. рисунок 3.2), який завершить процес створення домену та підвищення сервера до ролі контролера домену.

Запускається Майстер підвищення ролі сервера до доменного контролера, який вимагає виконання наступних кроків конфігурації:

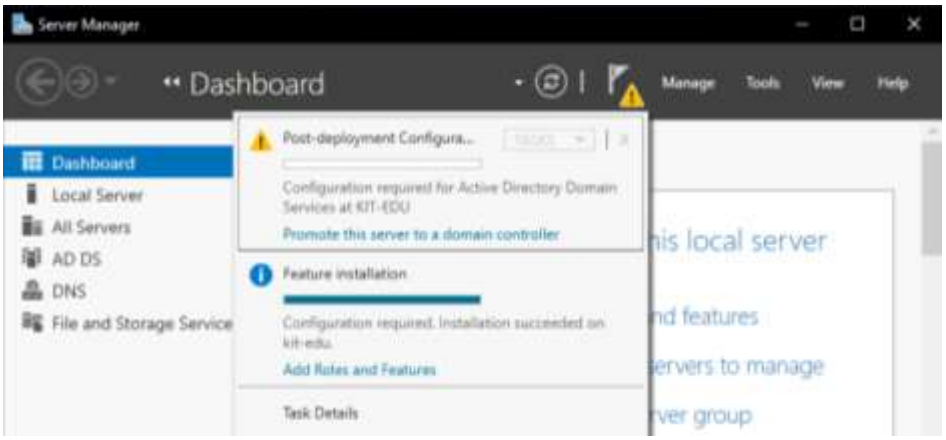


Рисунок 3.2 – Підвищення ролі сервера до доменного контролера

- у першому вікні Майстра необхідно обрати опцію Add a new forest. Потім вказати Root domain name – повне доменне ім'я (FQDN) для нового домену. У даному випадку використовується chudoostriv.local, що є поширеним вибором для внутрішніх мереж. Підтвердити вибір, натиснувши Next;

- у наступному вікні слід визначте параметри доменного контролера, такі як рівень функціональності (Functional Level) лісу/домену. В цьому випадку слід обрати найвищий рівень функціональності, який буде сумісний з усіма майбутніми доменними контролерами та клієнтами. Рекомендується Windows Server 2016 або 2022;

- у наступному вікні слід відмітити опції Domain Name System (DNS) server та Global Catalog (GC). Опцію Read-only domain controller (RODC) не потрібно встановлювати, оскільки це перший доменний контролер;

- на наступному кроці слід ввести та підтвердити надійний пароль для адміністратора контролериа домену. Цей пароль важливий для відновлення Active Directory у спеціальному режимі (DSRM) у випадку проблем;

- на етапі DNS Options може з'явитися попередження щодо делегування DNS. Опцію відмічати не потрібно, оскільки відбувається створення нового домену та нового DNS-сервера. Продовжити, натиснувши Next;

- у наступному вікні, у полі NetBIOS domain name перевірте автоматично згенероване ім'я (зазвичай, це перша частина FQDN). натиснути Next;

- у вікні Paths слід вказати розташування баз даних AD DS, файлів журналів та SYSVOL. Рекомендується залишити значення за замовчуванням;

- у вікні Review Options слід переглянути всі вибрані параметри, щоб переконатися в їх коректності та натиснути Next;

- Майстер виконає перевірку готовності сервера до виконання ролі доменного контролера. Необхідно переглянути всі попередження. Зазвичай, після виконання всіх підготовчих налаштувань, може бути лише попередження про DNS-делегування, яке в даному випадку можна ігнорувати. У випадку виявлення критичних помилок, їх необхідно виправити перед продовженням. У випадку відсутності критичних помилок натиснути Install;

- розпочнеться процес конфігурації сервера як доменного контролера. Цей процес може зайняти певний час, і після його завершення сервер автоматично перезавантажиться.

Після успішного перезавантаження сервера, вхід до нього здійснюватиметься вже у домен, використовуючи обліковий запис адміністратора домену (наприклад, TERKOM\Administrator). Наступним етапом після розгортання доменного контролера є додавання користувачів та створення груп користувачів для ефективної організації доступу до ресурсів та централізованого управління ними.

Для виконання цих операцій необхідно відкрити Диспетчер серверів (Server Manager), перейти у меню "Tools" та вибрати "Active Directory Users and Computers".

У вікні, що відкрилося, адміністратор має можливість переглядати існуючі вбудовані облікові записи користувачів та груп домену. Для створення нової групи слід у меню "Actions" обрати "New", а потім "Group".

При створенні групи обов'язково необхідно вказати її область дії як "Domain Local" (локальна в домені) та обрати тип групи "Security" (група безпеки).

Після створення необхідних груп можна переходити до створення облікових записів користувачів та їх додавання до відповідних груп. Для цього у меню "Actions" слід обрати "New", а потім "User".

У вікні, що відкривається, необхідно заповнити поле "First Name", а також вказати "User logon name" – логін, який використовуватиметься користувачем для входу в систему. Далі натиснути "Next".

На другому кроці майстра створення користувача необхідно ввести та підтвердити пароль для облікового запису користувача. При цьому рекомендується обрати опцію "User must change password at next logon", що зобов'язує користувача встановити власний унікальний пароль при першому вході в систему. За необхідності, також можна відмітити опцію "Account is disabled", щоб тимчасово заблокувати щойно створений обліковий запис. Після цього процес завершується натисканням кнопки "Finish".

3.2 Інструкції з налаштування комутаторів та маршрутизації між VLAN

3.2.1 Інструкції з налаштування комутаторів робочих груп

Конфігурація активного комутаційного обладнання розпочинається з налаштування комутаторів, які обслуговують окремі сегменти мережі.

Першим кроком є конфігурація комутатора робочих груп, розташованого у магазині №1 (див. додаток В). Для цього необхідно встановити консольне з'єднання з пристроєм. Після успішного підключення система автоматично переходить у користувацький режим комутатора. Для присвоєння імені комутатору слід ввести команди, представлені на рисунку 3.3.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sw1
Sw1(config)#
```

Рисунок 3.3 – Налаштування імені комутатора

Після присвоєння імені комутатору, наступним критично важливим кроком є налаштування парольного захисту пристрою. Для забезпечення повного захисту комутатора необхідно сконфігурувати декілька типів паролів [3]:

- пароль консолі (Console Password) – цей пароль захищає фізичний доступ до пристрою через консольний порт;

- пароль VTY (Virtual Teletype) або Telnet/SSH Password – забезпечує захист віддаленого доступу до комутатора за протоколами Telnet або SSH;

- пароль режиму привілейованого виконання (Privileged EXEC Mode Password): Цей пароль захищає доступ до режиму з розширеними правами (enable mode), де можлива зміна конфігурації пристрою;

- команда шифрування паролів – додатково застосовується команда для шифрування всіх незашифрованих паролів у конфігурації, підвищуючи загальний рівень безпеки.

Налаштування пароля режиму привілейованого виконання здійснюється за допомогою команди: enable secret <пароль>.

Ця команда є кращою, оскільки вона дозволяє зберігати пароль у зашифрованому вигляді, підвищуючи безпеку.

Для встановлення пароля на консольний порт, спочатку необхідно перейти до конфігурації консольного інтерфейсу, а потім встановити пароль за допомогою команди password. Команда login активує запит пароля при підключенні до консолі. На рисунку 3.4 представлено приклад налаштування паролів консольного доступу та режиму привілейованого виконання.

```
Sw1(config)#enable secret chudoostriv
Sw1(config)#line console 0
Sw1(config-line)#password chudoostriv
Sw1(config-line)#login
Sw1(config-line)#exit
Sw1(config)#
```

Рисунок 3.4 – Призначення паролю на привілейований режим

Паролі VTY (Virtual Teletype) є ключовими для захисту віддаленого доступу до комутатора через протоколи Telnet або SSH. Як правило, комутатори

мають кілька VTY-ліній (наприклад, від 0 до 15), що дозволяє кільком адміністраторам одночасно підключатися до пристрою для управління.

Повний набір команд, необхідних для встановлення паролів на віддалений доступ, представлено на рисунку 3.5.

```
Sw1(config)#line vty 0 15
Sw1(config-line)#password chudoostriv
Sw1(config-line)#login
Sw1(config-line)#transport input ssh
Sw1(config-line)#exit
Sw1(config)#service password-encryption
Sw1(config)#exit
```

Рисунок 3.5 – Встановлення парою на відділений доступ по SSH

Для забезпечення захищеного віддаленого доступу до комутатора, додатково налаштовується протокол SSH (Secure Shell). Крім того, з метою підвищення загальної безпеки, усі незашифровані паролі в конфігурації пристрою шифруються за допомогою команди service password-encryption. Важливо зазначити, що у наведених прикладах використовується умовний пароль "chudoostriv", який обов'язково слід замінити на реальний, надійний пароль доступу для забезпечення належного рівня захисту.

Після цих налаштувань необхідно створити користувача для SSH, ввівши команди, представлені на рисунку 3.6.

```
Sw1(config)#username admin privilege 15 secret chudoostriv
Sw1(config)#ip domain name chudoostriv.local
Sw1(config)#crypto key generate rsa
The name for the keys will be: Sw1.chudoostriv.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 256
```

Рисунок 3.6 – Створення користувача SSH

Далі потрібно створити на кожному комутаторі VLAN-и. Перелік номерів та назв усіх підмереж VLAN, що будуть створені, представлений у таблиці 3.1.

Таблиця 3.1 – Назви та ідентифікатори підмереж VLAN

Розташування та призначення підмережі	Під'єднано до комутатора	Назва VLAN	Номер VLAN
Магазин головного офісу	SwG	MagG	10
Магазин №1	Sw1	Mag1	11
Магазин №2	Sw2	Mag2	12
Магазин №3	Sw3	Mag3	13
IP-камери відеоспостереження магазину головного офісу	SwG	Cam	14
IP-камери магазину №1	Sw1	Cam	14
IP-камери магазину №2	Sw2	Cam	14
IP-камери магазину №3	Sw3	Cam	14
Бухгалтерія	SwG	Bug	15
Відділ логістики	SwG	Log	16
Відділ менеджменту та маркетингу	SwG	Man	17
Керівник	SwG	Dir	18
Сервер	SwG	Serv	19
Гостьова Wi-Fi головного магазину	SwG	Guest	20
Гостьова Wi-Fi магазину №1	Sw1	Guest	20
Гостьова Wi-Fi магазину №2	Sw2	Guest	20
Гостьова Wi-Fi магазину №2	Sw3	Guest	20

Як видно із таблиці 3.1 крім раніше описаних VLAN присутня віртуальна мережа із номером ID 20, яка буде підмережею із відкритим доступом для відвідувачів магазину.

Створення віртуальних локальних мереж (VLAN) на комутаторі розпочинається з переходу в режим глобальної конфігурації. Далі, використовуючи команду vlan <номер>, де <номер> є унікальним ідентифікатором, створюється

нова VLAN. Після цього за допомогою команди name <назва> [3] їй присвоюється зрозуміла назва. Відповідні команди проілюстровано на рисунку 3.7.

```
Swl(config)#vlan 10
Swl(config-vlan)#name MagG
Swl(config-vlan)#vlan 11
Swl(config-vlan)#name Mag1
Swl(config-vlan)#vlan 12
Swl(config-vlan)#name Mag2
Swl(config-vlan)#vlan 13
Swl(config-vlan)#name Mag3
Swl(config-vlan)#vlan 14
Swl(config-vlan)#name Cam
Swl(config-vlan)#vlan 15
Swl(config-vlan)#name Bug
Swl(config-vlan)#vlan 16
Swl(config-vlan)#name Log
Swl(config-vlan)#vlan 17
Swl(config-vlan)#name Man
Swl(config-vlan)#vlan 18
Swl(config-vlan)#name Dir
Swl(config-vlan)#vlan 19
Swl(config-vlan)#name Serv
Swl(config-vlan)#
Swl(config-vlan)#vlan 20
Swl(config-vlan)#name Guest
```

Рисунок 3.7 – Створення бази даних VLAN

Після створення віртуальних локальних мереж (VLAN), наступним кроком є налаштування типів портів комутатора, що забезпечує їх коректне функціонування. Розрізняють два основні типи портів: Access-порти для підключення кінцевих пристроїв та Trunk-порти – використовуються для міжкомутаторних з'єднань або для підключення до маршрутизатора.

Згідно зі схемою топології мережі (Додаток Б), для конфігурації інтерфейсів комутатора Sw1 у режимі глобального конфігурування необхідно виконати відповідні дії. Зокрема, uplink-інтерфейс комутатора Sw1 слід налаштувати як транковий, оскільки він буде забезпечувати з'єднання з маршрутизатором. Відповідні команди для налаштування інтерфейсів комутатора Sw1 проілюстровано на рисунку 3.8.

Подібним чином потрібно налаштувати комутатори Sw2 – Sw3 та SwG вказуючи лише інші назви інтерфейсів та номери VLAN, відпоідно до даних таблиці 3.2.

