Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту корпоратвиної комп'ютерної мережі філії агрохолдингу "Контінентал Фармерз Груп" в Тернопільській області**

Виконав: студент VII курсу, групи КІ-703

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

_____ Антон СКОРОМНИЙ
(ім'я та прізвище)

Керівник Андрій ЛЯПАНДРА
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2026

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

Відділення **телекомунікацій та електронних систем**
Циклова комісія **комп'ютерної інженерії**
Освітній ступінь **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
"18" травня 2026 року

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

Скоромному Антону Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту корпоратвиної комп'ютерної мережі філії агрохолдингу "Контінентал Фармерз Груп" в Тернопільській області**

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 18.05.2026р №4/9-252.

2. Строк подання студентом роботи: 22 червня 2026 року.

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

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- 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	Ірина ЛЕЩИК методист, викладач		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	18.05	
2	Збір і узагальнення інформації	21.05	
3	Написання першого розділу	25.05	
4	Розробка технічного та робочого проекту	1.06	
5	Написання спеціального розділу	8.06	
6	Розрахунок економічної частини	11.06	
7	Написання розділу охорони праці	12.06	
8	Виконання графічної частини	14.06	
9	Оформлення проекту	18.06	
10	Погодження нормоконтролю	19.06	
11	Попередній захист роботи	22.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 18 травня 2026 року

Студент _____ Антон СКОРОМНИЙ
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Скоромний А.І. Розробка проєкту корпоратвиної комп'ютерної мережі філії агрохолдингу "Контінентал Фармерз Груп" в Тернопільській області: кваліфікаційна робота на здобуття освітнього ступеня бакалавр за спеціальністю «123 – Комп'ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2026. 109 с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі філії агрохолдингу «Контінентал Фармерз Груп» згідно стандартів та вимог замовника. В проектовані мережі використано сучасні стандарти Gigabit Ethernet IEEE 802.3ab та Ethernet IEEE 802.3q. При цьому реалізовано розподіл мережі на віртуальні підмережі, планування та розподіл адресного простору. Розроблено інструкції з інсталяції та налаштування файлового сервера, фаєрвола, шлюзу доступу до мережі Інтернет, віртуальних підмереж та засобів захисту мережі. Створень віртуальну модель мережі в програмі Packet Tracert.

Ключові слова: комп'ютерна мережа, файловий сервер, FTP, файєрвол, маршрутизатор, комутатор, віртуальна мережа, VLAN, Cisco Packet Tracert

ANNOTATION

Skoromny A.I. Development of a project for a corporate computer network of a branch of the agricultural holding "Continental Farmers Group" in the Ternopil region: qualification work for obtaining a bachelor's degree in the specialty "123 - Computer Engineering". Ternopil: VSP "TFK TNTU", 2026. 109 p.

The qualification work involves the development of a project for a computer network of a branch of the agricultural holding "Continental Farmers Group" in accordance with the standards and requirements of the customer. The designed networks use modern Gigabit Ethernet IEEE 802.3ab 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 file server, firewall, Internet access gateway, virtual subnetworks and network protection tools are developed. Create a virtual network model in Packet Tracert.

Keywords: computer network, file server, FTP, firewall, 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;

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;

ОС – операційна система.

ПК – персональний комп’ютер.

ВСТУП

В умовах стрімкої цифровізації економіки інформаційні технології стають невіддільною складовою успішного функціонування будь-якого великого бізнесу. Сучасний аграрний сектор — це високотехнологічна галузь, яка активно впроваджує системи точного землеробства, ERP-системи для управління ресурсами, GPS-моніторинг техніки та інструменти автоматизованого збору даних з полів. Агрохолдинг «Контінентал Фармерз Груп» є одним із лідерів сільськогосподарського ринку Західної України, що вимагає безперебійної та швидкої обробки значних масивів інформації між центральним офісом, філіями та виробничими підрозділами.

У зв’язку з розширенням та модернізацією філії в Тернопільській області виникає гостра потреба у побудові надійної, масштабованої та безпечної корпоративної комп’ютерної мережі. Застарілі або неоптимізовані мережеві рішення призводять до затримок у передачі даних, вразливості до кібератак та зниження загальної ефективності управління. Тому розробка сучасного проєкту корпоративної мережі, що враховує специфіку географічного розташування об'єктів філії, потреби у пропускній здатності та високі стандарти інформаційної безпеки, є вкрай актуальним завданням.

Мета роботи полягає у розробці оптимального проєкту корпоративної комп’ютерної мережі для філії агрохолдингу «Контінентал Фармерз Груп» у Тернопільській області, що забезпечить високу надійність, безпеку та швидкість обміну даними, необхідними для ефективного управління виробничими процесами.

Запропонований проєкт є готовим технічним рішенням, яке може бути безпосередньо впроваджене у філії агрохолдингу «Контінентал Фармерз Груп» у Тернопільській області. Впровадження проєкту дозволить централізувати управління ІТ-інфраструктурою філії, підвищити рівень захисту комерційної інформації та мінімізувати простої, спричинені технічними збоями..

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Повна назва проєкту: «Проєкт корпоративної комп’ютерної мережі філії агрохолдингу "Контінентал Фармерз Груп" в місті Тернопіль».

Скорочена назва: ККМ філії АХ «КФГ» у м. Тернопіль.

Вид діяльності: проєктування та розгортання локальної та розподіленої мережевої інфраструктури (ланка LAN/WLAN/WAN) із забезпеченням засобів маршрутизації, комутації та мережевої безпеки.

Областю застосування розроблюваного проєкту є інформаційно-комунікаційне середовище регіонального підрозділу (філії) компанії «Контінентал Фармерз Груп» у місті Тернопіль. Проєкт охоплює адміністративні, диспетчерські, логістичні та господарські приміщення філії.

Мережа призначена для забезпечення повсякденної операційної діяльності таких підрозділів підприємства:

- адміністративно-управлінський апарат: забезпечення керівництва та менеджменту доступом до засобів аналітики, корпоративної пошти та систем планування;
- бухгалтерія та фінансовий відділ: організація захищеного доступу до сервісів електронного документообігу, баз даних 1С/ERP та систем клієнт-банк;
- логістична служба та диспетчерський центр: координація руху автотранспорту, моніторинг переміщення техніки в реальному часі, облік паливно-мастильних матеріалів та зібраного врожаю;
- агрономічна служба: опрацювання даних супутникового моніторингу полів, геоінформаційних систем (ГІС), даних з метеостанцій та систем точного землеробства.

- IT-служба та технічна підтримка: централізоване керування мережевими ресурсами, моніторинг стану обладнання та забезпечення інформаційної безпеки.

Розроблена комп'ютерна мережа інтегрується у загальну корпоративну структуру агрохолдингу. Вона забезпечує стабільну взаємодію локальних користувачів із центральним дата-центром компанії, хмарними сховищами даних, внутрішніми серверами та зовнішніми веб-ресурсами. Проєкт розрахований на використання як у штатному режимі повсякденної роботи, так і в умовах підвищеного навантаження під час сезонних польових робіт (посівна та збиральна кампанії).

1.1.2 Призначення розробки

Призначення розроблюваної корпоративної комп’ютерної мережі полягає у створенні сучасної, високошвидкісної та відмовостійкої інформаційно-комунікаційної інфраструктури для тернопільської філії агрохолдингу «Контінентал Фармерз Груп». Розробка покликана об'єднати всі апаратні та програмні ресурси підрозділу в єдиний безпечний простір.

Призначення проєкту доцільно розділити на два ключові напрями: функціональне (технічне) та експлуатаційне (практичне).

З технічного погляду розробка призначена для виконання таких завдань:

- організація локальних каналів зв'язку з високою пропускною здатністю для передачі великих масивів інформації (бази даних, геоінформаційні карти, медіафайли систем відеоспостереження);

- створення ізольованих віртуальних локальних мереж (VLAN) для різних відділів філії (адміністрація, бухгалтерія, агрономи, логісти) з метою оптимізації трафіку та підвищення безпеки;

- налаштування захищених каналів зв'язку (VPN-тунелів) для інтеграції філії в загальну розподілену мережу агрохолдингу та забезпечення доступу до хмарних сервісів і головного дата-центру;

- розгортання та розподіл функцій серверів для автоматизації видачі IP-адрес (DHCP), трансляції мережевих адрес (NAT), вирішення імен (DNS) та керування правами доступу;

- організація захищеної корпоративної мережі Wi-Fi для мобільних пристроїв співробітників (ноутбуків, планшетів, терміналів збору даних) та окремої ізольованої гостьової зони.

З погляду організації бізнес-процесів агрохолдингу, розробка призначена для:

- мінімізації ризиків простою підрозділів філії завдяки резервуванню ліній зв'язку та використанню надійного комунікаційного обладнання. Це вкрай важливо під час сезонних польових робіт, коли затримки в отриманні даних неприпустимі;

- запобігання несанкціонованому доступу до внутрішніх ресурсів філії, захист фінансової документації, інформації про врожайність, логістичні маршрути та кадровий склад від зовнішніх кібератак та внутрішніх витоків;

- створення такої архітектури мережі, яка дозволить оперативно підключати нові робочі місця, обладнання чи додаткові сервіси (наприклад, нові системи телеметрії чи датчики інтернету речей IoT на складах) без зупинки роботи наявної мережі та значних капіталовкладень;

- зниження витрат на адміністрування та технічну підтримку мережі за рахунок вибору збалансованого за критерієм «ціна/якість» обладнання, впровадження інструментів віддаленого моніторингу та спрощення схем комутації.

1.1.3 Вимоги до апаратного і програмного забезпечення

Цей розділ визначає базові вимоги до технічних та програмних засобів, які будуть використані під час реалізації проєкту корпоративної комп’ютерної мережі (ККМ) філії агрохолдингу «Контінентал Фармерз Груп».

Дотримання цих вимог гарантує сумісність обладнання, належну швидкість передачі даних та стійкість системи до відмов.

Апаратний комплекс мережі повинен забезпечувати цілодобове функціонування корпоративних сервісів, мати запас продуктивності для майбутнього розширення філії та підтримувати сучасні стандарти зв'язку.

Активне мережеве обладнання мережі передбачає наявність в структурі мережі маршрутизатора, комутаторів рівня ядра і розподілу та серврне обладнання.

Вимоги до маршрутизатора:

- наявність не менше двох WAN-портів зі швидкістю до 1 Гбіт/с для організації основного та резервного каналів зв'язку від різних провайдерів;
- апаратна підтримка шифрування для створення захищених VPN-тунелів (IPsec, OpenVPN, WireGuard) із центральним офісом агрохолдингу;
- продуктивність міжмережевого екрана (Firewall Throughput) не менше 1,5 Гбіт/с.

Вимоги до головного комутатора ядра мережі:

- наявність портів SFP/SFP+ (10 Гбіт/с) для швидкісного підключення серверів та магістральних каналів до комутаторів робочих груп;
- підтримка функцій керування рівня L2+/L3 (статична маршрутизація, агрегація каналів LACP, дзеркалювання портів).

Вимоги до комутаторів робочих груп:

- порти доступу: 10/100/1000 Base-T (Gigabit Ethernet);
- обов'язкова підтримка технології Power over Ethernet (PoE/PoE+) на частині портів для живлення камер відеоспостереження та бездротових точок доступу;
- підтримка стандарту 802.1Q для реалізації віртуальних мереж (VLAN).

Вимоги до серверної платформи:

- архітектура x86-64 з підтримкою апаратної віртуалізації;
- оперативна пам'ять (RAM): об'єм від 64 ГБ із функцією виправлення помилок (ECC);

- дискова підсистема: побудова RAID-масивів (RAID 1, RAID 10 або RAID 5) на базі швидкісних SSD (NVMe/SAS) для операційної системи та баз даних;

- наявність двох резервних блоків живлення з можливістю «гарячої» заміни (Hot-Swap).

Пасивне мережеве обладнання та структурована кабельна система (СКС) повинні відповідати наступним вимогам:

- кабельна інфраструктура: використання неекранованої (UTP) або екранованої (FTP) крученої пари категорії не нижче Cat 5e (передача даних до 1 Гбіт/с) або Cat 6 (до 10 Гбіт/с на коротких відстанях);

- комутаційні шафи: встановлення стандартних 19-дюймових телекомунікаційних шаф із замком для обмеження фізичного доступу сторонніх осіб та обладнаних блоками вентиляторів;

- гарантоване живлення: обов'язкове встановлення джерел безперебійного живлення з лінійно-інтерактивною або On-line архітектурою для захисту серверів та комутаційного вузла від перепадів напруги, із можливістю автономної роботи обладнання щонайменше 30–40 хвилин.

Програмне забезпечення мережі має бути ліцензійним (або розповсюджуватися за вільними ліцензіями типу GNU GPL), стабільним, мати регулярні оновлення безпеки та забезпечувати зручність адміністрування. Загальні вимоги до програмного забезпечення представлені в таблиці 1.1.