```
Sw1(config)#interface range gigabitethernet1/0/1-7,gigabitethernet1/0/10
Sw1(config-if-range)#ex
Sw1(config)#interface range gigabitethernet1/0/1-11
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#interface range gigabitethernet1/0/1-7,gigabitethernet1/0/10
Sw1(config-if-range)#switchport access vlan 11
Sw1(config-if-range)#interface range gigabitethernet1/0/8-9
Sw1(config-if-range)#switchport access vlan 14
Sw1(config-if-range)#interface gigabitethernet1/0/11
Sw1(config-if)#switchport access vlan 20
Sw1(config-if)#interface gigabitethernet1/1/1
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk allowed vlan 11,14,20
Sw1(config-if)#exit
Sw1(config)#
```

Рисунок 3.8 – Налаштування інтерфейсів комутатора Sw1

Таблиця 3.2 – Визначення інтерфейсів комутаторів робочих груп

Назва Switch	Інтерфейси Switch	Типи порпів	Команда визначення інтферйсу
1	2	3	4
Sw1	GigabitEthernet1/0/1 – GigabitEthernet1/0/7, GigabitEthernet1/0/10	access	switchport access vlan 11
	GigabitEthernet1/0/8 – GigabitEthernet1/0/9	access	switchport access vlan 14
	GigabitEthernet1/0/9	access	switchport access vlan 20
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 11,14,20
Sw2	GigabitEthernet1/0/1 – GigabitEthernet1/0/8	access	switchport access vlan 12
	GigabitEthernet1/0/9 – GigabitEthernet1/0/10	access	switchport access vlan 14
	GigabitEthernet1/0/11	access	switchport access vlan 20
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 12,14,20
Sw3	GigabitEthernet1/0/1 – GigabitEthernet1/0/8	access	switchport access vlan 13
	GigabitEthernet1/0/9 – GigabitEthernet1/0/10	access	switchport access vlan 14
	GigabitEthernet1/0/11	access	switchport access vlan 20
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 13,14,20

Продовження таблиці 3.2

1	2	3	4
Sw3	GigabitEthernet1/0/1 – GigabitEthernet1/0/8	access	switchport access vlan 10
	GigabitEthernet1/0/9 – GigabitEthernet1/0/13	access	switchport access vlan 14
	GigabitEthernet1/0/14	access	switchport access vlan 18
	GigabitEthernet1/0/15 – GigabitEthernet1/0/16	access	switchport access vlan 15
	GigabitEthernet1/0/17 – GigabitEthernet1/0/18	access	switchport access vlan 16
	GigabitEthernet1/0/19 – GigabitEthernet1/0/21	access	switchport access vlan 17
	GigabitEthernet1/0/22	access	switchport access vlan 19
	GigabitEthernet1/0/23	access	switchport access vlan 20
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 10,14,15, 16,17,18,19,20

Щоб зберегти всі внесені зміни в конфігурацію комутаторів та забезпечити їх застосування після наступного перезавантаження, виконайте команду “copy running-config startup-config” [3].

3.2.2 Інструкції з налаштування маршрутизатора

Завершальним етапом налаштування активного мережевого обладнання є конфігурація маршрутизатора, який відіграватиме роль шлюзу до Інтернету, а також є шлюзом для віртуальних підмереж в середині окремого магазину або головного офісу.

Перш ніж налаштовувати інтерфейси, призначте маршрутизатору унікальне ім'я, використовуючи ті самі команди, що й для комутаторів робочих

груп (див. рис. 3.3). Так само, необхідно налаштувати парольний захист маршрутизатора та створити обліковий запис користувача для безпечного віддаленого доступу через SSH. Приклади цих команд наведено на рисунках 3.4 – 3.6.

Далі потрібно створити та налаштувати віртуальні підінтерфейси шлюзів із кожної VLAN, що розташована в середині відпоідного магазину. Так для магазину №1 потрібно ввести команди пресдтавленя на рисунку 3.9

```
tl/0/1R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#interface GigabitEthernet0/0/1.11
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.11, changed state to up

R1(config-subif)#encapsulation dotlq 11
R1(config-subif)#ip address 192.168.0.62 255.255.255.224
R1(config-subif)#no shutdown
R1(config-subif)#interface GigabitEthernet0/0/1.14
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.14, changed state to up

R1(config-subif)#encapsulation dotlq 14
R1(config-subif)#ip address 192.168.0.158 255.255.255.224
R1(config-subif)#no shutdown
R1(config-subif)#interface GigabitEthernet0/0/1.20
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.11, changed state to up

R1(config-subif)#encapsulation dotlq 20
R1(config-subif)#ip address 192.168.0.234 255.255.255.224
R1(config-subif)#no shutdown
```

Рисунок 3.9 – Налаштування віртуальних підінтерфейсів маршрутизатора

Для створення підінтерфейсів використовується команда interface <назва>.<номер VLAN>, а потім встановити їх IP-адреси за допомогою ip address <адреса> <маска>. Обов'язково вказати метод інкапсуляції пакетів командою

encapsulation <метод> <номер VLAN>.

IP-адресу шлюзу слід брати із таблиці 2.5, де назви VLAN та адреси відповідних шлюзів, а ID кожної VLAN вказано в таблиці 3.1.

Подібні команди потрібно ввести для налаштування віртуальних інтерфейсів усіх інших маршрутизаторів. При цьому вирішено, що на всіх маршрутизаторах комутатори робочих груп під’єднано до однакового інтерфейсу GigabitEthernet0/0/1, а отже на цьому інтерфейсі будуть створюватись всі віртуальні віртуальні підінтерфси. Повний перелік створених підінтерфейсів представлено у таблиці 3.3.

Таблиця 3.3 – Визначення віртуальних підінтерфейсів маршрутизаторів

Назва Router	Підінтерфейси	Команда encapsulation dot1q	Команда ip address
1	2	3	4
R1	GigabitEthernet0/0/1.11	11	192.168.0.62 255.255.255.224
	GigabitEthernet0/0/1.14	14	192.168.0.158 255.255.255.224
	GigabitEthernet0/0/1.20	20	192.168.0.234 255.255.255.224
R2	GigabitEthernet0/0/1.12	12	192.168.0.94 255.255.255.224
	GigabitEthernet0/0/1.14	14	192.168.0.158 255.255.255.224
	GigabitEthernet0/0/1.20	20	192.168.0.234 255.255.255.224
R3	GigabitEthernet0/0/1.13	13	192.168.0.126 255.255.255.224
	GigabitEthernet0/0/1.14	14	192.168.0.158 255.255.255.224
	GigabitEthernet0/0/1.14	20	192.168.0.234 255.255.255.224
Sw2	GigabitEthernet0/0/1.10	10	192.168.0.30 255.255.255.224
	GigabitEthernet0/0/1.14	14	192.168.0.158 255.255.255.224
	GigabitEthernet0/0/1.15	15	192.168.0.166 255.255.255.248
	GigabitEthernet0/0/1.16	16	192.168.0.174 255.255.255.248
	GigabitEthernet0/0/1.17	17	192.168.0.182 255.255.255.248
	GigabitEthernet0/0/1.18	18	192.168.0.184 255.255.255.252
	GigabitEthernet0/0/1.19	19	192.168.0.190 255.255.255.252
	GigabitEthernet0/0/1.20	20	192.168.0.234 255.255.255.224

Для віртуальних підінтрфесів, які передбачають безпровілний сегменту мережі потрібно налаштувати адресу DHCP-сервера. Як вже повідомлялось це буде сервер мережі на платформі Microsoft Windows Server 2022 із IP-адресою 192.168.0.189. Приклад налаштування адреси DHCP-сервера на маршрутизаторі R1 показано на рисунку 3.10.

```
R1(config)#interface gigabitethernet0/0/1.11
R1(config-subif)#ip helper-address 192.168.0.189
R1(config-subif)#interface gigabitethernet0/0/1.20
R1(config-subif)#ip helper-address 192.168.0.189
R1(config-subif)#
```

Рисунок 3.10 – Встановлення адреси DHCP-севрера для безпровідних підмереж

Далі слід налаштувати статичний маршрут за замовчуванням, щоб забезпечити доступ до Інтернету та інших зовнішніх мереж. Це рішення дозволить обробляти весь трафік, який не має специфічного маршруту, направляючи його на IP-адресу шлюзу інтернет-провайдера. Для цього на маршрутизаторі R1 в режимі глобального конфігурвання слід ввести команду [2]:

ip route 0.0.0.0 0.0.0.0 178.98.17.10

На маршрутизаторі R2 відповідно команду [2]:

ip route 0.0.0.0 0.0.0.0 178.109.12.2

На маршрутизаторі R3 відповідно команду [2]:

ip route 0.0.0.0 0.0.0.0 178.119.134.1

На маршрутизаторі RG відповідно команду [2]:

ip route 0.0.0.0 0.0.0.0 178.99.18.1

На наступному кроці необхідно налаштувати трансляцію мережевих адрес (NAT). Ця функція відіграє важливу роль у забезпеченні ефективного та безпечного доступу внутрішніх мереж до Інтернету. Завдяки NAT, безліч пристроїв у локальній мережі можуть спільно використовувати лише одну публічну IP-адресу. Це не тільки економить цінні публічні IP-адреси, але й значно підвищує рівень безпеки мережі, приховуючи внутрішню структуру від зовнішнього світу.

Для коректної роботи NAT спочатку необхідно визначити внутрішні та зовнішні інтерфейси маршрутизатора [7]. Після цього створюється список контролю доступу (ACL), який ідентифікує трафік, що підлягає трансляції, і цей ACL застосовується до відповідного інтерфейсу [7]. Детальні команди для налаштування NAT можна знайти на рисунку 3.11.

```
R1(config)#interface gigabitethernet 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#interface gigabitethernet 0/0/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface gigabitethernet 0/0 overload
R1(config)#
```

Рисунок 3.11 – Налаштування NAT на маршрутизаторі

3.3 Інструкції по налаштуванню VPN-тунелів та маршрутизації

Для безпечного об'єднання віддалених офісів через загальнодоступний Інтернет, необхідно створити захищені VPN-тунелі. Ці віртуальні мережі, які функціонуватимуть як VPN-тунелі між магазинами та головним офісом, будуть використовувати IP-адреси 192.168.0.192/30, 192.168.0.196/30 та 192.168.0.200/30, як зазначено в таблиці 2.6.

Спочатку слід налаштувати віртуальний інтерфейс VPN-тунелю tunnel 1 на маршрутизаторі R1, вказавши для нього відповідно до таблиці 2.6 IP-адресу 192.168.0.193/30. Для цього слід ввести команди представлені на рисунку 3.12.