Таблиця 1.1 – Вимоги до програмного забезпечення проектованої мережі

Категорія ПЗ	Основні вимоги та характеристики	Приклади / Орієнтири
1	2	3
Мережеві ОС	Стабільність, підтримка сучасних мережевих протоколів (IPv4, IPv6, OSPF, BGP), наявність консолі керування (CLI) та веб-інтерфейсу.	Cisco IOS, MikroTik RouterOS, VyOS

Продовження таблиці 1.1

1	2	3
Платформи віртуалізації (Гіпервізори)	Ефективний розподіл апаратних ресурсів сервера, підтримка «знімків» (snapshots) стану систем, легке резервне копіювання.	Proxmox VE, VMware vSphere (ESXi)
Серверні ОС	Підтримка багатокористувацького режиму, висока безпека, сумісність із корпоратив-ним ПЗ (ERP, ГІС-системи, бази даних).	Windows Serverser, Ubuntu Serverser, Debian
Мережеві сервіси та служби	Автоматична та безвідмовна робота служб IP-адресації (DHCP), керування іменами (DNS), служби каталогів для авторизації користувачів.	Active Direcory (Samba4 / Windows), ISC DHCP, BIND
Моніторинг та безпека	Відстеження стану ліній зв’язку та навантаження пристроїв у реальному часі, сповіщення про аварії, антивірусний захист, логування подій.	Zabbix, Nagios, системи Syslog, міжмережеві екрани

Робочі станції користувачів філії повинні працювати під управлінням актуальних операційних систем (Windows 10/11, дистрибутиви Linux), мати встановлені клієнтські модулі для підключення до домену, антивірусний захист із централізованим керуванням та необхідне прикладне програмне забезпечення (браузери, офісні пакети, клієнти ERP та ГІС).

1.1.4 Вимоги до документації

Розроблювана проєктна та експлуатаційна документація для корпоратив-ної комп’ютерної мережі філії агрохолдингу «Контінентал Фармерз Груп»

повинна бути виконана у чіткій відповідності до чинних державних стандартів України (ДСТУ), нормативних документів галузі зв'язку та внутрішніх регламентів компанії.

Документація призначена для забезпечення якісного проведення монтажних робіт, подальшого обслуговування, адміністрування та можливого розширення мережі в майбутньому.

Готовий технічний проєкт повинен містити три основні блоки документів: проєктно-конструкторська, експлуатаційна документація та документація для кінцевих користувачів.

Проєктно-конструкторська (технічна) документація:

- пояснювальна записка – опис архітектурних та логічних рішень, обґрунтування вибору активного й пасивного обладнання, розрахунок адресного простору;

- структурна схема мережі – відображення взаємозв'язків між серверами, комутатором ядра, комутаторами робочих груп та маршрутизатором.

- схема фізичного розташування – плани приміщень філії із нанесеними трасами прокладання кабелів, точками розташування комутаційних шаф та розеток користувачів;

- кабельний журнал – таблиця із переліком усіх кабельних ліній, їхніх типів, довжини, маркування та точок підключення.

Експлуатаційна документація (для IT-спеціалістів та адміністраторів):

- інструкція системного адміністратора: детальні покрокові керівництва з конфігурування обладнання (налаштування VLAN, інтерфейсів маршрутизації, правил міжмережевого екрана);

- схема розподілу IP-адрес та VLAN – таблиця з чітким закріпленням адресних просторів за підрозділами філії та мережевими службами;

- регламент резервного копіювання – інструкція з налаштування та періодичності створення бекапів конфігурацій обладнання та серверних даних.

Документація для кінцевих користувачів:

- інструкція користувача – правила підключення до корпоративної мережі (зокрема через Wi-Fi або VPN для віддалених працівників).

- пам'ятка з інформаційної безпеки – перелік правил дотримання парольної політики та поводження з підозрілими повідомленнями чи файлами.

Текстова частина має бути надана у форматах .docx (чи .pdf), графічні схеми та креслення – у векторних форматах (.vsdx для MS Visio, або формати CAD-систем), а файли моделювання – у форматі відповідного симулятора (наприклад, .pkt для Cisco Packet Tracer).

За потреби графічні схеми повинні бути роздруковані на аркушах стандартних форматів (А4, А3) із дотриманням масштабу та використанням стандартних умовних позначень мережевих елементів;

Усі документи виконуються державною (українською) мовою. Допускається використання загальноприйнятих англомовних термінів та абревіатур у сфері IT (наприклад, VLAN, DHCP, IPsec) без їхнього обов'язкового перекладу, якщо це спрощує розуміння технічного тексту.

1.1.5 Техніко-економічні показники

Проєкт мережі має відповідати таким технічним метрикам продуктивності та надійності:

- коефіцієнт готовності – не нижче ніж 99,9% для магістральних каналів зв'язку та серверної інфраструктури (що допускає сумарний простій системи не більше 8–9 годин на рік, за винятком планового технічного обслуговування);

- пропускна здатність на рівні доступу (робочі місця користувачів) до 1 Гбіт/с;

- пропускна здатність на рівні ядра (магістральні канали, підключення серверів) до 10 Гбіт/с;

- пропускна здатність зовнішніх каналів зв'язку (Інтернет) не менше 100 Мбіт/с із можливістю динамічного розширення;

- час перемикання на резервний канал (Failover): в автоматичному режимі у разі відмови основного провайдера чи маршрутизатора – не більше 10–15 секунд;

Архітектура мережі повинна передбачати резерв ємності комутаційного обладнання та структурованої кабельної системи на рівні 20–30% без потреби заміни основних вузлів.

Економічна доцільність впровадження проєкту обґрунтовується оптимізацією витрат та зменшенням ризиків для бізнес-процесів агрохолдингу.

Оптимізація капітальних витрат досягається шляхом раціонального вибору вендорів обладнання (наприклад, поєднання рішень комерційного сегменту для ядра та продуктивного обладнання середнього цінового діапазону для робочих груп).

Впровадження централізованого моніторингу та автоматизації мережевих служб (DHCP, DNS, Active Direcory) дозволить зменшити трудовитрати на адміністрування мережі, мінімізуючи потребу у великому штаті місцевих IT-фахівців.

Згідно з вимогами до інвестиційних проєктів компанії, розрахований термін окупності за рахунок підвищення продуктивності праці та автоматизації логістики не повинен перевищувати 2–3 роки.

1.1.6 Стадії та етапи розробки

Процес проєктування, моделювання та подальшого розгортання корпоративної комп’ютерної мережі філії агрохолдингу «Контінентал Фармерз Груп» у місті Тернопіль базується на системному підході та реалізується у чіткій послідовності відповідно до вимог чинних нормативних стандартів, що регламентують життєвий цикл автоматизованих систем та інформаційних технологій.

Дотримання поетапності розробки дозволяє мінімізувати інженерні ризики, раціонально розподілити ресурси, забезпечити повну сумісність

апаратних і програмних компонентів, а також гарантувати відповідність створюваної інфраструктури специфічним вимогам сучасного агробізнесу.

Весь комплекс робіт у межах цієї кваліфікаційної роботи поділяється на кілька логічно пов'язаних стадій, кожна з яких є базою для виконання наступних кроків і має свій чітко визначений технічний результат.

Першою стадією є передпроєктне обстеження та аналіз вихідних даних, що починається з детального вивчення організаційної і штатної структури тернопільської філії компанії. На цьому етапі збирається інформація про кількість робочих місць, розташування адміністративних, логістичних та господарських підрозділів, а також аналізуються архітектурні плани та лінійні розміри приміщень, де буде розгортатися мережа.

Особлива увага приділяється дослідженню існуючих інформаційних потоків, специфіці використання корпоративного програмного забезпечення, обсягам трафіку від систем точного землеробства та телеметрії, а також вимогам до швидкості обміну даними та рівня захищеності комерційної таємниці.

Підсумком цієї стадії є формування концепції майбутньої мережі та розробка технічного завдання, яке фіксує всі архітектурні, технічні, програмні та експлуатаційні вимоги до проєкту.

Друга стадія охоплює безпосереднє технічне та робоче проєктування, яке становить інженерну основу дослідження. На цьому етапі здійснюється обґрунтування логічної топології корпоративної мережі та вибір архітектури побудови структурованої кабельної системи.

Інженерні розрахунки включають розробку схем фізичного розміщення кабельних трас, визначення оптимальних місць для монтажу телекомунікаційних шаф, комутаційних вузлів, розеточних модулів та точок бездротового доступу Wi-Fi з урахуванням мінімізації довжини ліній зв'язку та захисту від завад.

Паралельно виконується розрахунок та оптимізація адресного простору мережевих вузлів, планується логічна сегментація мережі на віртуальні

локальні підмережі (VLAN) для ізоляції трафіку окремих відділів, а також формується детальна специфікація активного й пасивного обладнання, серверних платформ і систем безперебійного живлення.

Третя стадія присвячена програмно-налагоджувальному забезпеченню та комп'ютерному моделюванню розробленої мережевої архітектури. Оскільки впровадження фізичного обладнання потребує попередньої перевірки, у роботі реалізується етап імітаційного моделювання у спеціалізованому програмному середовищі.

На цій стадії створюється віртуальний прототип мережі тернопільської філії, де програмуються конфігурації маршрутизаторів, головного комутатора та комутаторів робочих груп. Тут же розробляються та тестуються інструкції з налаштування маршрутизації між віртуальними мережами, правила списків контролю доступу (ACL) для міжмережевого екранування, а також алгоритми динамічної видачі адрес та вирішення мережевих імен.

Віртуальне тестування побудованої моделі дозволяє оцінити стійкість мережі до відмов у разі імітації обривів магістральних каналів зв'язку та перевірити коректність роботи всіх мережевих служб до початку закупівлі реальної техніки.

Заключна стадія розробки проєкту включає економічний аналіз та визначення регламентів введення системи в експлуатацію. На етапі економічних розрахунків здійснюється калькуляція капітальних витрат на придбання обладнання, матеріалів структурованої кабельної системи та ліцензій на програмне забезпечення, а також оцінюються операційні витрати на подальше адміністрування та технічну підтримку. Обчислюються показники ефективності проєкту, включаючи термін окупності інвестицій для агрохолдингу за рахунок мінімізації простоїв та підвищення продуктивності праці.

Окремо формується план перспективного впровадження, який описує послідовність монтажних і пусконалагоджувальних робіт, методику проведення підсумкових приймальних випробувань на відповідність вимогам

технічного завдання та порядок передачі повного пакету експлуатаційної документації системним адміністраторам підприємства.

1.1.7 Порядок контролю та прийому

Порядок контролю та прийому розроблюваного проєкту корпоративної комп'ютерної мережі філії агрохолдингу «Контінентал Фармерз Груп» визначає регламент перевірки якості виконаних інженерних рішень, оцінки їхньої відповідності вимогам технічного завдання, а також процедуру передачі готової системи в промислову експлуатацію.

Цей етап спрямований на виявлення можливих помилок, перевірку надійності функціонування мережевих сервісів та підтвердження готовності інфраструктури до забезпечення безперебійного виконання бізнес-процесів підприємства.

Весь процес контролю та прийому поділяється на кілька послідовних стадій, які включають внутрішній аудит документації, інструментальне тестування фізичних ліній, програмну валідацію сервісів та фінальне підписання актів приймання-передачі.

На першій стадії здійснюється документальний та теоретичний контроль, який полягає у перевірці повноти, коректності та відповідності розроблених текстових і графічних матеріалів чинним державним стандартам України та внутрішнім регламентам агрохолдингу.

На цьому етапі технічні керівники IT-департаменту компанії та науковий керівник роботи аналізують пояснювальну записку, структурні та фізичні схеми, кабельний журнал та інструкції з налаштування обладнання. Особлива увага приділяється перевірці коректності розрахунку адресного простору, схем сегментації віртуальних мереж (VLAN) та правил безпеки міжмережевих екранів.

Одночасно проводиться оцінка результатів комп'ютерного моделювання у спеціалізованому середовищі, де аналізуються звіти про проходження тестових пакетів та поведінку моделі в умовах імітації відмов магістральних каналів зв'язку.

Друга стадія передбачає проведення інструментального та технічного контролю безпосередньо після завершення монтажу структурованої кабельної системи на об'єкті філії в місті Тернопіль.

Усі змонтовані кабельні лінії (кручена пара, оптичні магістралі) підлягають обов’язковому сертифікаційному тестуванню за допомогою спеціалізованих кабельних аналізаторів. Під час цього етапу вимірюються такі параметри, як довжина кожної лінії, рівень загасання сигналу, перехресні наводки на ближньому кінці та опір провідників. Кожна розетка та порт патч-панелі повинні пройти перевірку на відповідність категорії кабельної системи (не нижче Cat 5e/Cat 6).

Результати тестування фіксуються в автоматично згенерованих звітах приладів, які додаються до виконавчої документації, а лінії, що не пройшли тест, підлягають обов'язковому перемонтажу та повторній перевірці.

На третій стадії виконується пусконалагоджувальний та функціональний контроль активного мережевого обладнання та серверних служб. Після завантаження розроблених конфігураційних скриптів на маршрутизатори та комутатори проводиться комплексне тестування мережі в робочих режимах. Перевіряється коректність динамічного розподілу IP-адрес службою DHCP, швидкість вирішення імен сервером DNS, а також доступність корпоративних ресурсів та баз даних для різних категорій користувачів відповідно до налаштованих списків доступу (ACL).

Окремо тестується надійність захищених VPN-тунелів із центральним дата-центром агрохолдингу, зона покриття та стабільність бездротової мережі Wi-Fi, а також працездатність системи моніторингу, яка має миттєво фіксувати відхилення параметрів роботи обладнання від норми.

Прикінцева стадія прийому проєкту полягає у проведенні комплексних приймально-здавальних випробувань за участю спільної комісії, до складу якої входять представники розробника, IT-директор агрохолдингу, системні адміністратори філії та фахівці з інформаційної безпеки.

Комісія оцінює роботу мережі за умов максимального навантаження, перевіряє швидкість автоматичного перемикання на резервні канали зв'язку у разі імітації аварії та контролює наявність повного комплекту експлуатаційних інструкцій для персоналу.

За відсутності зауважень або після усунення всіх виявлених недоліків складається та підписується двосторонній акт приймання-передачі виконаних робіт, що є офіційною підставою для введення корпоративної комп’ютерної мережі тернопільської філії в промислову експлуатацію.

1.2 Опис задачі та характеристика філії агрохолдингу «Контінентал Фармерз Груп» в місті Тернопіль

Агрохолдинг «Контінентал Фармерз Груп» є одним із провідних сільськогосподарських підприємств України з іноземними інвестиціями, утвореним у результаті об'єднання активів компаній «Мрія Агрохолдинг» та Continental Farmers Group за підтримки міжнародного інвестора SALIC. Компанія обробляє близько 195 тисяч гектарів земельного банку на території Тернопільської, Львівської, Хмельницької, Чернівецької та Івано-Франківської областей.

Виробничі потужності холдингу включають сучасні елеваторні комплекси, насіннєві та крохмальні заводи, а також великий парк сільськогосподарської техніки. Специфіка діяльності підприємства охоплює вирощування зернових, олійних та технічних культур, а також масштабне виробництво картоплі.

Філія компанії у місті Тернопіль, де безпосередньо розташований центральний офіс холдингу, відіграє роль головного адміністративного, координаційного та логістичного хабу. Саме звідси здійснюється управління

всіма виробничими кластерами, планування агрономічних операцій, контроль за переміщенням техніки та збутом продукції.

У тернопільському підрозділі зосереджені ключові департаменти компанії: топ-менеджмент, фінансова та бухгалтерська служби, відділ логістики, служба точного землеробства, центр диспетчеризації та IT-департамент. Ефективна взаємодія між цими відділами, а також їхня комунікація з віддаленими виробничими базами, вимагає наявності потужної інформаційно-комунікаційної інфраструктури.

Управління сучасним агробізнесом базується на технологіях точного землеробства та безперервній обробці великих масивів даних. Працівники тернопільської філії щоденно працюють із геоінформаційними системами (ГІС), аналізують супутникові знімки полів, отримують телеметричні дані з GPS-трекерів, встановлених на тракторах і комбайнах, та використовують ресурсомісткі корпоративні ERP-системи для обліку фінансів і матеріально-технічних ресурсів. Крім того, диспетчерський центр здійснює постійний відеомоніторинг віддалених об'єктів інфраструктури. Усі ці процеси генерують щільний інформаційний трафік, який потребує високої пропускної здатності каналів зв'язку та мінімальних затримок під час передачі даних.

Опис задачі в межах даної кваліфікаційної роботи полягає у розробці повноцінного проєкту сучасної корпоративної комп’ютерної мережі для забезпечення повсякденної операційної діяльності тернопільської філії. Наявна мережева інфраструктура потребує модернізації з огляду на зростання кількості персоналу та впровадження нових цифрових сервісів у процеси вирощування і логістики.

Головне завдання проєкту полягає у створенні надійного середовища, яке об'єднає робочі станції працівників, серверне обладнання, периферійні пристрої та засоби бездротового доступу в єдину керовану систему з високим рівнем відмовостійкості.

Технічна реалізація поставленої задачі передбачає проєктування структурованої кабельної системи з урахуванням архітектурних особливостей

офісних приміщень, вибір продуктивного комутаційного обладнання та організацію логічного розділення мережі.

З метою забезпечення інформаційної безпеки та оптимізації навантаження на обладнання, необхідно розробити детальну схему сегментації трафіку за допомогою віртуальних локальних мереж (VLAN). Це дозволить ізолювати фінансові дані бухгалтерії від загального трафіку диспетчерів чи гостьової зони Wi-Fi.

Окрім того, задача включає налаштування засобів маршрутизації для стабільного зв'язку із зовнішніми хмарними сервісами та розробку політик доступу, які унеможливлять несанкціоноване втручання в роботу інформаційної системи підприємства.

Філія агрохолдингу «Контінентал Фармерз Груп» у місті Тернопіль структурно поділене на підрозділи вищого менеджменту (керівництво підприємства), виробничий, комерційний, фінансово-економічний та адміністративний підрозділи. Загалом на підприємстві працює 135 осіб, із них робота 45 працівників безпосередньо пов’язана із регулярним використанням комп’ютерної техніки та мережевих ресурсів.

До керівництва підприємства Філія агрохолдингу «Контінентал Фармерз Груп» входять директор, секретар керівника та чотири профільні заступники.

Директор здійснює генеральне керівництво підприємством, забезпечує стратегічний розвиток та взаємодію із зовнішніми партнерами, при цьому в його кабінеті розташовано 1 персональний комп’ютер.

Секретар керівника виконує функції адміністративної підтримки, і на його робочому місці також розташовано 1 ПК. Заступник директора з виробництва здійснює безпосередній нагляд за виробничими процесами холдингу та його технічною базою, у кабінеті якого розташовано 1 вузол, що необхідно об’єднати в загальну мережу.

Заступник директора з комерційних питань, який здійснює нагляд за продажами, логістикою та закупівлями, заступник директора з фінансових питань, який контролює фінансову діяльність та облік, а також заступник

директора з персоналу та безпеки, що координує кадри, охорону праці та внутрішню безпеку, не мають окремих персональних комп'ютерів у своїх кабінетах і працюють безпосередньо через підпорядковані їм профільні відділи.

Виробничий підрозділ підпорядковується заступнику директора з виробництва і поділений на три основні структури. Першою є виробничий відділ та диспетчерська, куди входять керівник виробничого відділу, диспетчери та оператори оперативного обліку, які забезпечують постійний моніторинг агротехнологічних операцій, і всього у цьому відділі встановлено 4 ПК. Другим є агрономічний відділ, що складається із головного агронома та агрономів, які працюють із картами полів та системами точного землеробства, використовуючи для цього 3 ПК.

Третім у цій структурі є інженерно-техничний відділ, до якого належать посади головного інженера, інженерів та технічних спеціалістів, котрі мають у своєму розпорядженні 4 ПК.

Комерційний відділ підпорядковується заступнику директора з комерційних питань і складається із трьох великих підрозділів. Відділ продажів включає посади керівника відділу продажів та менеджерів з продажів, які забезпечують реалізацію вирощеної сільськогосподарської продукції, маючи для цього 11 комп’ютерів.

Відділ логістики складається з керівника відділу логістики, логістів та фахівців з транспортування та складського обліку, які координують рух техніки холдингу, і всього у відділі експлуатується 10 ПК.

Відділ закупівель та постачання включає керівника відділу закупівель, фахівців із закупівель та спеціалістів з постачання ТМЦ, які використовують у своїй роботі 3 ПК.

Фінансово-економічний підрозділ підпорядковується заступнику директора з фінансових питань і складається з бухгалтерії. До її складу входять головний бухгалтер, бухгалтери за основними ділянками, такими як

розрахунки, заробітна плата, облік основних засобів, а також касир, а всього в приміщенні бухгалтерії розташовано 5 комп’ютерів.

Адміністративний підрозділ підпорядковується напряму директору і складається із відділу кадрів та охорони праці. У відділі кадрів працюють керівник відділу кадрів та спеціалісти з кадрів, крім цього у цей підрозділ входить спеціаліст з охорони праці, а всього в адміністративному підрозділі розташовано 3 комп’ютери.

Всього на підприємстві встановлено 45 комп’ютерів, які необхідно об’єднати в єдину корпоративну мережу філії. Перілк кількості вузлів, що необхідно об’єднати в мережу представлено у таблиці 1.2.

Таблиця 1.2 – Розподіл комп'ютерного обладнання по підрозділах філії

Назва підрозділу та його внутрішніх відділів	Кількість ПК (вузлів)
Керівництво підприємства	
Кабінет директора	1
Секретар керівника	1
Заступник директора з виробництва	1
Виробничий підрозділ	
Виробничий відділ / диспетчерська	4
Агрономічний відділ	3
Інженерно-технічний відділ	4
Комерційний підрозділ	
Відділ продажів	11
Відділ логістики	10
Відділ закупівель та постачання	3
Фінансово-економічний підрозділ	
Бухгалтерія	5
Адміністративний підрозділ	
Відділ кадрів та охорони праці	3
Всього пристроїв для підключення	45

Для централізованого зберігання даних в проектованій мережі слід передбачити використання виділеного файлового сервера. Даний сервер повинен здійснювати довготривале та безпечне зберігання комерційної інформації, включаючи бази даних клієнтів, прайс-листи, договори з постачальниками та покупцями, маркетингові матеріали та звіти. Також сервер призначений для надійного збереження фінансової та бухгалтерської інформації, до якої належать бухгалтерські звіти, фінансові плани, платіжні відомості та податкова документація.

Організація спільного доступу до файлів на сервері дозволить співробітникам різних відділів легко отримувати доступ до необхідних документів та оперативно обмінюватися ними, що підвищить загальну ефективність співпраці та повністю усуне необхідність дублювання важливої інформації.

Важливим аспектом проєктування є також організація захищеного мережевого зв'язку між тернопільською філією та головним дата-центром агрохолдингу «Контінентал Фармерз Груп». Для цього в архітектурі мережі необхідно передбачити інтеграцію локальних користувачів із глобальними корпоративними сервісами, такими як хмарні сховища даних, системи корпоративної електронної пошти та сервери IP-телефонії.

Оскільки значна частина інформації, що циркулює між відділами, є комерційною таємницею, мережа філії повинна мати чітко налаштовані шлюзи безпеки. Це дозволить не лише захистити внутрішні ресурси від зовнішніх кібератак, але й гнучко керувати правами доступу, обмежуючи, наприклад, доступ співробітників комерційного відділу чи гостьової зони до фінансових серверів бухгалтерії.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Обґрунтування вибору логічного типу мережі

Ось унікальний, переформульований варіант тексту, який повністю зберігає початковий зміст, професійний стиль та технічні деталі:

У процесі розробки комп'ютерної мережі фундаментальне значення має коректний вибір технології, фізичного середовища передачі даних та топологічної схеми. Від типу топології безпосередньо залежать такі ключові показники, як загальна вартість системи, її продуктивність, здатність до масштабування та стійкість до збоїв. Відповідно до інформації, наведеної у розділах 1.1.3 та 1.1.4, корпоративна мережа філії агрохолдингу «Контінентал Фармерз Груп» будуватиметься з використанням кабельного (дротового) середовища.

Серед базових мережевих архітектур розрізняють шинну, кільцеву, зіркоподібну, деревоподібну та повнозв'язну (завершену).

Шинна топологія (Bus) об'єднує всі пристрої за допомогою єдиного магістрального кабелю. Попри економічність та простоту розгортання для дрібних мереж, ця архітектура є вкрай ненадійною. Будь-яке пошкодження центрального дроту зупиняє роботу всієї системи, а пошук місця аварії ускладнюється тим, що збій може спричинити будь-який підключений вузол. Для філії агрохолдингу «Контінентал Фармерз Груп», зважаючи на велику кількість робочих станцій та критичність бізнес-процесів, такий варіант категорично не підходить через високу вразливість та проблеми з розширенням.

Кільцева топологія (Ring) передбачає послідовне з'єднання обладнання у замкнене коло, де інформація рухається в одному напрямку. Хоча така структура здатна забезпечити хорошу швидкість передачі даних, класичне кільце дуже чутливе до обривів магістралі – одна несправність здатна паралізувати всю мережу. До того ж, підключення чи відключення клієнтів

вимагає зупинки роботи мережі, що є неприпустимим для діючого підприємства.

Топологія «Зірка» базується на підключенні кожного кінцевого пристрою окремим кабелем до центрального вузла — комутатора або концентратора. Це гарантує високу надійність: поломка одного ПК або обрив його кабелю ніяк не впливає на решту користувачів. Такий підхід значно спрощує діагностику мережі та дозволяє легко додавати нові пристрої. Її єдине вразливе місце – повна залежність від працездатності центрального комутатора, відмова якого зупинить весь сегмент. Саме ця архітектура є базою для побудови більш складних систем.

Підсумовуючи, під час проєктування сучасних корпоративних мереж для середнього та великого бізнесу прості топології (шина чи кільце) майже не застосовуються через свої недоліки. Пріоритет віддається більш гнучким ієрархічним моделям, таким як деревоподібна топологія або розширена зірка. Вони є тісно пов'язаними концепціями, побудованими на базі звичайних «зірок».

Розширена зірка є еволюцією базової зіркоподібної структури. Якщо у простій «зірці» всі клієнти підключені до одного комутатора, то в розширеній – головний (кореневий) комутатор з'єднується з комутаторами нижчого рівня (рівня доступу). Вже до цих другорядних пристроїв під'єднуються кінцеві станції, сервери тощо. Таким чином створюється багаторівнева відмовостійка структура, де кожен локальний комутатор утворює власну міні-зірку, інтегровану в загальну мережу підприємства.