```
R1(config)#interface tunnel 1

R1(config-if)#
%LINK-5-CHANGED: Interface Tunnel1, changed state to up

R1(config-if)#ip address 192.168.0.193 255.255.255.252
R1(config-if)#tunnel source gigabitethernet0/0/0
R1(config-if)#tunnel destination 178.99.18.20
R1(config-if)#exit
R1(config)#
```

Рисунок 3. 12 – Налаштування віртуального тунелю на маршрутизаторі R1

На рисунку 3.12 адреса 178.99.18.20 відповідає зовнішній адресі маршрутизатора RG головного офісу.

Після цього необхідно перейти на маршрутизатор головного офісу і ввести налаштування його відповідно до даних таблиці 3.4. Команди налаштування цього маршрутизатора представлено на рисунку 3.13

Таблиця 3.4 – Фізична та віртуальна адресація VPN-тунелів мережі

Нгомер тунелю	Номер магазину	Фізичні IP-адреси на маршрутизаторах		IP-адреси VPN	
		клієнт	сервер	клієнт	сервер
1	№1	178.98.17.101	178.99.18.20	192.168.0.193	192.168.0.194
2	№2	178.109.12.201	178.99.18.20	192.168.0.197	192.168.0.198
2	№3	178.119.134.178	178.99.18.20	192.168.0.201	192.168.0.202

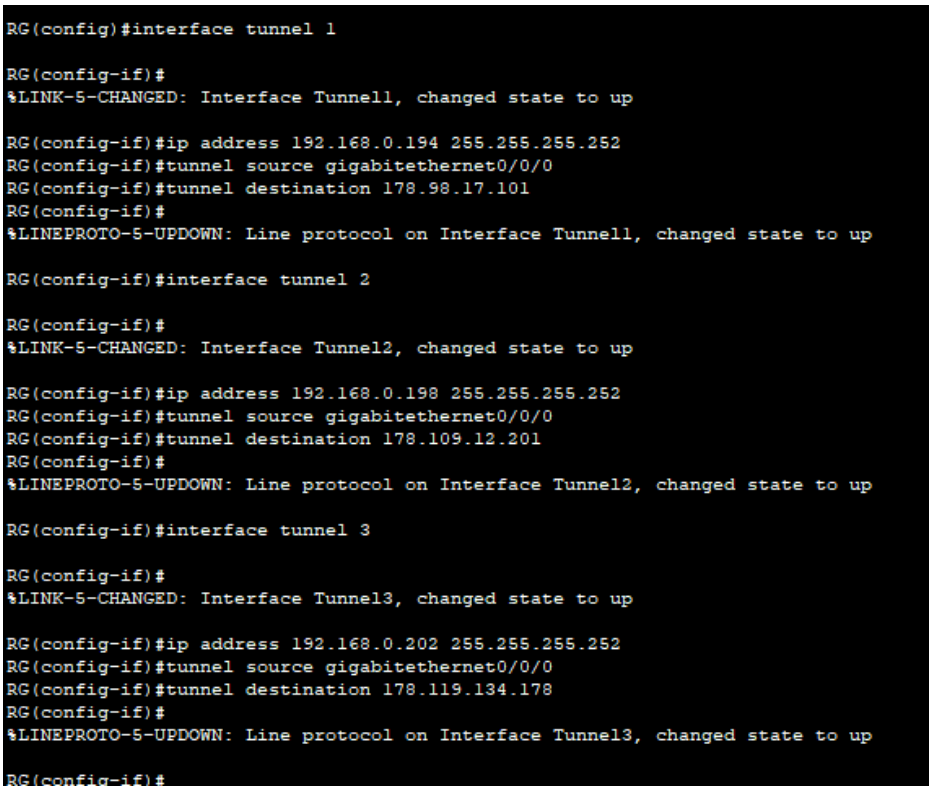


Рисунок 3. 13 – Налаштування віртуального тунелю на маршрутизаторі RG

Відповідно до даних таблиці 3.4 та команд, представлених на рисунку 3.12 необхідно створити інтерфейси VPN-тунелів на маршрутизаторах R2 та R3.

Отже, базові VPN-тунелі створені. Однак, самі по собі вони не є захищеним, тому поверх нього необхідно налаштувати IPSec. Ми будемо використовувати транспортний режим IPSec, який інкапсулює дані, що знаходяться вище мережевого рівня (моделі OSI), не змінюючи при цьому сам IP-заголовок.

Процес налаштування IPSec складається з двох етапів, які потрібно послідовно виконати на обох маршрутизаторах:

На першому етапі слід налаштувати політики ISAKMP. Для цього переходимо в режим глобального конфігурування і створюємо політику безпеки, використовуючи команду представлені а рисунку 3.14.

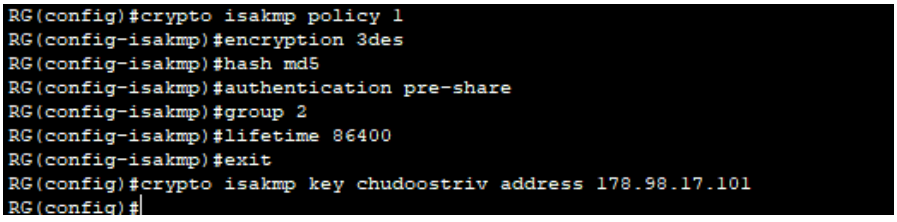


Рисунок 3.14 – Налаштування політики ISAKMP

На рисунку 3.14 в якості методу шифрування вибрано симетричний блоковий шифр 3des та метод хешування MD5 командою hash. Далі вказано метод аутентифікації з наперед визначеним спільним ключем в якості методу перевірки достовірності (pre-share) [7]. Наступною командою задано другу групу Діффі-Хеллмана [7]. Командою lifetime задано час життя ключа сеансу. Тоді задано ключ із іменем “chudoostriv” та адресу фізичного публічного інтерфейсу другого маршрутизатора, відповідно до даних таблиці 3.4. Потрібно зауважити, що ключ аутентифікації повинен співпадати для обидвох точок VPN-тунелю [7].

Тепер переходимо до другої фази налаштування IPSec, де слід створити набір перетворень, які будуть використовуватись для захисту даних. Назвемо цей набір TS. Для його створення вводимо команди представлені на рисунку 3.15. Наступною командою встановлюємо IPSec в транспортний режим

```
RG(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
RG(cfg-crypto-trans)# mode transport
RG(cfg-crypto-trans)# exit
```

Рисунок 3.15 – Встановлення траснпортного режиму роботи IPSec

Далі потрібно налаштувати IPSec на GRE-тунелі за допомогою Crypto Map. Вкажемо назву Crypto Map MY_CRYPTO_MAP і порядковий номер 10. Якщо є кілька записів у Crypto Map, вони обробляються послідовно за цим номером. Далі виконання команди представлені на рисунку 3.16 [7]. Після введення команди створення Crypto Map відбудеться перехід в режим його конфігурації. Далі потрібно вказати адресу відаленого піра, це публічна IP-адреса маршрутизатора на іншому кінці VPN-тунелю 178.98.17.101, представлена в таблиці 2.6. Наступною командою слід прив'язати набір до Crypto Map.

```
RG(config)#crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RG(config-crypto-map)#set peer 178.98.17.101
RG(config-crypto-map)#set transform-set MY_TRANS_SET
```

Рисунок 3.16 – Налаштування Crypto Map

Для GRE over IPSec потрібно, щоб IPSec захищав саме GRE-трафік, який проходить між публічними IP-адресами маршрутизаторів. Для цього створимо

Access Control List (ACL). Цей ACL має дозволяти трафік GRE (протокол 47) між публічними IP-адресами маршрутизаторів представлені у таблиці 2.6. Після цього слід повернутись Crypto Map та прив'яжзати ACL та його до фізичного (зовнішнього) інтерфейсу. Відповідні команди представлені на рисунку 3.17.

```
RG(config)#ip access-list extended PROTECT_GRE_TRAFFIC
RG(config-ext-nacl)#permit gre host 178.99.18.20 host 178.98.17.101
RG(config-ext-nacl)#exit
RG(config)#crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
RG(config-crypto-map)#match address PROTECT_GRE_TRAFFIC
RG(config-crypto-map)#exit
RG(config)#interface gigabitethernet0/0/0
RG(config-if)#crypto map MY_CRYPTO_MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
RG(config-if)#exit
RG(config)#
```

Рисунок 3.17 – Створення ACL та прив’язування до Crypto Map

Перший маршрутизатор налаштовано. Далі потрібно аналогічні команди застосувати до другого маршрутизатора тунелю, врахувавши що в команді crypto isakmp key адреса цільового маршрутизатора буде 178.99.18.20.

Подібним чином слід налаштувати шифрування інші віртуальних тунелів.

Для забезпечення повноцінного зв'язку маршрутизаторsd з усіма внутрішніми віртуальними підмережами необхідно налаштувтаи статичну маршрутизацію між ними. Вся необхідна інформація про IP-адреси та маски цих підмереж буде взята з таблиці 2.4. При цьому, для досягнення цих внутрішніх мереж, адресою наступного переходу (next-hop) слугуватиме IP-адреса віртуального інтерфейсу тунелю відповідного сусіднього маршрутизатора, представлені в таблиці 3.4. Команди для реалізації цих налаштувань на маршрутизаторі R1 проілюстровано на рисунку 3.18.

```
R1(config)#ip route 192.168.0.0 255.255.255.224 192.168.0.194
R1(config)#ip route 192.168.0.32 255.255.255.224 192.168.0.194
R1(config)#ip route 192.168.0.64 255.255.255.224 192.168.0.194
R1(config)#ip route 192.168.0.96 255.255.255.224 192.168.0.194
R1(config)#ip route 192.168.0.128 255.255.255.224 192.168.0.194
R1(config)#ip route 192.168.0.160 255.255.255.248 192.168.0.194
R1(config)#ip route 192.168.0.168 255.255.255.248 192.168.0.194
R1(config)#ip route 192.168.0.176 255.255.255.248 192.168.0.194
R1(config)#ip route 192.168.0.184 255.255.255.252 192.168.0.194
R1(config)#ip route 192.168.0.188 255.255.255.252 192.168.0.194
R1(config)#
```

Рисунок 3.18 – Налаштування маршрутизації на маршрутизаторі R1

Команди налаштування статичної на маршрутизаторі R2 представлено на рисунку 3.19.

```
R2(config)#ip route 192.168.0.0 255.255.255.224 192.168.0.198
R2(config)#ip route 192.168.0.32 255.255.255.224 192.168.0.198
R2(config)#ip route 192.168.0.96 255.255.255.224 192.168.0.198
R2(config)#ip route 192.168.0.128 255.255.255.224 192.168.0.198
R2(config)#ip route 192.168.0.160 255.255.255.248 192.168.0.198
R2(config)#ip route 192.168.0.160 255.255.255.248 192.168.0.198
R2(config)#ip route 192.168.0.168 255.255.255.248 192.168.0.198
R2(config)#ip route 192.168.0.176 255.255.255.248 192.168.0.198
R2(config)#ip route 192.168.0.184 255.255.255.252 192.168.0.198
R2(config)#ip route 192.168.0.188 255.255.255.252 192.168.0.198
R2(config)#
```

Рисунок 3.19 – Налаштування маршрутизації на маршрутизаторі R2

Команди налаштування статичної на маршрутизаторі R3 представлено на рисунку 3.20.

```
R3(config)#ip route 192.168.0.0 255.255.255.224 192.168.0.202
R3(config)#ip route 192.168.0.32 255.255.255.224 192.168.0.202
R3(config)#ip route 192.168.0.96 255.255.255.224 192.168.0.202
R3(config)#ip route 192.168.0.128 255.255.255.224 192.168.0.202
R3(config)#ip route 192.168.0.160 255.255.255.248 192.168.0.202
R3(config)#ip route 192.168.0.168 255.255.255.248 192.168.0.202
R3(config)#ip route 192.168.0.176 255.255.255.248 192.168.0.202
R3(config)#ip route 192.168.0.184 255.255.255.252 192.168.0.202
R3(config)#ip route 192.168.0.188 255.255.255.252 192.168.0.202
R3(config)#
```

Рисунок 3.20 – Налаштування маршрутизації на маршрутизаторі R2

Команди налаштування статичної на маршрутизаторі RG представлено на рисунку 3.21.