Компоненти архітектури розширеної зірки [3]:

- центральний комутатор або ядро мережі – головний вузол усієї системи, до якого сходяться лінії від решти комутаційного обладнання. Його ключове завдання – швидка комутація та агрегація (зведення в єдиний потік) всього мережевого трафіку підприємства;

- комутатори розподілу та рівня доступу – периферійні пристрої, які безпосередньо підключаються до центрального ядра. Саме до них під'єднується

кінцеве обладнання користувачів (робочі станції, сервери, принтери тощо). Залежно від топографії об'єкта, ці комутатори розміщують у різних кабінетах, на окремих поверхах або у сусідніх будівлях, формуючи локальні сегменти мережі для конкретних робочих груп.

До головних переваг цієї архітектури належать [3]:

- високий рівень масштабованості. Архітектура дозволяє безперешкодно нарощувати мережу шляхом підключення нових користувацьких пристроїв або додаткових периферійних комутаторів до існуючої інфраструктури;

- відмовостійкість та локалізація збоїв. Вихід з ладу окремого кабелю чи комп'ютера ніяк не позначається на інших учасниках мережі. У разі поломки комутатора рівня доступу непрацездатним стає лише його локальний сегмент, тоді як решта мережі продовжує функціонувати;

- спрощена діагностика. Завдяки чіткій ієрархії пошук несправностей стає системним. За відсутності зв'язку адміністратор послідовно перевіряє лінію до пристрою, відповідний порт на локальному комутаторі та лінію зв'язку з ядром;

- зручність адміністрування: використання керованого мережевого обладнання забезпечує централізований контроль над трафіком та дає змогу гнучко налаштовувати віртуальні локальні мережі (VLAN).

Серед недоліків варто виділити [3]:

- залежність від ядра. Поломка центрального комутатора призводить до зупинки всієї системи або її більшої частини. У системах з високими вимогами до надійності цю проблему вирішують шляхом апаратного резервування;

- значні витрати на кабельну інфраструктуру. Порівняно з шинною топологією, розгортання «зірки» потребує значно більшої кількості кабелю, адже від кожного кінцевого вузла до комутатора прокладається індивідуальна лінія.

Деревоподібна архітектура є логічним продовженням розширеної зірки, адаптованим для складних корпоративних мереж. Її принцип базується на суворій підпорядкованості: кожен вузол має лише один висхідний канал (до

«батьківського» комутатора), але може обслуговувати безліч низхідних («дочірніх» пристроїв). Це формує структуру, аналогічну дереву.

Фактично, розширена зірка – це дворівневе або трирівневе «дерево». Цей підхід відповідає класичним галузевим стандартам, зокрема ієрархічній моделі мережевого дизайну від Cisco [7].

Додаткові переваги деревоподібної структури [2]:

- чіткий поділ на рівні знижує навантаження на ядро. Локальний трафік обробляється комутаторами доступу, міжсегментний — на рівні розподілу, і лише глобальні запити доходять до ядра;

- ієрархія дозволяє впроваджувати багаторівневі політики захисту, наприклад, списки контролю доступу (ACL) або міжмережеві екрани;

- модернізація або заміна обладнання на одному з рівнів відбувається без впливу на загальну працездатність системи.

Недоліки деревовидної структури [3]:

- складність проєктування: вимагає глибокого аналізу та детального планування багаторівневих зв'язків;

- як і в розширеній зірці, зберігається залежність від кореневого вузла та потреба у великій кількості комутаційного обладнання й кабелю.

Проєктована комп'ютерна мережа для філії агрохолдингу побудована за принципом розширеної зірки, що утворює деревоподібну логічну топологію. Вся інфраструктура чітко розділена на два основні функціональні рівні: ядро мережі, а також рівень розподілу та доступу.

На рівні ядра (Core Layer) головну роль відіграє комутатор SwG, розташований у серверній кімнаті №4а. Цей центральний вузол агрегує трафік з усіх локальних сегментів і забезпечує стабільний зв'язок із корпоративним сервером та маршрутизатором R1.

Рівень розподілу та доступу (Distribution/Access Layer) сформований із шести окремих комутаторів, які безпосередньо підключають робочі станції персоналу відповідно до специфіки та розташування відділів. На першому поверсі будівлі розгорнуто два пристрої. Комутатор Sw1 забезпечує мережею

кабінет директора (№1), приймальню секретаря (№2), заступника директора (№3), інженера з охорони праці (№4) та відділ кадрів (№8). Сусідній комутатор Sw2 об'єднує агрономічний відділ (№7) та відділ закупівель і постачання (№6).

На другому поверсі встановлено ще чотири комутатори для обслуговування решти підрозділів. Пристрій Sw3 виділений суто для відділу продажів (кімната №13). Комутатор Sw4 обслуговує інженерно-технічний відділ (№12) та операторів оперативного обліку (№11). Бухгалтерські служби, зокрема каса (№15), кабінет головного бухгалтера (№9) та загальна бухгалтерія (№10), підключені через комутатор Sw5. Останній пристрій, Sw6, повністю забезпечує роботу відділу логістики у кімнаті №14.

Крім того, проєкт передбачає розгортання бездротового сегмента інфраструктури. У залі для нарад (кімната №5) буде встановлено точку доступу Wi-Fi, яка дозволить організувати ізольований гостьовий доступ для мобільних пристроїв під час проведення зустрічей та презентацій.

Детальну схему спроєктованої топології наведено на рисунку 2.1.

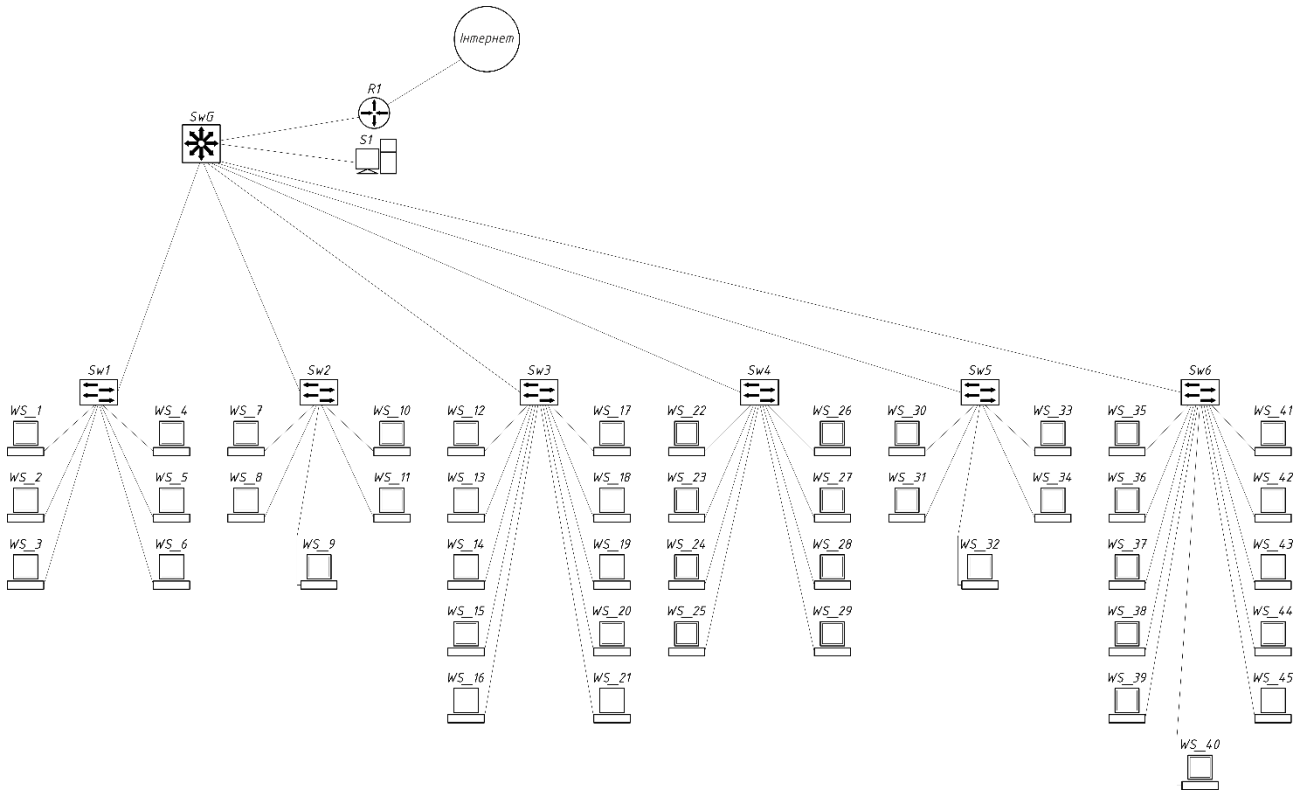

Рисунок 2.1 – Логічна топологія мережі філії агрохолдингу «Контінентал Фармерз Груп»

Для побудови комп'ютерної мережі у філії агрохолдингу «Контінентал Фармерз Груп» було затверджено мережеву технологію Gigabit Ethernet, що базується на стандарті 1000BASE-T. Таке технічне рішення є цілком раціональним, оскільки воно повністю задовольняє теперішні запити підприємства щодо продуктивності, потенціалу для розширення та фінансової доцільності.

Ця технологія розроблялася спеціально для забезпечення гігабітної швидкості передачі інформації через мідну кручену пару категорій 5e або 6 на відстань, що не перевищує 100 метрів. Завдяки помірній вартості розгортання та сумісності з типовими кабельними системами, цей стандарт став базовим вибором під час проектування більшості сучасних локальних мереж.

Пропускна здатність на рівні 1000 Мбіт/с ідеально відповідає навантаженням, притаманним сучасному офісному та адміністративно-виробничому середовищу філії. Висока швидкість дозволяє організувати ефективну роботу корпоративного сервера, встановленого в серверній кімнаті №4а. Він відповідає за функціонування баз даних та внутрішніх файлових сховищ, надаючи безперебійний та швидкий доступ до інформації для всіх сорока п'яти підключених комп'ютерів.

Крім того, така швидкість є критично важливою для фахівців агрономічного, інженерно-технічного та диспетчерського відділів, які щодня оперують важкими файлами, графічними схемами, цифровими картами полів та об'ємною документацією. Надійна гігабітна лінія зв'язку також гарантує високу якість обслуговування (QoS), необхідну для стабільної роботи систем IP-телефонії та проведення сеансів відеоконференцзв'язку без затримок звуку чи зображення.

Додатковим аргументом на користь Gigabit Ethernet є колосальний асортимент сумісного обладнання на ринку.

Комутатори, маршрутизатори та мережеві карти з підтримкою цього стандарту випускаються багатьма виробниками, що забезпечує лояльну цінову

політику, легкість у підборі аналогів та простоту подальшого сервісного обслуговування.

У підсумку, інтеграція технології Gigabit Ethernet у структуру філії «Контінентал Фармерз Груп» є зваженим та далекоглядним кроком. Це рішення підтримує ідеальний баланс між швидкістю роботи, надійністю та витратами на впровадження.

2.2 Проєктування схеми фізичного розміщення мережевих вузлів та кабельних трас

2.2.1 Специфікація кабельних комунікацій і побудова кабельних трас

Для повноцінного розгортання локальної комп'ютерної мережі у філії агрохолдингу необхідно сформувати комплекс активного та пасивного обладнання. До пасивної частини інфраструктури належать комутаційні шафи, патч-панелі, кабельні траси, конектори, розетки та з'єднувальні шнури.

Саме від надійності кабельної системи, яка є фундаментом для зв'язку між усіма вузлами, критично залежить стабільність та якість передачі даних. Тому вибір матеріалів та дотримання стандартів монтажу є першочерговим завданням під час реалізації проєкту.

Оскільки раніше було прийнято рішення про використання стандарту Gigabit Ethernet (1000Base-T), фізичним середовищем передачі даних безальтернативно виступає мідна кручена пара. У межах підприємства буде розгорнуто класичну структуровану кабельну систему (СКС), що концептуально поділяється на три взаємопов'язані функціональні блоки: комутаційні шнури, а також горизонтальну та магістральну розводки. Патч-корди (комутаційні шнури) являють собою гнучкі кабелі невеликої довжини, які виконують роль сполучних ланок. Це гнучке рішення дозволяє швидко

переконфігуровувати мережу та легко замінювати пошкоджені ділянки під час експлуатації, адже такі кабелі є звичайним витратним матеріалом.

Горизонтальна кабельна підсистема є базовою частиною СКС. Її завдання – забезпечити стаціонарне, приховане з'єднання між інформаційними розетками в кабінетах працівників та портами комутаторів рівня доступу, що змонтовані на відповідних поверхах. Таким чином, кожне робоче місце отримує виділений фізичний канал зв'язку.

У філії агрохолдингу ці лінії прокладатимуться від розеток безпосередньо до комутаторів першого (Sw1, Sw2) та другого (Sw3, Sw4, Sw5, Sw6) поверхів. До цієї ж підсистеми технічно відносяться лінії, що сполучають корпоративний сервер і бездротову точку доступу в залі засідань безпосередньо із центральним ядром мережі (комутатором SwG).

Вертикальна (магістральна) кабельна система відповідає за об'єднання всіх периферійних комутаторів у єдину цілісну мережу.