```
RG(config)#ip route 192.168.0.32 255.255.255.224 192.168.0.193
RG(config)#ip route 192.168.0.128 255.255.255.224 192.168.0.193
RG(config)#ip route 192.168.0.64 255.255.255.224 192.168.0.197
RG(config)#ip route 192.168.0.128 255.255.255.224 192.168.0.197
RG(config)#ip route 192.168.0.96 255.255.255.224 192.168.0.201
RG(config)#ip route 192.168.0.128 255.255.255.224 192.168.0.201
RG(config)#
```

Рисунок 3.21 – Налаштування маршрутизації на маршрутизаторі RG

3.4 Інструкції по налаштуванню засобів захисту мережі

Захист мережевих пристроїв є фундаментальним етапом як на стадії проектування, так і під час подальшої експлуатації комп'ютерних мереж. Будь-який недолік у цьому аспекті може призвести до серйозних наслідків: несанкціонованого доступу до керування обладнанням, перехоплення трафіку та витоку конфіденційних даних.

Згідно з джерелом [3], до ключових механізмів забезпечення захисту мережевих пристроїв належать:

- застосування стійких паролів, а також надійних методів автентифікації та авторизації;
- деактивація непотрібних протоколів і сервісів для зменшення поверхні атаки;
- автоматична активація компонентів безпеки;
- обмеження часу для підключень та активних сесій;
- налаштування системних попереджень.

У мережі ТзОВ "ЧудоОстрів" безпеці активного мережевого обладнання (комутаторів та маршрутизатора) приділено особливу увагу через багаторівневий парольний захист:

- консольний доступ: захист при прямому підключенні;
- віддалений доступ (SSH): захист від несанкціонованого керування, з перевагою SSH завдяки шифруванню (на відміну від Telnet);
- привілейований режим: обмеження доступу до критичних налаштувань.

Деталі конфігурації цих паролів описані в розділі 3.2.1.

Для всебічного та надійного захисту мережевої інфраструктури "ЧудоОстрів", окрім базових парольних заходів, впроваджено такі ключові аспекти безпеки:

- управління обліковими записами та привілеями (через Active Directory). Забезпечення принципу мінімальних привілеїв, регулярний перегляд облікових записів та впровадження політики складних паролів (12-14 символів);
- актуальне антивірусне ПЗ, активовані брандмауери, регулярні оновлення ОС та ПЗ, обмеження використання неперевірених знімних носіїв;
- сегментація мережі (VLAN), конфігурація ACL (принцип "заборонити все, що не дозволено"), розгляд IDS/IPS для моніторингу та блокування атак;
- автоматизоване копіювання критичних даних, дотримання стратегії 3-2-1 (3 копії, 2 носії, 1 поза офісом), регулярне тестування відновлення;

- централізований збір журналів подій, система моніторингу для відстеження аномалій та раннього виявлення загроз.

- розробка чіткої політики використання ресурсів, регулярні тренінги з кібербезпеки для всього персоналу (фішинг, безпека паролів, реагування на інциденти), а також розробка плану дій у разі інцидентів.

Впровадження цих заходів дозволить "ЧудоОстрів" створити надійну, багаторівневу захищену мережеву інфраструктуру для безперебійної роботи, збереження даних та підтримки репутації.

3.5 Моделювання мережі

Для практичної реалізації теоретично спроектованої мережі необхідно виконати декілька кроки в середовищі симулятора Cisco Packet Tracer.

На першому етапі потрібно з панелі елементів (у лівому нижньому куті) встановити усі необхідні мережеві пристрої та з'єднайте їх кабелями згідно з логічною схемою, представленою в Додатку Б.

Після цього вибрати на панеді елеметів відповідний тип каьелю і клікнути на першому пристрої для з’єднання, вибрати назву інierфейсу для з’єднання, а тоді клікнути на іншому пристрої і теж вибрати назву інтерфейсу.

Далі, для кожної робочої станції необхідно відкрити вікно налаштування пристрою, перейти на вкладку Desktop, обрати IP Configuration. Встановити IPv4 Address та Subnet Mask (відповідно до таблиці 2.4), Default Gateway (відповідно до таблиці 2.5) та DNS Server (192.168.0.189). Рисунок 3.22 демонструє приклад налаштування IP-адреси для комп'ютера PC_1_1 з підмережі магазину №1.

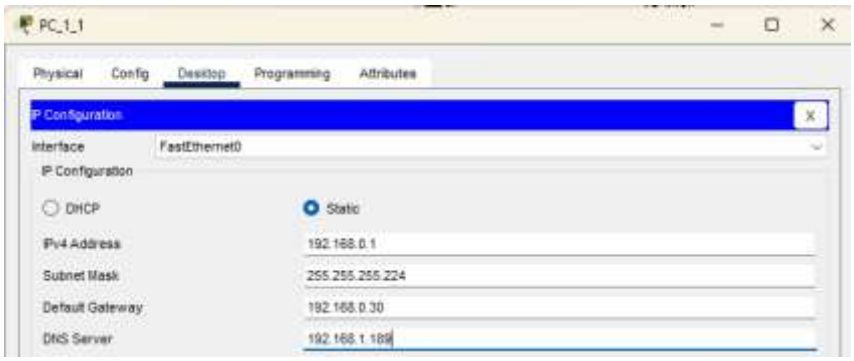


Рисунок 3.22 – Приклад призначення статичних адрес кінцевим вузлам

Оскільки мережа включає бездротові вузли, потрібно налаштувати точки доступу. Для цього у вікні їх налаштувань перейдіть до Config > Port1, де вкажіть SSID (назва Wi-Fi-мережі), протокол аутентифікації WPA2-PSK та PSK-Pass Phrase. Приклад налаштування Wi-Fi-мережі магазину №1 на рисунку 3.23.

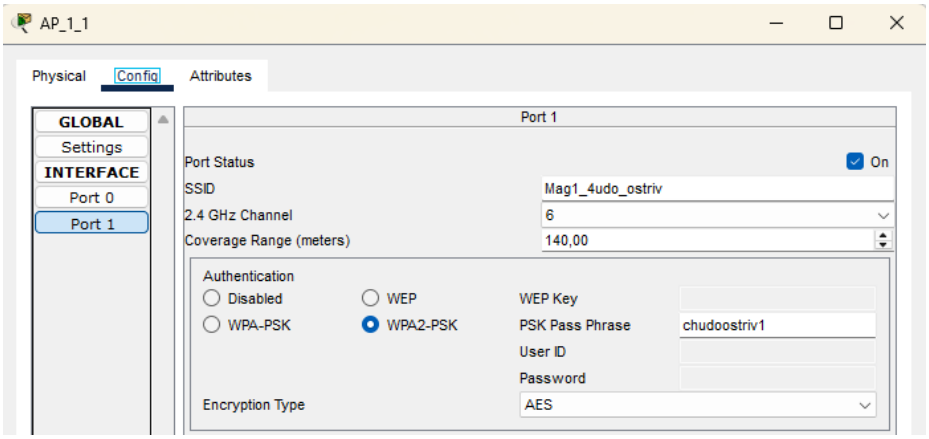


Рисунок 3.23 – Налаштування точки доступу безпровідної Wi-Fi мережі

Після цього, ідентичні налаштування зробити на всіх мережевих вузлах, що будуть під'єднані до цієї Wi-Fi-підмережі, додатково ввівши параметр IP-адреси пристрою. Приклад налаштування безпровідного пристрою підмережі магазину №1 показано на рисунку 3.24.

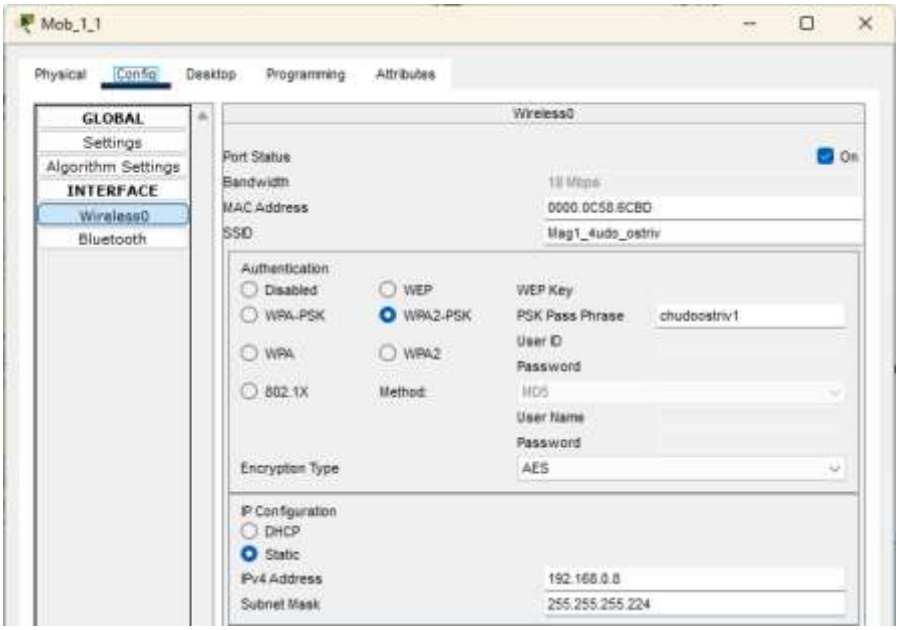


Рисунок 3.24 – Налаштування безпровідних пристроїв працівників магазину №1 та POS-терміналів

Також необхідно прописати адреси камер відеоспостоереження ввівши параметри віртуальної підмережі Cam, представлені у таблциях 2.4 та 2.5. Приклад налаштування IP-камери показано на рисунку 2.25

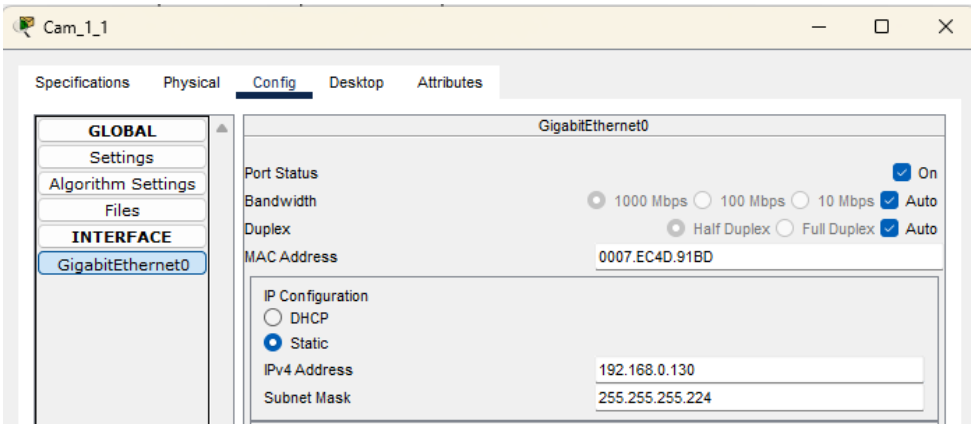


Рисунок 3.25 – Приклад налаштування IP-адреси камери відеоспостереження

Для налаштування активних мережевих пристроїв таких як комутатори та маршрутизатори використано консольний режим під'єднання. Для цього слід під'єднати до кожного комутатора та маршрутизатора ПК або ноутбук в консольному режимі за допомогою кабелю Console із розділу Connections.

Всі команди налаштування активного мережевого обладнання представлені в попередніх розділах 3.2 та 3.3 даної кваліфікаційної роботи.

Остаточний проект мережі представлено у додатку Г.

3.5 Тестування роботи побудованої моделі мережі

Для тестування спроектованої мережі було проведено перевірку з'єднання між пристроями, що належать до різних VLAN. Ця перевірка виконувалася за допомогою команди ping з робочої станції PC_1_1, що знаходиться в підмережі Mag1. Додатково, було здійснено перевірку маршрутів проходження пакетів командою tracert. При цьому дана команда буде демонструвати використання VPN-тунелю при перевірці з'єднання із підмережеми ріхних магазинів та головного офісу.

Щоб змоделювати роботу мережі в Cisco Packet Tracer, перейдіть у режим емуляції, натиснувши кнопку Simulation (правий нижній кут вікна), а потім Play.

Щоб перевірити функціональність мережі центрального офісу, необхідно виконати ping-перевірку з'єднання з комп'ютерами інших десяти підмереж. З будь-якого ПК (наприклад, PC_G_1 з MagG) відкрийте Command Prompt (через Desktop) і по черзі надсилайте ping на адреси інших підмереж, закінчуючи сервером 192.168.1.89 (див. рис. 3.26).

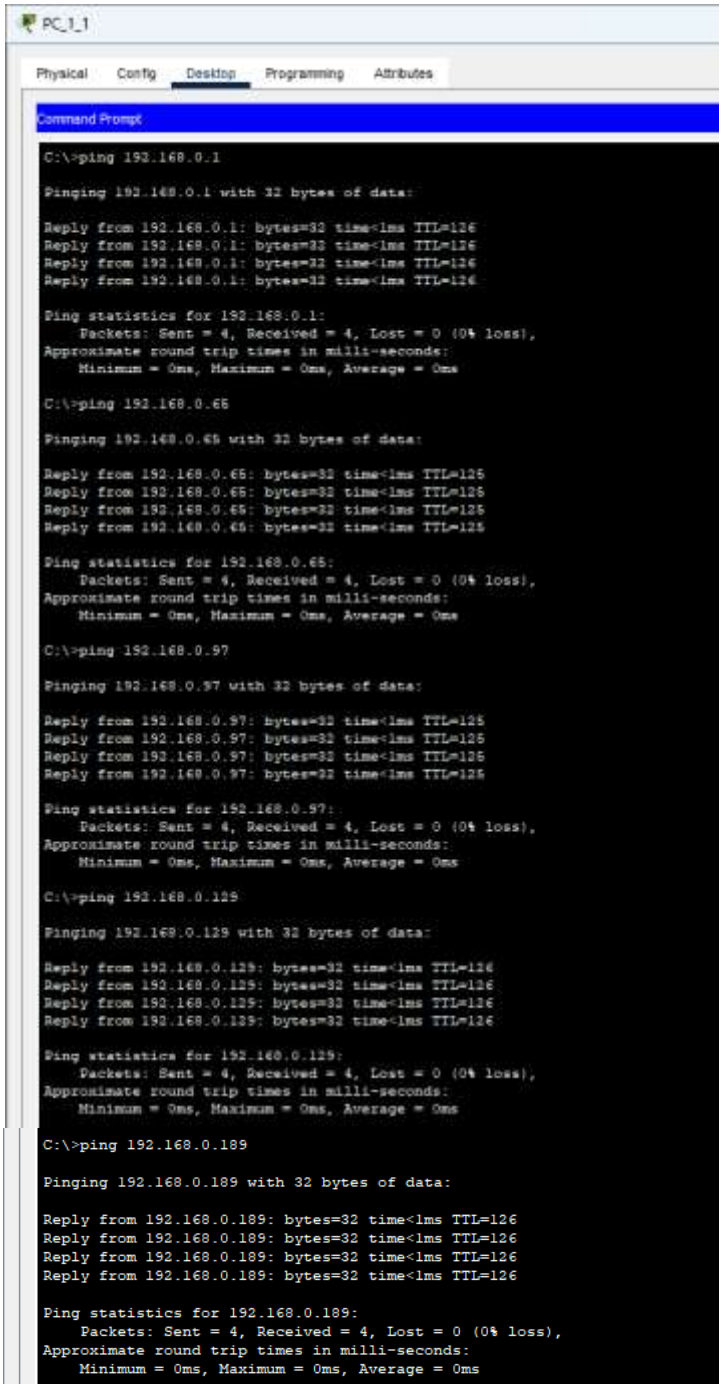


Рисунок 3.26 – Тестування з'єднання командою ping

Для аналізу повного маршруту проходження даних по мережі та визначення затримок на її різних ділянках також рекомендується використовувати команду tracert (див. рис. 3.27).

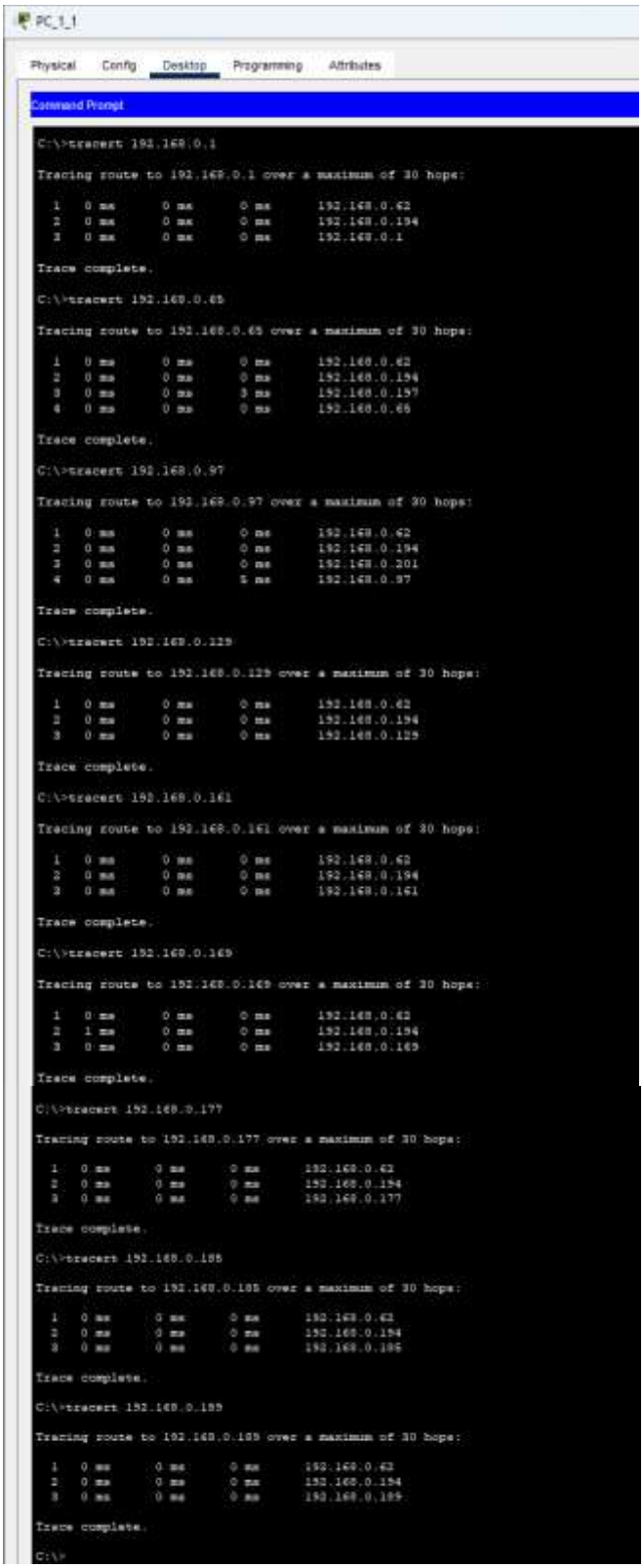


Рисунок 3.27 – Тестування мережі командою Tracert

Якщо проаналізувати маршрути проходження пакетів, то можна зробити висновок, що дані між будівлями магазинів проходять через створені VPN-тунелі (адреса VPN-тунелю – 192.168.0.194). Отже, захищені віртуальні тунелі через загальнодоступну мережу Інтернет налаштовані правильно.

Також на маршрутизаторах можна переглянути таблиці маршрутизації командою show ip route (див. рис. 3.28).

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 11 subnets, 3 masks
S       192.168.0.0/27 [1/0] via 192.168.0.194
C       192.168.0.32/27 is directly connected, GigabitEthernet1/0
S       192.168.0.64/27 [1/0] via 192.168.0.194
S       192.168.0.96/27 [1/0] via 192.168.0.194
S       192.168.0.128/27 [1/0] via 192.168.0.194
S       192.168.0.160/29 [1/0] via 192.168.0.194
S       192.168.0.168/29 [1/0] via 192.168.0.194
S       192.168.0.176/29 [1/0] via 192.168.0.194
S       192.168.0.184/30 [1/0] via 192.168.0.194
S       192.168.0.188/30 [1/0] via 192.168.0.194
C       192.168.0.192/30 is directly connected, GigabitEthernet0/0

R1#
```