Вона формує високошвидкісні канали передачі даних, поєднуючи комутатори робочих груп із головним вузлом, розташованим у серверній кімнаті. Тип середовища для магістралі (мідь чи оптоволокно) зазвичай визначається відстанню та обсягами агрегованого трафіку. Для даного проєкту принципово важливо створити магістраль, здатну без затримок пропускати сукупний трафік від усіх гігабітних клієнтських пристроїв.

На основі технічних вимог, виділеного бюджету та необхідного запасу продуктивності, як основний носій інформації було обрано неекранований кабель U/UTP Cat.6 4Pr від вітчизняного виробника «Одескабель».

Цей провідник має струмопровідну жилу з м'якої міді діаметром 0,57 мм (відповідає калібру 23 AWG) у надійній поліетиленовій ізоляції, при цьому загальна товщина жили з оболонкою становить 1,05 мм. Виріб повністю задовольняє жорсткі вимоги міжнародних інженерних стандартів ISO/IEC 11801, EN 50173-1, ANSI/TIA/EIA-568-B.2-1 та IEC 61156-5.

Для зручної та надійної комутації зі стаціонарними кабельними магістралями невід'ємним елементом інфраструктури є мережеві розетки. У рамках

даного проєкту прийнято рішення про використання накладної моделі Cablexpert RJ45x1 UTP Cat.6, зовнішній вигляд якої продемонстровано на рисунку 2.2.

Рисунок 2.2 – Зовнішній вигляд розеток Cablexpert RJ45x1 UTP cat.6

Головна перевага такого вибору полягає в максимальній практичності та простоті монтажних робіт. Це рішення є оптимальним для умов офісного середовища, оскільки воно дозволяє оперативно організувати підключення клієнтського обладнання на робочих місцях без необхідності проведення будівельних робіт зі штроблення стін для прихованого встановлення портів [12].

Для підключення комп'ютерного обладнання до цих розеток передбачено використання готових фабричних патч-кордів довжиною 1,5 метра моделі 2E CAT6 UTP RJ-45 (26AWG), що гарантує надійний електричний контакт та довговічність системи.

Філія агрохолдингу «Контінентал Фармерз Груп» розміщується у двоповерховій адміністративній будівлі, що налічує п'ятнадцять основних приміщень та спеціалізовану кімнату №4а, виділену під серверну інфраструктуру. Графічне планування споруди із детальним розташуванням кабінетів наведено у додатку А на рисунках А.1 та А.2. Оскільки мережа проєктується за принципом ієрархічної зірки, архітектурним центром трасування виступає саме серверна кімната, яка розташована на першому поверсі.

Під час проєктування кабельних трас головним завданням було мінімізувати сумарну довжину ліній, зберігши при цьому легкий доступ до кожної робочої зони. Усі кабельні потоки захищаються від фізичних деформацій, надмірного розтягування, критичних перегинів та джерел

електромагнітного випромінювання, таких як силові електромережі чи потужні двигуни.

У коридорних зонах, місцях проходження крізь стіни та всередині шаф дроти впорядковуються за допомогою захисних гофрованих труб, пластикових коробів та металевих лотків під стелею. Для спрощення подальшого сервісного обслуговування та швидкої локалізації неполадок кожен кабель та інформаційний порт підлягають обов'язковому маркуванню згідно із затвердженою номенклатурою.

На першому поверсі робочі місця керівництва, відділу кадрів, інженера з охорони праці та відділу продажів підключаються індивідуальними лініями безпосередньо до комутатора Sw1, що встановлений у серверній. Водночас робочі станції агрономічного підрозділу та відділу закупівель і постачання з'єднуються за допомогою настінних пластикових коробів із комутатором Sw2, який базується у кімнаті №6.

Для прокладання горизонтальних ліній використовуються декоративні пластикові кабель-канали з профілем 50х35 мм, що монтуються вздовж стін або над плінтусами. Там, де це дозволяють конструктивні особливості приміщень, застосовується прихований монтаж за гіпсокартонними перегородками чи над фальшстелею. Перехід кабельних ліній крізь міжкімнатні стіни реалізується через заздалегідь підготовлені отвори діаметром 16 мм, всередині яких обов'язково протягується захисна гофра. Аналогічна 16-міліметрова гофрована трубка застосовується для захисту магістралей над підвісною стелею в коридорах – зокрема на ділянках між кабінетом директора і відділом кадрів, а також між серверною та відділом закупівель.

На другому поверсі будівлі для підключення техніки відділів логістики та продажів застосовується інший інженерний підхід: кабелі ховаються під фальшпідлогою у спеціальних захисних металевих коробах. Така конструкція створює вільний технологічний простір між перекриттям та фінішним покриттям, суттєво спрощуючи обслуговування ліній. Організація кабельних трас під підлогою суворо підпорядковується чинним нормативним актам

України, серед яких ключовими є Правила улаштування електроустановок (ПУЕ), державні будівельні норми ДБН В.2.5-56:2014 та стандарт ДСТУ EN 50085-2-2:2015 [4].

Для виведення інтерфейсів безпосередньо до робочих столів інтегруються спеціальні підлогові розетки, монтаж яких виконується у кілька послідовних етапів [8]. Спочатку у плиті фальшпідлоги за допомогою спеціальної коронки вирізається рівний отвір під розмір монтажного лючка. Потім крізь захисну трубу до цього місця виводиться кабель із невеликим технологічним запасом. На наступному етапі сам лючок надійно фіксується в підлозі гвинтами чи затискачами. Після цього майстер зачищає провідники, розподіляє жили за обраною схемою (T568A або T568B), затискає їх у контактах модуля RJ45 та зрізає залишки міді. Фінальним штрихом є встановлення готового інформаційного модуля в монтажну рамку лючка.

Особлива увага в проєкті приділена пожежній безпеці, тому всі кабелі мають оболонку типу LSZH, яка в умовах займання не підтримує горіння, не виділяє токсичних речовин та має мінімальне димоутворення.

Захист ліній під фальшпідлогою від механічних пошкоджень та гризунів забезпечують металеві перфоровані або суцільні лотки, які одночасно виконують роль пасивної вентиляції. Усі кабелепроводи жорстко кріпляться до опорних конструкцій підлоги для запобігання провисанням чи випадковим зміщенням. Крім того, під час монтажних робіт суворо контролюється радіус вигину крученої пари, який повинен становити від 4 до 8 зовнішніх діаметрів кабелю, що гарантує збереження цілісності мідних жил та стабільні частотні характеристики всієї системи.

2.2.2 Планування розміщення мережевих вузлів

Визначення оптимального місця для серверної кімнати є одним із базових етапів проєктування локальної мережі, оскільки саме тут зосереджується головне технічне ядро системи, включно з маршрутизатором

та центральним комутатором. Для комп'ютерної інфраструктури філії агрохолдингу «Контінентал Фармерз Груп» як ключовий технологічний вузол було обрано кімнату №4а. Такий вибір повністю обґрунтований кількома важливими факторами.

По-перше, кімната №4а має вкрай вигідне географічне розташування на плані будівлі. Це дозволяє прокласти найкоротші кабельні траси від центрального обладнання, зокрема комутаторів SwG і Sw1, маршрутизатора R1 та сервера S1, до периферійних комутаторів Sw2, Sw3, Sw4, Sw5, Sw6 і кінцевих користувачів. Зменшення довжини ліній мінімізує затухання сигналу, суттєво підвищує стабільність зв'язку, оптимізує фінансові витрати на монтаж і значно спрощує розгортання деревоподібної топології. Додатковим технологічним плюсом є те, що серверна розташована у безпосередній близькості до точки введення в будівлю зовнішніх комунікацій від Інтернет-провайдера.

По-друге, архітектурні особливості цього приміщення дозволяють організувати високий рівень фізичної безпеки та захистити дороговартісну апаратуру і конфіденційну інформацію від сторонніх осіб. Кімната взагалі не має вікон та прямого виходу в загальний коридор, а потрапити до неї можна виключно через суміжний кабінет інженера з охорони праці. Це суттєво полегшує контроль доступу та виключає ризик несанкціонованого проникнення чи випадкового пошкодження техніки.

Усі галузеві норми проєктування вимагають, щоб доступ до серверної був суворо обмежений для переважної більшості персоналу та відвідувачів підприємства, а її розміщення зводило до мінімуму витрати на побудову структурованої кабельної системи з усіх сегментів мережі. Обрана кімната №4а повністю задовольняє ці критерії, забезпечуючи максимальну економічну та безпекову доцільність для філії агрохолдингу.

Для акуратного розміщення та систематизації активних і пасивних мережевих компонентів у серверній передбачено встановлення телекомунікаційної шафи. Вона повинна мати достатню монтажну висоту, що

вимірюється в юнітах (U), та оптимальну глибину для інтеграції комутаторів, патч-панелей, кабельних організаторів та блоків безперебійного живлення із обов'язковим просторовим запасом під майбутнє розширення інфраструктури.

З огляду на поточні масштаби мережі, для проєкту обрано компактну настінну шафу моделі WMNC-9U-FLAT із корисним об'ємом 9U та фізичними габаритами 600x450x380 мм, зовнішній вигляд якої зображено на рисунку 2.3. Ці технічні параметри ідеально відповідають архітектурним завданням філії та дозволяють надійно й захищено скомпонувати весь стартовий пакет обладнання.

.

Рисунок 2.3 – Зовнішній вигляд комутаційної шафи WMNC-9U-FLAT

Внутрішній простір обраної телекомунікаційної шафи WMNC-9U-FLAT буде відведено під монтаж ключових елементів системи, серед яких центральний комутатор ядра SwG, комутатор рівня доступу Sw1, головний маршрутизатор, джерело безперебійного живлення, а також комутаційні панелі та елементи впорядкування ліній. Комутацію та систематизацію кабельних потоків всередині шафи забезпечить 19-дюймова патч-панель Panduit на 24 порти, що відповідає категорії 6 [15].

Особливістю цього пасивного обладнання є наявність інтегрованих модулів RJ-45 з безінструментальною системою фіксації. Технологія автоматичного прорізання ізоляції жил суттєво прискорює монтажні роботи та підвищує надійність з'єднання. Панель комплектується оригінальними

елементами кріплення, хомутами Colring і повністю задовольняє вимоги стандарту EIA/TIA 568 B.2-1.

Для підтримки порядку та запобігання заплутуванню комутаційних шнурів у шафі встановлюється горизонтальний кабельний організатор. Захист активної апаратури від стрибків напруги, високовольтних імпульсів або раптового зникнення живлення в зовнішній електромережі покладено на джерело безперебійного живлення (ДБЖ) моделі APC Back-UPS Pro 1500VA. Цей апарат гарантує автономне та безперервне функціонування мережевих вузлів, нівелюючи ризики втрати корпоративних даних чи виходу з ладу плат комутаторів.

Планування офісного простору, де робочі місця співробітників розташовані переважно вздовж стін приміщень, істотно спрощує розгортання структурованої кабельної системи. Завдяки такому компонуванню персональні комп'ютери підключатимуться безпосередньо до мережевих розеток, які інтегровані у настінні захисні короби. Загалом дротова інфраструктура філії розрахована на стабільну роботу 45 комп'ютерів, що функціонують як робочі станції.

Відповідно до графічних схем у додатку Б, найбільше навантаження на мережу та найвища щільність комп'ютерної техніки зафіксована у приміщенні відділу логістики. Великий локальний сегмент сформовано також у відділі продажів, де встановлено десять ПК. По чотири комп'ютерні станції розгорнуто в інженерно-технічному відділі, кімнаті операторів оперативного обліку (яка належить до ремонтного підрозділу), а також у кабінетах логістики та постачання. Менші групи пристроїв, що налічують по три комп'ютери, обслуговують потреби загальної бухгалтерії та кабінету відділу закупівель і постачання.

2.3 Обґрунтування вибору комунікаційного обладнання

Базою інфраструктури локальної мережі філії агрохолдингу «Континентал Фармерз Груп» є активне мережеве обладнання. Його технічні

характеристики безпосередньо впливають на відмовостійкість, захищеність, пропускну здатність та потенціал для подальшого масштабування системи. Для реалізації проєкту було обрано апаратні рішення від компанії Cisco, яка є лідером у сфері корпоративних мережевих технологій і гарантує високу якість інтеграції та технічної підтримки.

Відповідно до розробленої топології (див. рис. 2.1), структуру мережі формують такі компоненти:

- центральний (головний) комутатор – 1 од.;
- маршрутизатор (шлюз доступу) – 1 од.;
- комутатори робочих груп (рівня доступу) – 6 од.;
- бездротова точка доступу (Wi-Fi) – 1 од.

Маршрутизатор, який відповідає за вихід до глобальної мережі Інтернет, та головний комутатор територіально розміщуються в ізольованому серверному приміщенні.

Центральний комутатор виступає ядром архітектури «розширеної зірки», об'єднуючи окремі підмережі в цілісну інфраструктуру. З огляду на це, до нього висуваються підвищені вимоги щодо продуктивності та функціонала. Пристрій має підтримувати:

- маршрутизацію на третьому рівні моделі OSI (L3);
- інтелектуальні сервіси керування трафіком (динамічну пріоритезацію QoS, списки контролю доступу ACL, обробку багатоадресного мовлення Multicast);
- достатній пул портів Gigabit Ethernet для магістральних з'єднань (Uplink) та локальних серверів.

Для комутації всіх запланованих елементів мережі, до центрального вузла необхідно підключити:

- комутатори робочих груп – 6 інтерфейсів;
- локальний сервер – 1 інтерфейс.
- бездротову точку доступу – 1 інтерфейс;
- прикордонний маршрутизатор – 1 інтерфейс.

Мінімальна місткість інтерфейсів головного комутатора для забезпечення поточної схеми підключень становить 9 портів. При цьому швидкість LAN-портів повинна бути не меншою за 1 Гбіт/с, оскільки саме на цій швидкості працюють магістральні канали від комутаторів робочих груп та інтерфейс сервера.

Для запобігання затримкам під час пікових навантажень внутрішня матриця комутатора має забезпечувати неблоковану передачу даних. Розрахунок ведеться з урахуванням загальної кількості генераторів трафіку в мережі – 46 абонентів (45 робочих станцій користувачів та 1 виділений сервер).

Необхідна комутаційна спроможність для забезпечення повнодуплексного (Full-Duplex) режиму роботи обчислюється за формулою:

(45 користувачів + 1 сервер) x 2 (дуплекс) = 92 Гбіт/с (2.1)

Таким чином, інтегральна продуктивність матриці центрального комутатора повинна становити щонайменше 92 Гбіт/с.

Застосування комутатора третього рівня (L3) є важливою умовою для побудови корпоративної мережі. На відміну від стандартних L2-пристроїв, апарати L3 спроможні виконувати маршрутизацію між віртуальними локальними мережами (Inter-VLAN routing). Це дозволяє гнучко сегментувати мережу на логічні зони, ізолювати критичну інфраструктуру, оптимізувати розподіл мережевих ресурсів та локалізувати широкомовний шторм.

На основі проведеного порівняльного аналізу та розрахованих технічних параметрів, як головний комутатор було обрано модель Cisco Catalyst WS-C3560CX-12XPD-S.

Зовнішній вигляд комутатора Cisco Catalyst WS-C3560CX-12XPD-S наведено на рисунку 2.4.

Рисунок 2.4 – Зовнішній вигляд комутатора Cisco CWS-C3560CX-12XPD-S

З внутрішньою комутаційною пропускною здатністю 128 Гбіт/с, що відповідає розрахунковим потребам мережі, цей комутатор забезпечує надлишкову потужність та відсутність перевантажень.

Повний перелік технічних специфікацій та функціональних можливостей обраного комутатора наведено нижче у таблиці 2.1 [14].

Таблиця 2.1 – Технічні характеристики комутатора Cisco WS-C3560CX-12XPD-S

Характеристика	Значення
Тип пристрою	Комутатор третього рівня L3
Порти LAN	12 x Gigabit Ethernet (RJ-45 1000 Мбіт/с)
Порти Uplink	4x 10 Gigabit Ethernet (SFP+ 10000 Мбіт/с)
Пропускна здатність	128 Гбіт/с
Пам’ять	DRAM 512 МБ / Flash 128 Мб
Підтримка протоколів	IEEE 802. 1d (Spanning Tree) IEEE 802. 1p (Priority tags) IEEE 802. 1q (VLAN) IEEE 802. 1s (Multiple Spanning Tree) SNMP , IGMP , DHCP-клієнт
Продуктивність маршрутизації	68. 4 mpps
Кількість VLAN	4000
Міжмережевий екран	Присутній
Розмір	4 269 x 44 x 264 мм
Вага	2,72 кг
Живлення	230 В, 35,2 Вт
Вартість	65 345 грн.

Апаратна платформа Cisco Catalyst WS-C3560CX-12XPD-S підтримує широкий спектр інтелектуальних технологій та сервісів керування мережею, серед яких варто виділити наступні [14]:

- Quality of Serversice (QoS) – механізм динамічної пріоритезації трафіку, критичного до затримок (зокрема, IP-телефонії та потокового відео);

- Rate Limiting (обмеження швидкості) – інструмент для гнучкого регулювання та контролю смуги пропускання всередині окремих логічних сегментів;

- Access Control Lists (ACL) – списки контролю доступу, що використовуються для реалізації політик безпеки та фільтрації трафіку;

- Multicast Management – функціонал оптимізації багатоадресного мовлення для зниження загального навантаження на мережу;

- Link Aggregation (агрегація каналів) – технологія об'єднання кількох фізичних інтерфейсів в один логічний для масштабування пропускної здатності, підвищення відмовостійкості, а також підсумовування енергетичного бюджету PoE;

- Cisco Express Forwarding (CEF) – фірмова технологія апаратної високошвидкісної IP-маршрутизації, яка забезпечує максимальну продуктивність під час передачі трафіку між віртуальними мережами (Inter-VLAN routing).

Комутатори робочих груп функціонують на рівні доступу мережевої архітектури. Їхнє головне завдання полягає в агрегації трафіку від кінцевих абонентських пристроїв (робочих станцій, мережевих принтерів тощо) та його подальшому перенаправленні до магістралі мережі й центрального комутаційного вузла.

Усього в межах проєкту передбачено розгортання шести таких пристроїв. Вибір конкретної моделі базується на двох ключових критеріях: сумарній кількості фізичних інтерфейсів та інтегральній пропускній здатності внутрішньої матриці. Відповідно до технічного завдання, для кожного

користувача необхідно забезпечити швидкість підключення на рівні 1 Гбіт/с, що вимагає інтеграції портів стандарту Gigabit Ethernet.

Щоб визначити оптимальні технічні характеристики комутаторів рівня доступу, розрахунок проводиться за параметрами найбільшого локального сегмента. Згідно з логічною топологією мережі (Додаток Б), максимальна концентрація хостів спостерігається у відділі міжнародної логістики, де зосереджено 11 кінцевих вузлів.

Таким чином, мінімальна кількість портів для цього сегмента обчислюється як:

- 11 інтерфейсів – для підключення клієнтських станцій;
- 1 інтерфейс (Uplink) – для створення магістрального каналу зв'язку з головним комутатором.

Для забезпечення поточної схеми комутації та організації висхідного каналу комутатор найзавантаженішого сегмента повинен мати мінімум 12 портів Gigabit Ethernet.

Для забезпечення номінальної швидкості 1 Гбіт/с без виникнення «вузьких місць», внутрішня комутаційна спроможність пристрою має підтримувати повнодуплексний режим роботи для всіх активних ліній. Це гарантує одночасний прийом та передачу пакетів без внутрішніх затримок.

Мінімально необхідна пропускна здатність матриці для найзавантаженішого вузла на 11 хостів розраховується за формулою:

$$\text{Пропускна здатність} = N_{\text{вузлів}} \times V_{\text{порту}} \times 2_{\text{дуплекс}} \quad (2.2)$$

Звідси:

$$11 \text{ вузлів} \times 1 \text{ Гбіт/с} \times 2 = 22 \text{ Гбіт/с}$$

Отже, внутрішня шина комутатора робочої групи повинна мати продуктивність не менше 22 Гбіт/с.

Для реалізації завдань рівня доступу було обрано керований комутатор другого рівня (L2) Cisco Catalyst C1000-16T-2G-L (див. рис. 2.5), який повністю задовольняє проектні вимоги та забезпечує:

Рисунок 2.5 – Зовнішній вигляд комутатора Cisco C1000-16T-2G-L

- стабільну гігабітну швидкість на всіх абонентських лініях;
- надійну трансляцію магістрального трафіку через виділені аплінк-інтерфейси;
- обробку потоків даних без буферних затримок.

Для покриття цих потреб обрано модель, що оснащена 16 LAN-інтерфейсами типу RJ-45 із автовизначенням швидкості (10/100/1000 Мбіт/с) для підключення локальних хостів [15]. Крім того, архітектура пристрою містить 2 окремі виділені аплінк-порти Gigabit Ethernet (1000 Мбіт/с), які використовуються для побудови відмовостійких магістральних з'єднань із ядром мережі.

Завдяки загальній комутаційній спроможності у 32 Гбіт/с, цей комутатор суттєво перевищує розрахований мінімум (22 Гбіт/с). Наявність такого технологічного запасу гарантує високу продуктивність під час пікових навантажень та створює потенціал для подальшого розширення робочих місць у кімнатах без заміни обладнання.

Вичерпний перелік технічних і експлуатаційних параметрів комутатора рівня доступу зведено у таблиці 2.2.

Наступним етапом проектування інфраструктури є підбір прикордонного маршрутизатора, який виконуватиме функції шлюзу за замовчуванням (Default Gateway) для виходу локальної мережі філії до глобальної мережі Інтернет.

Таблиця 2.2 – Технічні характеристики комутатора робочих груп рівня доступу

Характеристика	Значення
Тип пристрою	Комутатор другого рівня L2
Порти LAN	16x Gigabit Ethernet (RJ-45 10/100/1000 Мбіт/с)
Порти Uplink	2x Gigabit Ethernet (SFP 1000 Мбіт/с)
Пропускна здатність	32 Гбіт/с
Пам’ять	DRAM 512 Мб / Flash 256 Мб
Розмір	26,8x21x4,4 см
Вага	1,42 кг
Блок живлення	100-127V, 1A, 200-240V, 0.5A, 50-60Hz
Вартість	27 313,25 грн

Оскільки взаємодія з Інтернет-провайдером відбуватиметься через волоконно-оптичну лінію зв'язку, критично важливою архітектурною вимогою до пристрою є наявність оптичного SFP-слота. Інтеграція SFP-інтерфейсу дозволяє:

- організувати пряме підключення до ліній провайдера без використання додаткових зовнішніх медіаконвертерів, які знижують надійність схеми;
- забезпечити максимальну пропускну здатність та мінімальний рівень затримок під час трансляції пакетів;
- підвищити стабільність з'єднання завдяки природній стійкості оптичного волокна до електромагнітних завад.

Орієнтуючись на ці технічні критерії, а також на необхідність забезпечення високого рівня безпеки та відмовостійкості під час передачі даних, для реалізації проєкту було обрано маршрутизатор інтегрованих послуг корпоративного класу Cisco ISR4221/K9. Дана апаратна платформа підтримує сучасні протоколи шифрування та інструменти захисту периметра мережі, що повністю задовольняє вимогам безпеки агрохолдингу.

Зовнішній вигляд обраного прикордонного маршрутизатора Cisco ISR4221/K9 наведено на рисунку 2.6.

Рисунок 2.6 – Зовнішній вигляд маршрутизатора Cisco ISR4221/K9

Повний перелік технічних характеристик та підтримуваних стандартів наведено в таблиці 2.3 [16].

Таблиця 2.3 – Технічні характеристик Cisco ISR4221/K9 [15]

Характеристика	Значення
Макс. Кількість VLAN	20
Швидкість передачі	2 Гбіт/с
Оперативна пам’ять	4 ГБ із можливістю розширення до 16 ГБ.
Флеш пам’ять	4 ГБ
Підтримувані VLAN	802.1q Tag-на основі, на основі портів
Локальний сервер DNS	+
Захист від атак DoS	+
Захист від спуфінгу	+
Пропускна здатність NAT	2.2 Гбіт/с
Маршрутизація	Статична, RIP v1/v2, OSPF, EIGRP, BGP
Підтримка IPSec	+
Монтаж в стійку	4U
WAN-порт	SFP – 2 шт.
LAN-порт	Gigabit Ethernet RJ-45
Розмір (мм)	273 x 171 x 45 мм
Вартість	24 706 грн.

Апаратна платформа Cisco ISR4221/K9 являє собою високопродуктивне рішення, розраховане на обробку інтенсивних потоків зовнішнього трафіку та підтримання стабільного зв'язку із глобальною мережею. Висока обчислювальна потужність пристрою дозволяє суміщати базові операції маршрутизації з апаратною генерацією та шифруванням VPN-тунелів, що значно розширює можливості для побудови захищених корпоративних каналів.

- До ключових завдань та інтелектуальних функцій маршрутизатора належать:

- шлюз забезпечує безперебійний обмін даними між Інтернетом та внутрішніми сегментами (VLAN) філії агрохолдингу «Контінентал Фармерз Груп». Поряд із простими статичними конфігураціями пристрій підтримує розгортання складних протоколів динамічної маршрутизації (OSPF, EIGRP, BGP), які автоматично оптимізують шляхи проходження пакетів у разі зміни стану мережі;

- пристрій бере на себе функції брандмауера. Завдяки впровадженню списків контролю доступу (ACL) здійснюється ретельний моніторинг та фільтрація вхідного і вихідного трафіку, що дозволяє надійно захистити локальну інфраструктуру від зовнішніх кіберзагроз та несанкціонованих підключень.

Для побудови бездротової інфраструктури (Wi-Fi) в межах даного проєкту передбачено інтеграцію точки доступу TP-LINK EAP225 (див. рис. 2.7).

Рисунок 2.7 – Зовнішній вигляд точки доступу TP-LINK EAP225

Дане бездротове рішення є високопродуктивною дводіапазонною точкою доступу, що функціонує за стандартом Wi-Fi 5 (802.11ac). Пристрій забезпечує

максимальну швидкість бездротового з'єднання до 867 Мбіт/с у частотному діапазоні 5 ГГц та до 450 Мбіт/с у смузі 2,4 ГГц, що гарантує високу швидкість обміну даними для мобільних клієнтів.