Рисунок 3.28 – Перегляд таблиць маршрутизації на маршрутизаторі R1

Всі виконані команди тестування мережі ТзОВ експертФан "ЧудоОстрів" були успішними, тому можна зробити висновок, що мережа даної сітки магазинів із створеною статичною маршрутизацію та VPN-тунелями побудована успішно.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Для визначення загальної тривалості науково-дослідної роботи (НДР) необхідно зібрати дані про час, витрачений на кожен етап технологічного процесу.

Ця інформація, включаючи етапи та середній час їхнього завершення, буде представлена в Таблиці 4.1. Збором даних займатимуться керівник, інженер та технік.

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Постановка задачі, формування технічного завдання на проект локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проекту	15
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі ТзОВ експертФан "ЧудоОстрів". Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури ТзОВ експертФан "ЧудоОстрів"для сегментування локальної мережі на підмережі.	Інженер	25

Продовження таблиці 4.1

1	2	3	4
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Технік	35
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	30
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
		Разом	110

Сумарний час виконання операцій технологічного процесу проектування мережі становить 110 години, з них 15 годин – робота керівника проекту, 60 години – інженера, 35 години – техніка.

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.

Виходячи з рекомендованих тарифних ставок встановимо таку ставку для керівник проекту – 230 грн, інженера – 185 грн./год. а для техніка – 150 грн./год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 15 \cdot 230 = 3450$ грн.
- інженера – $З_{осн2} = 60 \cdot 185 = 11100$ грн.
- техніка – $З_{осн3} = 35 \cdot 150 = 5250$ грн.

Сумарна основна заробітна плата становить

$$З_{осн}=3450 +11100+ 5250 =19800 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника $З_{дод1}=3450 \cdot 0,12= 414$ грн.
- інженера $З_{дод1}=11100 \cdot 0,12= 1332$ грн.
- техніка $З_{дод3}=5250 \cdot 0,12= 630$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=414 + 1332 + 630 = 2376 \text{ грн.}$$

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

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

Отже, загальні витрати на оплату праці становлять:

$$В_{о.п.}= 19800 + 2376 = 22176 \text{ грн.}$$

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

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з} = 22176 \cdot 0,22 = 4878,72 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/	Категорія працівни-ків	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн
		Тарифна ставка, грн.	К-сть відпрац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	220	10	3450	414		
2	Інженер	180	40	11100	1332	-	-
3	Технік	150	25	5250	630	-	-
			Разом	19800	2376	4878,72	27054,72

Отже, загальні витрати на оплату праці становлять 27054,72 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{BI} = q_i \cdot P_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} \sum M_{B_i} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа Hypernet WMNC-6U-FLAT	шт.	3	3580	10740
2	Патчпанель 24 порти, кат. 6	шт.	3	1180	3540
3	Розетка RJ-45 (категорія 6)	шт.	39	120	4680
4	Розетка підлогова RJ-45	шт.	9	190	1710
5.	Роз’єм 8P8C (100 шт)	шт.	1	590	590
6	Короб (середня ціна)	м.	245	112	27440
7	Короб пілоговий	м.	13	195	2535
8	Кабель UTP (кат. 6) (бухта)	шт.	3	5353	16059
9	Патчкорди (кат. 6)	шт.	48	51	2448
10	Патчкорди (оптоволокно)	шт.	3	75	225
11	Кабель опотоволоконний	м.	4	33	132
12	Конектор SC	шт.	3	38	114
13	Гофрована трубка	м.	22	40	880
14	Маршрутизатора Cisco ISR4221/K9	шт.	3	24510	73530
15	Комутатор робочих груп Cisco Catalyst 2960L-24PS-LL	шт.	3	47313	141939
16	Точка доступу TP-LINK EAP225	шт.	6	2890	17340
17	IP-камера Reolink RLC-1224A	шт.	10	5699	56990
18	ДБЖ APC Back-UPS Pro 1200VA	шт.	3	3680	11040
Р а з о м			-	-	371938

Отже, загальна сума матеріальних витрат на розробку мережі становить 371938 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 10 годин, споживана потужність – 0,5 кВт/год, вартість 1 кВт електроенергії - 7 грн. Тому витрати на електроенергію будуть становити::

$$З_е = 0,5 \cdot 10 \cdot 7 = 35 \text{ грн.}$$

4.5 Визначення транспортних затрат

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

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

де $Т_В$ – транспортні витрати.

Отже,

$$Т_В = 371938 \cdot 0,08 = 29755,04 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

В процесі використання основних фондів виконуються заходи що до їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх

відшкодування у вартісній формі, яке здійснюється шляхом амортизації. Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення. Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_в \cdot Н_А}{100\%} \cdot T \quad (4.9)$$

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

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

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 26000 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{26000 \cdot 0{,}04}{150} \cdot 10 = 69{,}33 \text{ грн}$$

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.

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

де H_B – накладні витрати.

$$H_B = 22176 \cdot 0{,}4 = 8870{,}4 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

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

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

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	22176	5,07
Відрахування на соціальні заходи	4878,72	1,11
Матеріальні витрати	371938	84,97
Витрати на електроенергію	35	0,01
Транспортні витрати	29755,04	6,8
Амортизаційні відрахування	69,33	0,02
Накладні витрати	8870,4	2,03
Собівартість	437722,49	100

В таблиці 4.4 зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати, тобто собівартість ($С_в$) НДР розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.п.} + З_{м.в.} + З_е + Т_в + А + Н_в \quad (4.11)$$

Отже, собівартість дорівнює C_B=437722,49 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де $P_{рен.}$ – рівень рентабельності;

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

Отже, ціна НДР становить:

$$Ц = 437722{,}49 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 682847{,}08 \text{ грн}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

де *П* – прибуток;

C_B – собівартість;

$$П = 682847{,}08 - 437722{,}49 = 245124{,}59$$

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою:

$$E_p = \frac{П}{С_в} = \frac{245124{,}59}{437722{,}49} = 0{,}56 \quad (4.14)$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень $Т_р$:

$$T_p = \frac{1}{E_р} \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку:

$$T_p = \frac{1}{0{,}56} = 1{,}8$$

Всі дані внесемо в зведену таблицю 4.5 економічних показників.

Таблиця 4.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	437722,49 грн.
2.	Плановий прибуток, грн.	245124,59 грн.
3.	Ціна, грн.	682847,08 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп’ютерної мережі для сітки магазинів ТзОВ експертФан "ЧудоОстрів" становить 682847,08 грн. Зважаючи на високі показники економічної ефективності – 0,56, кошти, вкладені в проведення проектних робіт окупляться за 1,8 року.

.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

5.1 Система організаційно-технічних заходів з пожежної безпеки в ТзОВ експертФан "ЧудоОстрів"

Комплексний підхід до пожежної безпеки вимагає інтеграції як організаційних, так і технічних заходів, спрямованих на запобігання виникненню пожеж, мінімізацію можливих збитків та, найголовніше, гарантування безпеки для всього персоналу та відвідувачів.

В рамках організаційних заходів на підприємстві призначені відповідальні особи за пожежну безпеку, як на рівні всього ТзОВ, так і для кожного окремого магазину та офісу. Їхні обов'язки включатимуть контроль за дотриманням протипожежного режиму, що охоплює управління електроприладами, контроль за зберіганням горючих матеріалів та загальний порядок у приміщеннях [2].

Життєво важливим є розробка та затвердження детальних інструкцій з пожежної безпеки для всіх типів приміщень (торгові зали, складські приміщення, офіси).

Технічні заходи спрямовані на розгортання та підтримку надійних систем протипожежного захисту. Усі приміщення магазинів та головного офісу облад-нані автоматичною пожежною сигналізацією (АПС), яка має бути у постійно справному стані, з обов'язковим виведенням сигналу на пульт пожежного спостереження Державної пожежно-рятувальної служби (ДПРЗ). Паралельно з АПС функціонує система оповіщення про пожежу та управління евакуацією (СОУЕ), що забезпечує своєчасне голосове інформування людей про пожежу та чіткі вказівки щодо евакуації. Ці системи доповнюються світловими покажчиками "Вихід", що встановлені вздовж евакуаційних шляхів та біля виходів, як це також вказано на схемах евакуації, представлених на долатку Д.

У приміщеннях з великим скупченням людей (наприклад, торгові зали) або специфічними ризиками встановлено систему димовидалення для забезпечення безпечної евакуації.

Щодо первинних засобів пожежогасіння, кожен об'єкт ТзОВ "ЕкспертФан "ЧудоОстрів" буде забезпечений необхідною кількістю та типами вогнегасників.

В Україні основним нормативним документом, що визначає вимоги до кількості та розміщення вогнегасників, є ДБН В.2.5-56:2014 "Системи протипожежного захисту" [12]. Хоча цей ДБН стосується систем протипожежного захисту в цілому, він містить посилання на інші нормативні документи, зокрема "Правила експлуатації та типові норми належності вогнегасників" (Наказ МВС України від 15.01.2018 № 25). Саме ці Правила є основним документом, який детально регламентує розрахунок кількості вогнегасників [2].

Перш за все, необхідно визначити потенційні класи пожежі в кожному приміщенні або зоні. Це впливає на тип необхідного вогнегасника [1]:

- клас A – горіння твердих речовин (дерево, папір, тканина, пластмаси);
- клас B – горіння рідких речовин (бензин, мастила, фарби, розчинники);
- клас C – горіння газоподібних речовин (природний газ, пропан, ацетилен);
- клас D – горіння металів та їх сплавів (магній, натрій, калій).
- клас F (або K в українській класифікації) – Горіння жирів та олій у кухонних приладах.
- електроустановки під напругою (E) – вогнегасники, призначені для гасіння електроустановок, маркуються відповідним чином (наприклад, ВВК - вуглекислотні, ВП - порошкові, що мають допуск для електроустановок).

Виходячи з класів пожежі, обираються відповідні типи вогнегасників (порошкові, вуглекислотні, водопінні тощо) та їхній ранг (вогнегасна здатність). Ранг вогнегасника вказується на його етикетці (наприклад, 2A, 55B).

Оскільки, магазини іграшок та дитячого одягу можна віднести до пожеж класу А та Е, використовуються водопінні (ВВП) або порошкові (ВП) вогнегасники. Ранг (наприклад, 2А, 3А, 4А) показує, який об'єм твердих матеріалів може погасити вогнегасник.

Розрахунок базується на площі приміщення та вогнегасній здатності вогнегасників. "Правила експлуатації та типові норми належності вогнегасників" містять таблиці норм належності, де вказано:

– мінімальна кількість вогнегасників для різних категорій приміщень (виробничі, складські, адміністративні, громадські, торгові) та їх площі.

– тип та ранг вогнегасника для конкретного класу пожежі та площі.

На кожні 100-200 м² площі приміщення потрібен даного типу потрібно один вогнегасник з відповідним рангом.

Вогнегасники повинні бути розташовані на відстані не більше 20 м від можливого місця виникнення пожежі для приміщень категорій А, Б, В.

Розрахуємо орієнтовну кількість вогнегасників для торгового залу та загальної площі будівлі.

Торговий зал із розмірами 6м×9м=54м^2. Класи пожежі, як вже відзначалось А та Е.

Площа 54 м² менша за 100 м², але для малих приміщень все одно потрібна мінімальна кількість вогнегасників. Зазвичай, на невеликі приміщення встановлюють 1-2 вогнегасники, щоб забезпечити доступність у разі займання.

Для приміщення потрібно 1 х Вогнегасник порошковий ВП-5 (або ВП-6) – для покриття класів А та Е. Це універсальний варіант для торгового залу [2].

Вогнегасник вуглекислотний ВВК-3,5 (або ВВК-5) – особливо якщо багато електроніки (каси, холодильники) і важлива відсутність забруднення. ВВК-3,5 ефективно гасить пожежі класу В, С та Е [2].

Найкраще комбіноване рішення для торгового залу: 1 ВП-5 (універсальний) плюс 1 ВВК-3,5 (для електроніки, де не бажаний порошок) або щонайменше 1 ВП-5 (що покриває усі основні ризики).

Загальна площа всього прміщення 108 м² перевищує 100 м², тому це потребує мінімум 2 вогнегасників. Враховуючи, що будівля містить різні зони (торговий зал, склад, офіс), типи ризиків відрізняться.

Оптимально (для кращого захисту) на все приміщення магазину 2 х ВП-5 (або ВП-6) плюс 1 х ВВК-3,5 (або ВВК-5). Розміщення: 1 ВП-5 у торговому залі,

1 ВП-5 на складі/офісі, 1 ВВК-3,5 біля електрообладнання (каси, серверна, офісні комп'ютери).

Площа 108 м² значно менша за 5000 м². Отже, окремий пожежний щит/стенд з повним комплектом інвентарю не є обов'язковим для такої площі.

Для кожного з чотирьох об'єктів розроблено та затверджено індивідуальні плани евакуації, представлені на схемах додатку Д. Ці плани чітко позначають шляхи евакуації, місця розташування евакуаційних виходів та первинних засобів пожежогасіння.

Усі співробітники, включно з тимчасовим персоналом, проходять обов'язкові інструктажі та навчання правилам користування вогнегасниками. Регулярні тренування з евакуації, що проводитимуться щонайменше раз на півроку на кожному об'єкті, дозволять відпрацювати дії персоналу в екстремальних ситуаціях згідно з цими планами.

Протипожежний режим також включатиме облаштування спеціальних місць для куріння, забезпечення безперешкодного доступу до пожежного обладнання та регулярне прибирання приміщень.

Технічні заходи спрямовані на створення надійних систем протипожежного захисту. У всіх приміщеннях магазинів та головного офісу встановлено та підтримується справний стан автоматичної пожежної сигналізації (АПС) із виведенням сигналу на пульт пожежного спостереження.

Одночасно з цим, працює система оповіщення про пожежу та управління евакуацією (СОУЕ), що забезпечує своєчасне голосове інформування та світлові покажчики, які вказують на евакуаційні виходи, чітко позначені на схемах евакуації.

Кожен об'єкт забезпечений необхідною кількістю та типами вогнегасників (вуглекислотні, порошкові, водопінні), розміщених у легкодоступних місцях, як це також вказано на схемах евакуації. Періодичні перевірки та обслуговування вогнегасників є обов'язковими.

Важливим аспектом є електробезпека, що передбачає регулярні вимірювання опору ізоляції та перевірку заземлення, а також захист електро-

мережі від перевантажень. Евакуаційні шляхи та виходи, детально промальовані на планах евакуації, завжди утримуватимуться вільними та незахарашеними, а двері, що ведуть назовні, завжди відчинятимуться без перешкод.

Постійний контроль та моніторинг пожежної безпеки забезпечується через регулярні внутрішні перевірки на всіх об'єктах та тісну взаємодію з місцевими підрозділами ДСНС.

5.2 Загальні вимоги безпеки з охорони праці для користувачів ПК

Дотримання вимог безпеки праці при роботі з персональним комп'ютером є запорукою збереження здоров'я та високої працездатності користувача. Перед початком роботи необхідно переконатися, що робоче місце належним чином організовано: монітор, клавіатура та миша розташовані зручно, освітлення достатнє і рівномірне, а електричні дроти та обладнання не мають видимих пошкоджень. Не допускається починати роботу на несправному обладнанні або у разі виявлення будь-яких несправностей в електромережі чи електроприладах.

Під час роботи з ПК необхідно суворо дотримуватися ергономічних вимог. Монітор слід розміщувати на відстані 60-70 см від очей, верхній край екрана має бути на рівні або трохи нижче рівня очей. Клавіатура повинна лежати рівно, щоб кисті рук були прямими, а лікті згиналась під кутом близько 90 градусів. Миша має бути розташована поруч із клавіатурою, забезпечуючи природне положення руки. Крісло повинно бути стійким, з регульованою висотою сидіння та спинки, а також, бажано, з підлокітниками, щоб забезпечити опору для рук та комфортну позу. Слід уникати тривалого перебування в одній позі.

Електробезпека є одним із найважливіших аспектів. Забороняється самостійно ремонтувати або втручатися в роботу ПК та периферійного обладнання. У разі будь-яких несправностей, таких як іскріння, запах диму, нехарактерні звуки, необхідно негайно вимкнути обладнання від електромережі та повідомити про це керівництво або відповідального за технічне

обслуговування. Неприпустимо працювати мокрими руками або в умовах підвищеної вологості. Слід уникати потрапляння рідин на обладнання.

Для запобігання перевтомі очей, опорно-рухового апарату та нервової системи, користувачам ПК рекомендується робити регулярні перерви. Після кожної години роботи бажано робити 5-10-хвилинні перерви, під час яких виконувати вправи для очей, розминку для шиї, плечей та спини, а також короткі фізичні вправи. Кожні 2-3 години рекомендується робити більш тривалу перерву (15-20 хвилин) з можливістю змінити діяльність або вийти на свіже повітря. Загальна тривалість безперервної роботи з ПК протягом робочого дня повинна відповідати встановленим нормам.

Окрім цього, важливо підтримувати належний мікроклімат у приміщенні: забезпечувати регулярне провітрювання, підтримувати оптимальну температуру та вологість повітря. Робоче місце повинно утримуватися в чистоті, без зайвих предметів, що можуть заважати або створювати ризик травмування. Дотримання цих простих, але ефективних вимог безпеки праці дозволить мінімізувати ризики для здоров'я користувачів ПК та забезпечити комфортні умови для продуктивної роботи.

.

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проект корпоративної мережі сітки магазинів ТзОВ "ЕкспертФан "ЧудоОстрів". Основні технічні характеристики розробленого проекту локальної мережі:

- фізична топологія всередині приміщення – «гібридна», що поєднує «ієрархічну розширену зірку» та комірчасту безпровідну топології;
- топологія WAN – VPN over Internet;
- технології використані для розробки мережі - IEEE 802.3ab, IEEE 802.11ac, IEEE 802.1Q;
- маршрутизатор-шлюз – Cisco ISR4221/K9;
- комутатори робочих груп – Cisco Catalyst 2960L-24PS-LL;
- стек протоколів локальної мережі – TCP/IP версії 4.

В кваліфікаційній роботі спроектовано логічну та фізичну топологію мережі. Підібрано відповідне апаратне та програмне забезпечення. При виборі апаратного забезпечення (активного) враховано можливість масштабування локальної мережі в майбутньому.