Серед ключових архітектурних та функціональних особливостей моделі варто виділити наступні:

- апаратний інтерфейс пристрою представлений одним гігабітним портом Ethernet (RJ-45) із підтримкою стандартів живлення PoE 802.3af/at. Це дозволяє подавати електроживлення на точку доступу безпосередньо через мережевий кабель (кручену пару), нівелюючи потребу в прокладанні додаткових силових ліній та значно спрощуючи вибір локації для монтажу;

- завдяки лаконічному корпусу, який візуально нагадує стельовий світильник, обладнання органічно інтегрується в офісний інтер'єр. Конструкція передбачає швидке кріплення як на вертикальні (стіни), так і на горизонтальні поверхні (підвісна стеля);

- модель оптимізована для стабільної роботи в умовах одночасного підключення великої кількості бездротових хостів (офісні приміщення, зони очікування відвідувачів, конференц-зали);

- інтегровані інструменти автентифікації користувачів (включаючи функціонал гостьового порталу – Captive Portal) дозволяють мережевим адміністраторам гнучко регламентувати права доступу до бездротового сегмента, надійно захищаючи корпоративний периметр від несанкціонованих підключень.

2.4 Обґрунтування вибору програмного забезпечення

Побудова надійної IT-інфраструктури філії агрохолдингу «Континентал Фармерз Груп» потребує ретельного підбору базового та прикладного програмного забезпечення (ПЗ). Системне ПЗ має забезпечувати відмовостійкість сервісів, високий рівень захисту інформації, проактивний моніторинг процесів та комфортні умови для роботи кінцевих користувачів.

Вибір серверної операційної системи є надзвичайно важливим кроком, оскільки вона формує фундамент для розгортання корпоративних служб. Критерії оцінки серверних операційних систем (ОС) базуються на показниках стабільності, безпеки та сукупної вартості володіння (TCO) [9]. Натомість для клієнтських систем головним є зручність інтерфейсу та сумісність із прикладним софтом [10].

Під час проектування інфраструктури було проведено порівняльний аналіз чотирьох поширених серверних платформ, результати якого наведено в таблиці 2.4.

Таблиця 2.4 – Порівняльний аналіз серверних операційних систем

Операційна система	Основні переваги	Недоліки та обмеження
MS Windows Serverser	Тісна інтеграція з екосистемою Microsoft (Active Direcory), наявність GUI, широка сумісність із ПЗ [10].	Висока вартість ліцензування (TCO, CALs), підвищені вимоги до апаратних ресурсів [9].
Red Hat Enterprise Linux (RHEL)	Виняткова відмовостійкість, інтегрована безпека (SELinux), офіційна підтримка до 10 років [9].	Висока вартість комерційної підписки, складність адміністрування (потрібні навички CLI).
Linux Debian	Максимальна стабільність через консервативне тестування, безкоштовність, низькі вимоги до заліза.	Повільне впровадження нових технологій, відсутність прямої комерційної підтримки від розробника.
Ubuntu Serverser	Зручність розгортання, 5-річна підтримка LTS-релізів, безкоштовність, величезна база знань.	Менша кількість специфічного комерційного ПЗ порівняно з Windows.

За результатами аналізу для філії було обрано операційну систему Ubuntu Serverser. Цей вибір є найбільш обґрунтованим з огляду на такі фактори:

- платформа є абсолютно безкоштовною, що суттєво знижує витрати на впровадження порівняно з Windows Serverser або RHEL та мінімізує загальну вартість володіння інфраструктурою;
- наявність детальної документації та великої спільноти користувачів дозволяє персоналу швидко налаштувати файловий сервер без залучення дорогих зовнішніх фахівців;
- релізи із довгостроковою підтримкою (LTS) гарантують п'ять років стабільних оновлень безпеки, що мінімізує ризики простою бізнес-процесів філії;
- гнучкість ОС дозволяє у майбутньому розгортати на ній додаткові служби (бази даних, внутрішні веб-ресурси чи CRM) без зміни платформи.

Для забезпечення безперебійної роботи персоналу (бухгалтерія, логістика, менеджмент) стандартним рішенням для робочих місць було обрано Microsoft Windows 11 Pro [10].

Даний вибір забезпечує такі переваги:

- звичний та інтуїтивний дизайн мінімізує час на адаптацію та навчання співробітників, які не мають глибоких IT-знань;
- платформа підтримує весь спектр офісного, бухгалтерського та аналітичного софту, необхідного для щоденних операцій агрохолдингу;
- центр оновлень Windows вчасно інсталює патчі безпеки та драйвери у фоновому режимі, підтримуючи стабільність системи;
- оптимізовані алгоритми ОС забезпечують швидку багатозадачність та ефективне використання ресурсів сучасного апаратного забезпечення.

2.6 Вибір мережевого сервера та визначення його функцій

Центральна серверна платформа філії агрохолдингу «Контінентал Фармерз Груп» розгортається як багатофункціональний вузол, що забезпечує роботу кількох критично важливих корпоративних сервісів. Організація консолідованої серверної архітектури дозволяє раціонально використовувати апаратні потужності та значно спрощує процес централізованого адміністрування. При цьому фізичний сервер мережі буде виконувати наступні функції

Файловий сервер – призначений для створення єдиного захищеного сховища корпоративної документації із гнучким розмежуванням прав доступу. Завдяки інтеграції програмного пакета Samba на базі Ubuntu Serverser, робочі станції користувачів (переважно під керуванням ОС Windows) отримують безшовний доступ до мережевих каталогів. Це впорядковує збереження файлів профільних відділів (бухгалтерії, логістики, кадрової служби, клієнтського сервісу), автоматизує внутрішній документообіг, забезпечує суворий контроль версій та формує надійну базу для подальшого архівування даних.

Сервер резервного копіювання (Backup Serverser) – відповідає за регулярне автоматизоване створення резервних копій конфігураційних файлів, баз даних та користувацьких документів. Використання утиліти BorgBackup дозволяє реалізувати ефективну дедуплікацію та шифрування архівних масивів. Сервер гарантує безкомпромісний захист інформації від технічних збоїв накопичувачів, випадкових дій персоналу або деструктивного впливу шкідливого ПЗ (зокрема, вірусів-вимагачів). Швидке відновлення систем із резервних копій зводить до мінімуму фінансові та репутаційні ризики від потенційних простоїв.

Сервер моніторингу (Monitoring Serverser) – здійснює цілодобовий проактивний нагляд за станом активного мережевого обладнання Cisco та серверної операційної системи. Комплекс інструментів у складі Prometheus (із модулем Node Exporter) та протоколу SNMP збирає метрики продуктивності

апаратних засобів, а платформа Grafana забезпечує їх наочну візуалізацію у вигляді графіків.

Адміністратори мають можливість у реальному часі відстежувати утилізацію процесора (CPU), заповнення оперативної пам'яті (RAM) та дискових масивів, інтенсивність мережевого трафіку й температурні показники, що дозволяє ліквідувати аномалії ще до виникнення аварійних ситуацій.

З огляду на необхідність суміщення ролей файлового сховища, сервера бекапів та системи моніторингу для офісу чисельністю близько 46 користувачів, до апаратного забезпечення висуваються високі вимоги щодо дискової місткості, відмовостійкості та процесорної потужності.

Для реалізації проєкту обрано стійковий сервер корпоративного класу Dell PowerEdge R450, зовнішеій вигляд якого представлено на рисунку 2.8.

Основні аргументи а користь втбору даної моделі сервера:

Рисунок 2.8 – Зовнішній вигляд сервера класу Dell PowerEdge R450

- компактні розміри (форм-фактор 1U) дозволяють ідеально інтегрувати пристрій у наявну серверну шафу поруч із комутаторами та маршрутизатором Cisco;

- апаратний RAID-контролер забезпечує створення дзеркальних дискових масивів (RAID 1/5/10), що критично важливо для збереження файлів у разі виходу з ладу одного чи кількох накопичувачів;

- наявність двох блоків живлення із підтримкою гарячої заміни (Hot-Plug) захищає сервер від зупинки в разі аварії на одній із ліній електропостачання.

2.7 Розподіл адресного простору мережевих вузлів

Для організації ефективної та безпечної адресації вузлів у локальній мережі філії агрохолдингу «Контінентал Фармерз Груп» було обрано приватний адресний простір IPv4 класу C – 192.168.0.0/24. Даний діапазон є оптимальним для поточного масштабу проєкту, оскільки він дозволяє розгорнути до 254 унікальних IP-адрес, що з великим запасом перекриває потребу у підключенні 45 кінцевих пристроїв та залишає простір для майбутнього масштабування.

Принципи сегментації на VLAN та визначення ємності підмереж

З метою ізоляції широкомовного трафіку, оптимізації маршрутизації та підвищення рівня інформаційної безпеки, єдиний адресний простір логічно розділено на віртуальні підмережі (VLAN) відповідно до організаційної структури підприємства.

Для точного визначення розмірності кожної підмережі було проведено аудит кількості активних підключень. Важливою архітектурною умовою є те, що до кількості фізичних хостів у кожному сегменті обов'язково додається ще одна IP-адреса, яка резервується під мережевий шлюз.

З огляду на це, усі структурні підрозділи підприємства та службові вузли було логічно згруповано у три категорії за рівнем потреби в адресних ресурсах:

- сегменти підвищеної місткості (потреба від 11 до 12 адрес). До цієї групи увійшли наймасовіші підрозділи філії: відділ логістики (VLAN Log), який налічує 11 робочих станцій, та відділ продажів (VLAN Prodag) із 10 терміналами;

- сегменти базової місткості (потреба від 3 до 6 адрес). Найширша категорія, що об'єднує вузли середніх і малих робочих груп. Сюди належать: бухгалтерія (VLAN Bugh – 5 ПК), інженерно-технічна служба (VLAN Techn – 4 ПК) та оператори обліку (VLAN Oper – 4 пристрої). Також до цієї групи відносяться відділи з потребою у трьох робочих місцях (дирекція – VLAN

Direc, відділ кадрів та охорони праці – VLAN Kadr, постачання – VLAN Zakupk) та агрономічний відділ (VLAN Agron), що має 2 ПК;

вузькоспеціалізовані та інфраструктурні мережі (потреба суворо у 2 адресах). Сюди віднесено ізольований серверний сегмент (VLAN Servers), що містить один центральний сервер. Окремо виділено транзитну магістраль (Sw-R), яка не містить користувацьких пристроїв, а використовується виключно для організації прямого (point-to-point) зв'язку між центральним комутатором рівня розподілу та шлюзовим маршрутизатором.

Для раціонального розподілу базової мережі 192.168.0.0/24 застосовано метод маски змінної довжини – VLSM. На відміну від класичного поділу з фіксованою маскою (FLSM), VLSM дозволяє призначати кожному сегменту маску, яка максимально точно відповідає кількості його хостів. Це унеможливлює марнотратство вільних IP-адрес та створює гнучку архітектуру.

Для мінімізації фрагментації адресного простору список підмереж сортується за спаданням потреб (від найбільшої до найменшої). Розмір блоку адрес обчислюється за формулою 2^n, де n – кількість бітів, виділених для хостів. Довжина префікса (маски) розраховується як 32 - n.

Відповідно до цього алгоритму, мережі отримали такі параметри:

- блоки по 16 адрес (2^4, маска /28) – необхідні для відділів Log (12 адрес) та Prodag (11 адрес);
- блоки по 8 адрес (2^3, маска /29) – покривають потреби середніх відділів – Bugh, Techn, Oper, Direc, Kadr, Zakupk, Agron (від 3 до 6 адрес у кожному);
- блоки по 4 адреси (2^2, маска /30) – ідеальні для з'єднань типу «точка-точка» та малих сегментів – Servers та Sw-R (по 2 адреси).

Призначення блоків відбувається послідовно. Наприклад, першою йде найбільша підмережа (Log). Вона отримує базову адресу 192.168.0.0/28. Цей блок містить 16 адрес: 14 доступних для використання (від 192.168.0.1 до 192.168.0.14) та одну широкомовну (Broadcast) — 192.168.0.15.

Наступна підмережа (Prodag) розпочинається одразу після попередньої — з адреси 192.168.0.16/28, маючи робочий діапазон від .17 до .30, і так далі.

Повний та деталізований результат розрахунку IP-адресації за алгоритмом VLSM зведено до таблиці 2.5.

Таблиця 2.5 – Карта розподілу адресного простору локальної мережі

Назва VLAN	Розмір блоку	Маска підмережі	Адреса мережі	Діапазон доступних IP-адрес	Широкомовна адреса
1	2	3	4	5	6
Log	16	/28	192.168.0.0	192.168.0.1 – 192.168.0.14	192.168.0.15
Prodag	16	/28	192.168.0.16	192.168.0.17 – 192.168.0.30	192.168.0.31
Bugh	8	/29	192.168.0.32	192.168.0.33 – 192.168.0.38	192.168.0.39
Techn	8	/29	192.168.0.40	192.168.0.41 – 192.168.0.46	192.168.0.47
Oper	8	/29	192.168.0.48	192.168.0.49 – 192.168.0.54	192.168.0.55
Direc	8	/29	192.168.0.56	192.168.0.57 – 192.168.0.62	192.168.0.63
Kadr	8	/29	192.168.0.64	192.168.0.65 – 192.168.0.70	192.168.0.71
Zakupk	8	/29	192.168.0.72	192.168.0.73 – 192.168.0.78	192.168.0.79
Agron	8	/29	192.168.0.80	192.168.0.81 – 192.168.0.86	192.168.0.87
Servers	4	/30	192.168.0.88	192.168.0.89 – 192.168.0.90	192.168.0.91
Sw-R	4	/30	192.168.0.92	192.168.0.93 – 192.168.0.94	192.168.0.95

Після завершення розподілу IP-адрес для десяти основних підмереж, крайньою точкою використаного простору є адреса 192.168.0.95. Це залишає

значний обсяг вільних ресурсів, починаючи з 192.168.0.96. Даний резерв доцільно використати для організації бездротового доступу в залі засідань №5 (деталі в додатку Б).