Описано процедуру налаштування активного комутаційного обладнання. Розроблено інструкцію з тестування та налагодження мережі, віртуальних тунелів VPN over Internet із ширфування даних стеком проктолів IPSec, розгортання доменного контролера на основі Microsoft Windows Server 2022, налаштування вірутальних

Логічна та фізична топології локальної мережі подано в графічній частині.

В економічній частині зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі. Отримана вартість мережі є в межах запропонованої замовником.

Останній розділ роботи описує питання охорони праці, та техніки безпеки, які є важливими для безпечної праці користувачів комп’ютерної техніки

ПЕРЕЛІК ПОСИЛАНЬ

1. Атаманчук П. С., Мендерецький В. В., Панчук О. П. Чорна О. Г. Основи охорони праці. Навч. посіб. – К.: Центр учбової літератури, 2017. – 224 с.

2. Бедрій Я.І., Основи охорони праці : навчальний посібник для студентів вищих навчальних закладів / Я.І. Бедрій. Вид. 4-те переробл. і допов. — Тернопіль : Навчальна книга – Богдан, 2016. – 240 с.

3. Буров Є., Митник М. Комп'ютерні мережі.(у 2-х томах) Львів, Магнолія, 2018.

4. Єфіменко А. А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. – Житомир : Житомирська політехніка, 2021. – 116 с.\

5. Запорожець О. І.. Основи охорони праці. Підручник. – К.: Центр учбової літератури, 2019. – 264 с.

6. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2016 р.) - 500 с.

7. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2015 р.) – 500 с.

8. Методичні вказівки до виконання дипломного проекту зі спеціальності 5.091504 «Обслуговування комп′ютерних та інтелектуальних систем та мереж» напрямок "Обслуговування технічних засобів комп'ютерних систем і мереж"

9. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.

10. Базові поняття мережевих технологій. URL: http://um.co.ua/8/8-17/8-1748.html. Дата звернення: 5.06.2025.

11. ДСТУ EN 50110-1:2014. Експлуатація електроустановок. Частина 1: Загальні вимоги. URL: https://standards.ua/50110-1. (Дата звернення: 10.06.2025)

12. ДБН В.2.5-56:2014 "Системи протипожежного захисту". URL: https://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_56_2014_sistemi_protipozhezhnogo_zakhistu/1-1-0-1204. (Дата звернення: 8.06.2025)

13. App.Diagrams сайт для створення схем URL: https://app.diagrams.net. (Дата звернення: 10.06.2025)

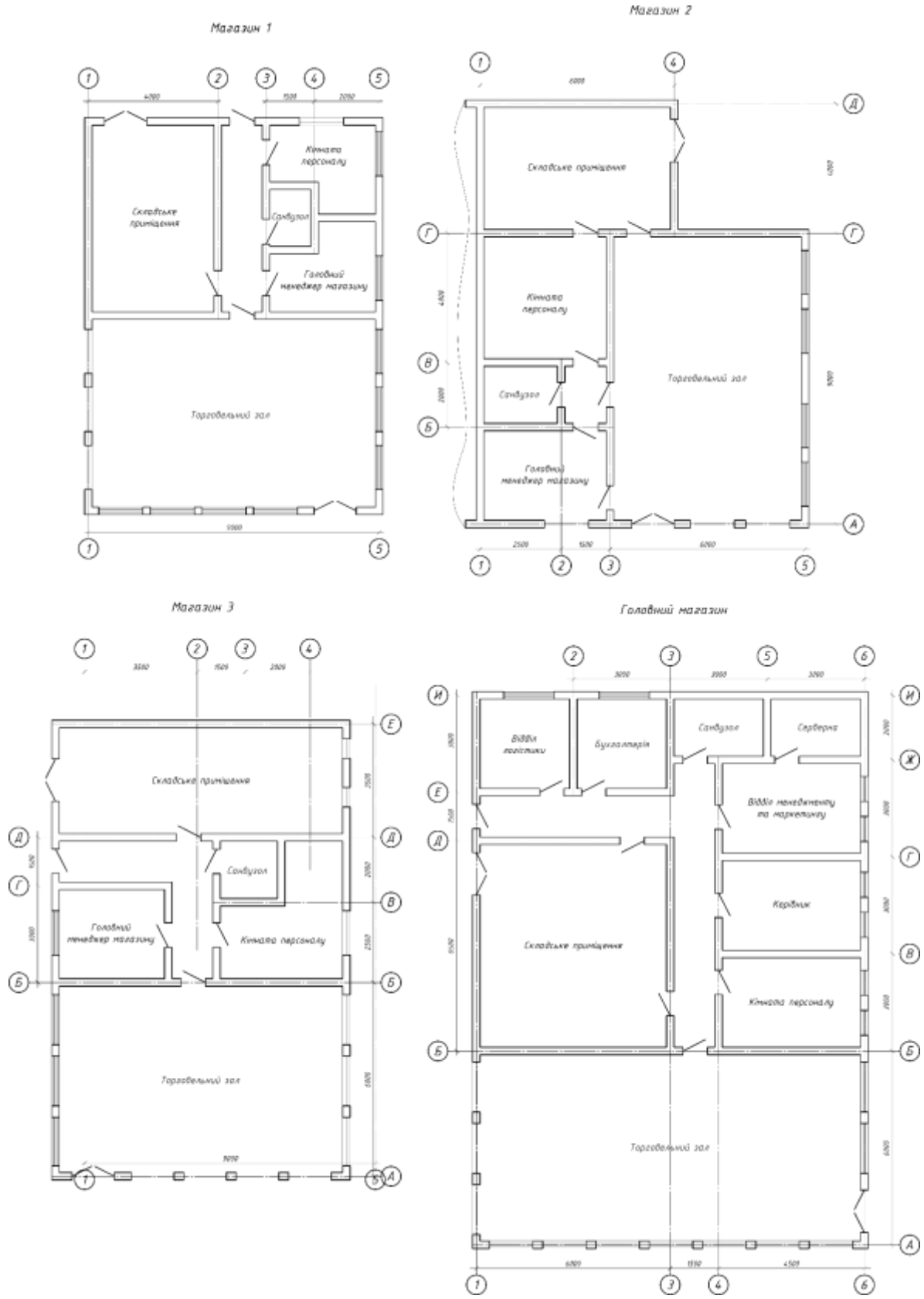
14. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 2.06.2025)

15. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 3.06.2025)

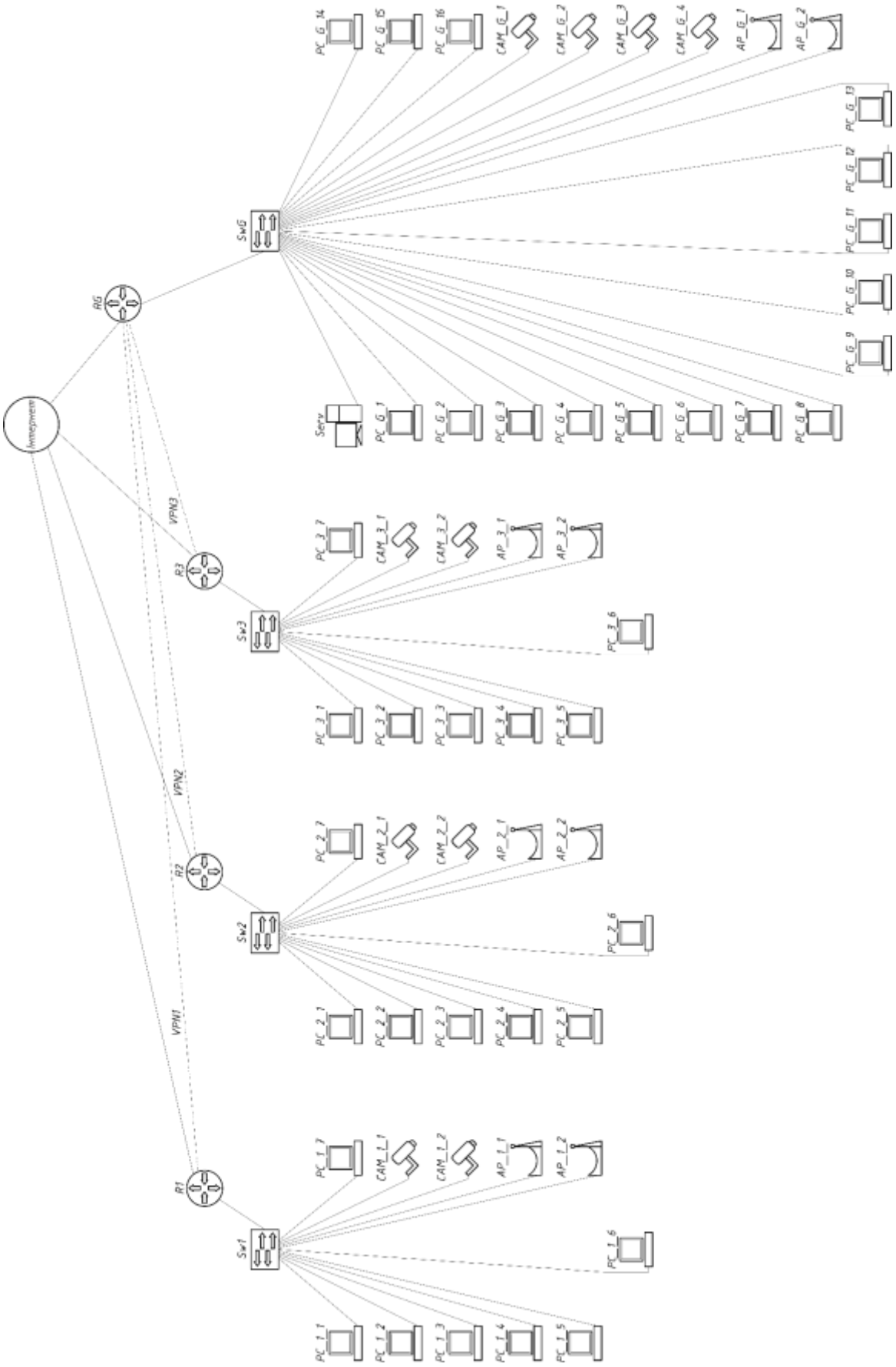
16. Комутатор Cisco WS-C2960L-24PS-LL URL: https://stack-systems.com.ua/kommutator-cisco-ws-c2960l-24ps-ll]

ДОДАТКИ

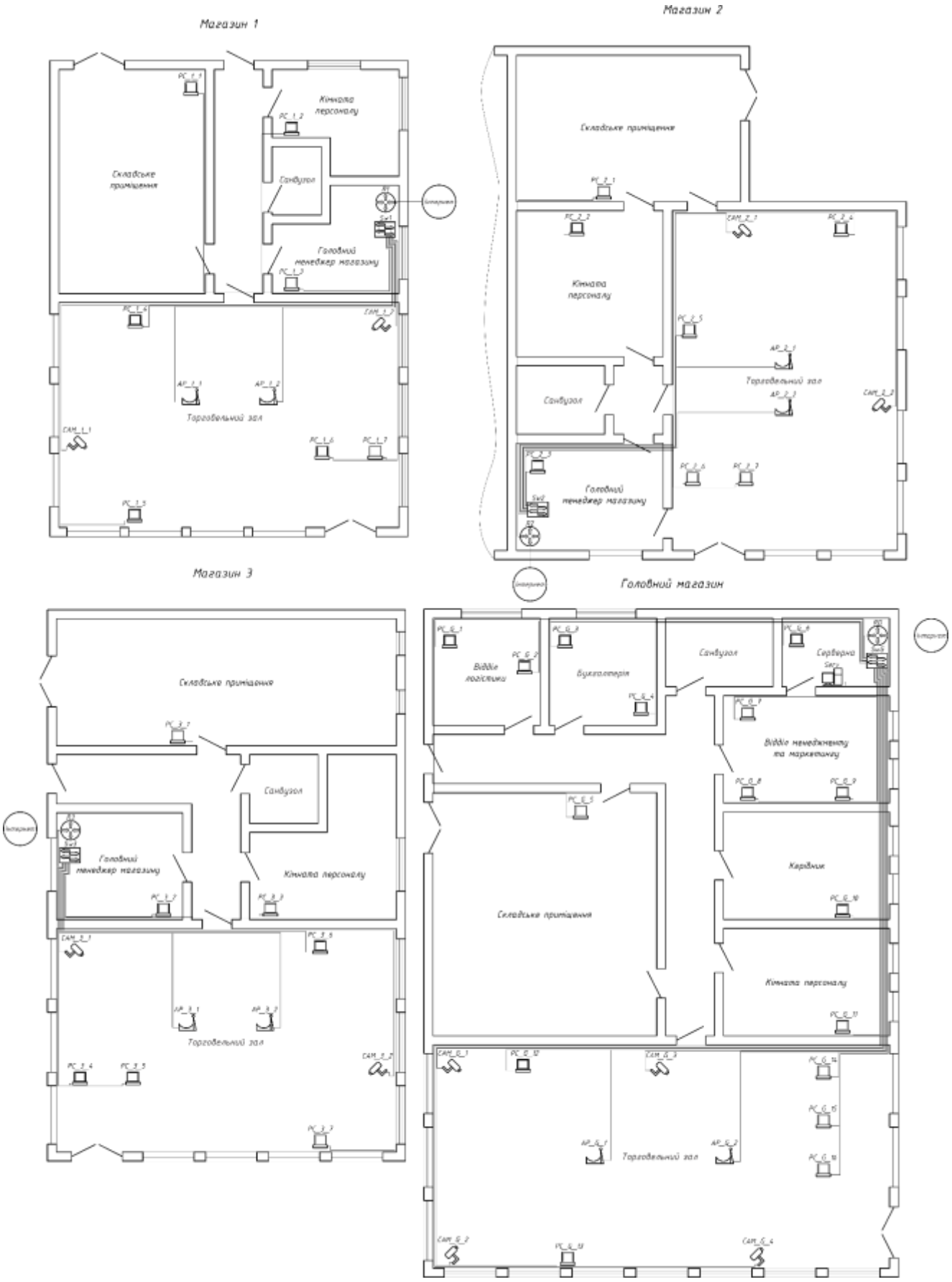
Додаток А. План приміщення будівель ТзОВ "ЕкспертФан "ЧудоОстрів"



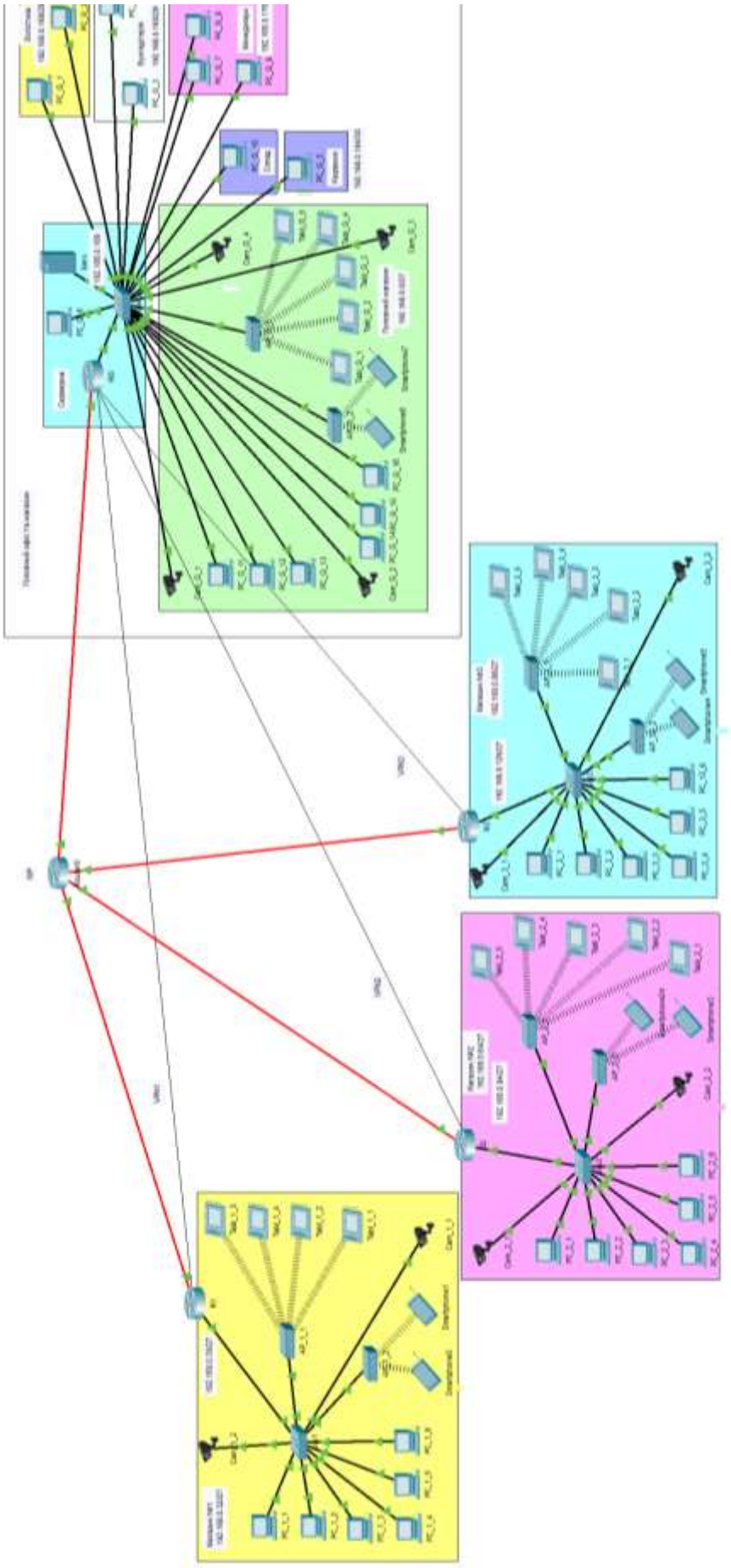
Додаток Б. Логічна топологія мережі ТзОВ "ЕкспертФан "ЧудоОстрів"



Додаток В. Схема прокладання кабелів "ЕкспертФан "ЧудоОстрів"

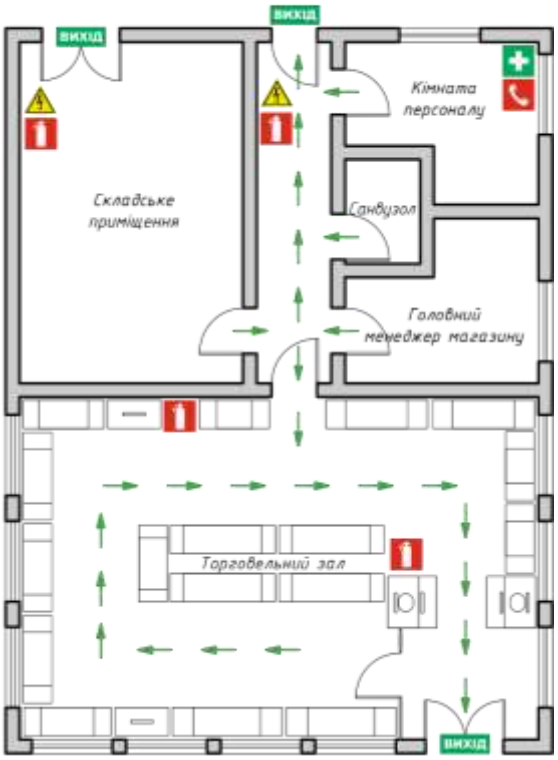


Додаток Г. Модель мережі в Cisco Packet Tracer

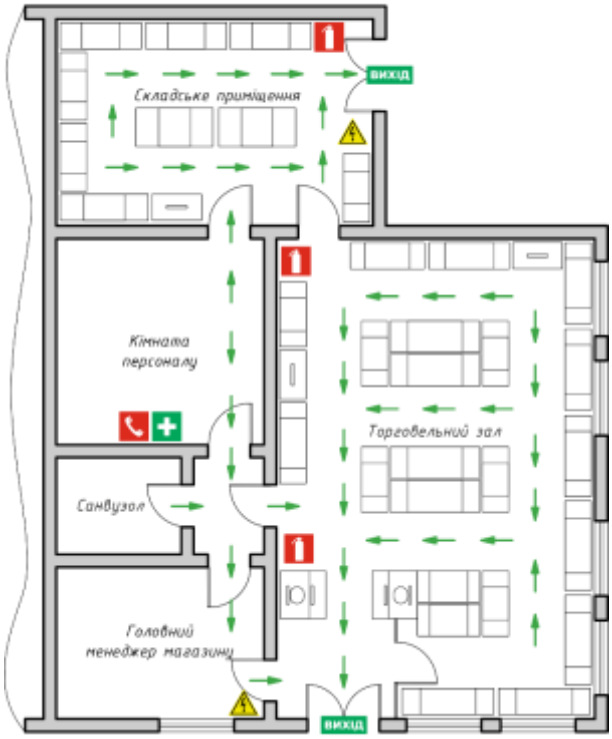


Додаток Д. План евакуації на випадок пожежі

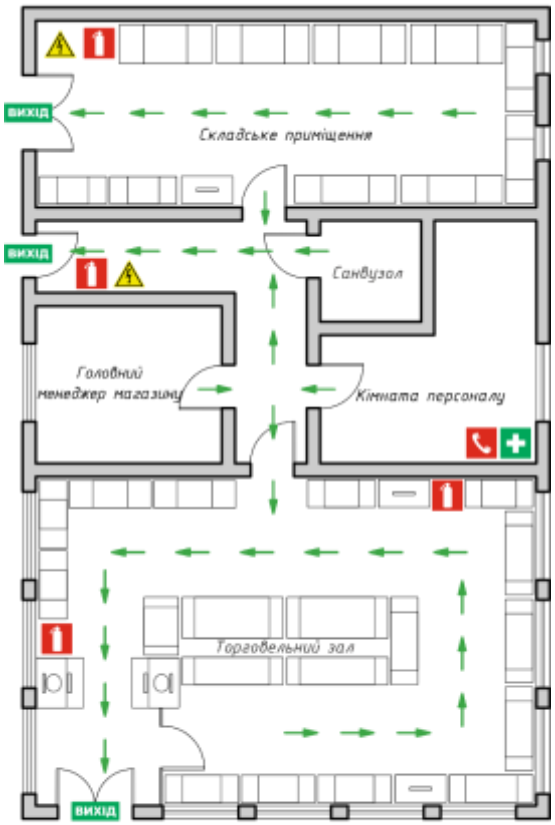
Магазин 1



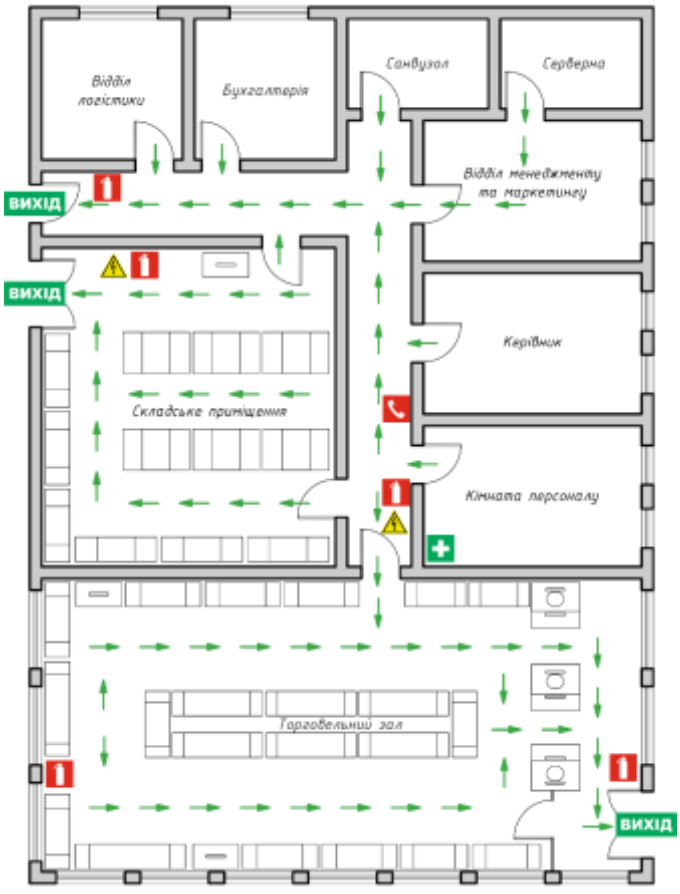
Магазин 2



Магазин 3



Головний магазин



Умовні позначення

- шляхи евакуації
- ВИХІД вихід
- вогнегасник
- телефон
- електричний щит
- аптечка