З огляду на потребу у 50 динамічних вузлах, було обрано блок із 128 адрес (що відповідає 27). Такий підхід забезпечує необхідний запас ємності. Параметри розрахунку: кількість біт хоста – 7, маска підмережі – 32 - 7 = /25, мережева адреса – 192.168.0.96/25, діапазон хостів 192.168.0.97 – 192.168.0.222, шлюз – 192.168.0.222, широкосмугова адреса –192.168.0.223.

Для стабільної роботи стаціонарне обладнання отримає статичні параметри, тоді як автоматизація розподілу IP для мобільних девайсів буде реалізована через DHCP-сервер на базі комутатора SwG.

2.7 Тестування та налагодження мережі

Етап тестування є завершальним циклом розгортання мережі, що слідує за монтажними роботами. Його ключове завдання полягає у верифікації реалізованої архітектури на відповідність технічному завданню, усуненні експлуатаційних дефектів та оптимізації параметрів для забезпечення надійної роботи сервісів. Діагностика проводиться ієрархічно за рівнями моделі OSI.

На фізичному рівні (L1) виконуються наступні тестування:

- візуальний контроль цілісності кабельних трас, надійності фіксації розеток та патч-панелей. Особлива увага приділяється верифікації маркування згідно зі схемою адміністрування;

- діагностика ліній за допомогою аналізатора СКС (Категорія 6). Перевіряються такі метрики, як цілісність провідників, відсутність перехресних наводок (NEXT) та загасання сигналу;

- формування цифрових звітів, що підтверджують готовність кабельної системи до промислової експлуатації.

На канальному рівні (L2) виконуються наступні тестування:

- аналіз світлодіодних індикаторів на комутаторах SwG та Sw1–Sw6 для підтвердження активності лінків;

- перевірка логічної сегментації на комутаційному обладнанні та маршрутизаторі R1. Контроль ізоляції трафіку між 10 віртуальними мережами та працездатності тегованих магістралей (Trunk, 802.1Q).

На мережевому та вищих рівня (L3+) виконуються наступні тестування:

- верифікація роботи DHCP-пулу на L3-комутаторі SwG для клієнтських пристроїв та перевірка коректності статичних IP-налаштувань;

- тестування міжмережевої взаємодії через шлюз R1, перевірка резолвінгу імен через DNS (8.8.8.8) та вимірювання реальної пропускної здатності;

- аудит доступу до ресурсів Samba. Перевірка політик розмежування прав (читання/запис) та стрес-тест швидкості передачі даних.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування комутаторів та маршрутизації між VLAN

3.1.1 Інструкції з налаштування комутаторів рівня доступу

Процес ініціалізації активного мережевого інвентарю розпочинається з базового налаштування комутаторів, відповідальних за стабільне функціонування окремих сегментів інфраструктури. Цей етап передбачає реалізацію комплексу стратегічних завдань, спрямованих на забезпечення керованості та захищеності системи.

Зокрема, особлива увага приділяється присвоєнню пристроям унікальних мережевих імен для їх ідентифікації в топології, а також впровадженню параметрів безпеки шляхом встановлення паролів автентифікації, що обмежують несанкціонований доступ до функцій управління.

Крім того, здійснюється підготовка інтерфейсів для підтримки технології VLAN, що дозволяє реалізувати логічну сегментацію мережі відповідно до розробленого проєкту.

Практична реалізація налаштувань бере свій початок із комутатора робочих груп, розташованого у серверному приміщенні згідно з планом, наведеним у додатку Б. Першочерговим кроком є встановлення фізичного консольного з'єднання з пристроєм для отримання доступу до його операційного середовища.

Одразу після ініціалізації підключення система автоматично активує користувацький режим керування. Для подальшого переходу до адміністративних функцій та безпосереднього присвоєння пристрою ідентифікаційного імені необхідно виконати послідовність термінальних команд, що детально задокументовані та представлені на рисунку 3.1.

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

Рисунок 3.1 – Лістинг налаштування назви комутатора

Наступним важливим етапом адміністрування є впровадження багаторівневої системи парольного захисту, що дозволяє мінімізувати ризики несанкціонованого втручання в роботу мережі.

Комплексна безпека комутатора базується на обмеженні доступу до різних методів взаємодії з пристроєм. Зокрема, пароль консолі забезпечує захист від прямого фізичного підключення через відповідний порт, тоді як паролі віртуальних ліній (VTY) є обов’язковими для безпечного віддаленого керування за допомогою протоколів Telnet або SSH.

Окремий рівень захисту передбачено для режиму привілейованого виконання, який надає розширені права на зміну конфігурації. Для забезпечення конфіденційності всіх встановлених кодів у системному файлі конфігурації обов'язково застосовується спеціалізована команда глобального шифрування, яка перетворює відкриті текстові дані на нечитабельні символьні послідовності.

Для активації захищеного доступу до режиму з розширеними правами використовується команда enable secret, яка є пріоритетною завдяки автоматичному шифруванню пароля за допомогою стійких алгоритмів.

Це гарантує, що навіть при отриманні доступу до файлу конфігурації зловмисник не зможе розпізнати встановлену комбінацію. На відміну від застарілих методів, такий підхід забезпечує вищий рівень криптографічної стійкості, що є критичним для адміністрування сучасних мереж.

Процедура обмеження фізичного доступу через консольний порт вимагає попереднього входу в режим конфігурування відповідного інтерфейсу. Після цього за допомогою директиви password призначається необхідна комбінація символів.

Важливою деталлю є використання команди login, яка безпосередньо активує запит автентифікації при спробі встановлення з'єднання. Повна послідовність дій, що включає налаштування паролів як для консольного інтерфейсу, так і для привілейованого режиму виконання, наочно продемонстрована на рисунку 3.2.

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

Рисунок 3.2 – Конфігурування параметрів безпеки для привілейованого режиму та консольного інтерфейсу.

Для забезпечення безпеки віддаленого керування пристроєм через протоколи Telnet або SSH застосовуються паролі ліній VTY. Архітектура комутатора зазвичай передбачає наявність кількох таких ліній (наприклад, у діапазоні від 0 до 4), що створює технічну можливість для паралельної роботи кількох адміністраторів у сесіях дистанційного доступу. Вичерпний перелік інструкцій, необхідних для активації та захисту віртуальних ліній віддаленого керування, наведено в матеріалах рисунка 3.3.

```
Sw1(config)#line vty 0 4
Sw1(config-line)#password agropolis
Sw1(config-line)#login
Sw1(config-line)#transport input ssh
Sw1(config-line)#exit
Sw1(config)#service password-encryption
Sw1(config)#
```

Рисунок 3.3 – Введення паролю для SSH доступу

Для забезпечення високого рівня конфіденційності при дистанційному адмініструванні впроваджується протокол SSH, який, на відміну від Telnet, використовує криптографічні методи захисту трафіку. Додатковим заходом безпеки є активація глобального шифрування всіх паролів, що зберігаються в

пам'яті пристрою, за допомогою директиви service password-encryption. Це дозволяє приховати символьні комбінації від перегляду у відкритому вигляді через файл конфігурації. Варто зауважити, що згаданий у документації пароль «agropolis» є виключно демонстраційним, тому під час реального розгортання мережі його необхідно замінити на складну та унікальну комбінацію, що відповідає корпоративним стандартам безпеки.

Завершальним етапом підготовки системи до віддаленої роботи є створення локального облікового запису користувача з відповідними правами доступу. Процедура генерації ключів шифрування та реєстрації адміністратора в базі даних комутатора вимагає виконання набору специфічних команд. Детальна послідовність налаштування ідентифікаційних даних для роботи через захищений протокол SSH наведена на рисунку 3.4.

```
Sw1(config)#username admin privilege 15 secret agropolis
Sw1(config)#ip domain name agropolis.local
Sw1(config)#crypto key generate rsa
The name for the keys will be: Sw1.agropolis.local
```

Рисунок 3.4 – Процедура генерації локального облікового запису для автентифікації через захищений протокол SSH

Наступним кроком є формування віртуальних локальних мереж на кожному комутаційному пристрої інфраструктури. Процес логічної сегментації передбачає створення десяти окремих доменів колізій, що дозволяє ізолювати трафік різних відділів та груп користувачів. Вичерпна специфікація, яка містить ідентифікаційні номери (VLAN ID) та відповідні текстові назви для кожної з проектованих підмереж.

Процедура формування віртуальних локальних мереж передбачає ініціалізацію відповідних структур у режимі глобальної конфігурації пристрою. Кожна нова VLAN створюється шляхом введення директиви vlan із зазначенням її унікального цифрового ідентифікатора. Для спрощення подальшого адміністрування та візуальної ідентифікації сегментів кожній мережі присвоюється описова назва за допомогою команди name. Такий підхід

дозволяє чітко розмежувати логічні групи користувачів згідно з технічним завданням. Детальний перелік термінальних інструкцій, що використовуються для генерації та найменування віртуальних мереж, наведено на рисунку 3.5.

```
Sw1(config)#vlan 101
Sw1(config-vlan)#name Logist
Sw1(config-vlan)#vlan 102
Sw1(config-vlan)#name Prodag
Sw1(config-vlan)#vlan 103
Sw1(config-vlan)#name Buhgal
Sw1(config-vlan)#vlan 104
Sw1(config-vlan)#name Techn
Sw1(config-vlan)#vlan 105
Sw1(config-vlan)#name Oper
Sw1(config-vlan)#vlan 106
Sw1(config-vlan)#name Direct
Sw1(config-vlan)#vlan 107
Sw1(config-vlan)#name Kadry
Sw1(config-vlan)#vlan 108
Sw1(config-vlan)#name Zakup
Sw1(config-vlan)#vlan 109
Sw1(config-vlan)#name Agronom
Sw1(config-vlan)#vlan 110
Sw1(config-vlan)#name Serv
Sw1(config-vlan)#vlan 111
Sw1(config-vlan)#name Sw-Rout
Sw1(config-vlan)#exit
Sw1(config)#
```

Рисунок 3.5 – Формування бази даних віртуальних локальних мереж у середовищі конфігурування комутатора.

Наступним етапом після формування бази даних віртуальних мереж є визначення режимів роботи комутаційних портів, що є критично важливим для коректної ізоляції та передачі трафіку.

В архітектурі мережі застосовуються два базові типи інтерфейсів. Порти доступу орієнтовані на підключення кінцевого клієнтського обладнання, зокрема персональних комп'ютерів, і здійснюють обробку виключно нетегованих кадрів, що належать до однієї конкретної VLAN.

Натомість транкові порти використовуються для організації магістральних каналів зв'язку між самими комутаторами або для їхнього підключення до маршрутизатора. Їхньою головною функцією є забезпечення одночасного проходження трафіку з багатьох підмереж через єдине фізичне з'єднання завдяки механізму тегування.

Відповідно до затвердженої структурної схеми, наведеної в додатку Б, подальша конфігурація комутатора Sw1 вимагає призначення відповідних ролей для його інтерфейсів у середовищі глобального налаштування. Особливу увагу слід приділити останньому порту пристрою, який виконує роль висхідного каналу (uplink) до центрального комутатора SwG.

Цей інтерфейс обов'язково переводиться в транковий режим для гарантування безперешкодного обміну багатомережевим трафіком із ядром системи. Вичерпний перелік термінальних команд, необхідних для ініціалізації клієнтських портів доступу та налаштування магістрального з'єднання на вузлі Sw1, наочно продемонстровано на рисунку 3.6.

```
Sw1(config)#interface range gigabitethernet0/1-gigabitethernet5/1
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#interface range gigabitethernet0/1-gigabitethernet2/1
Sw1(config-if-range)#switchport access vlan 106
Sw1(config-if-range)#interface range gigabitethernet3/1-gigabitethernet5/1
Sw1(config-if-range)#switchport access vlan 107
Sw1(config-if-range)#interface gigabitethernet9/1
Sw1(config-if)#switchport mode trunk

Sw1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet9/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet9/1, changed state to up

Sw1(config-if)#switchport trunk allowed vlan 106,107
Sw1(config-if)#exit
Sw1(config)#
```

Рисунок 3.6 – Процедура конфігурування портів доступу та магістральних з'єднань на комутаційному вузлі Sw1

Аналогічний підхід до конфігурування застосовується і для решти периферійних пристроїв – від Sw2 до Sw6 включно. Процес налаштування цих комутаторів повторює раніше описаний алгоритм, однак потребує внесення корективів відповідно до специфіки кожного вузла.

Зокрема, під час термінального введення необхідно адаптувати назви та ідентифікатори мережевих інтерфейсів, а також вказати відповідні номери VLAN, що закріплені за конкретними портами згідно з розробленою схемою адресації та фізичного підключення кінцевого обладнання.

Завершальним етапом роботи з комутаційним обладнанням є фіксація внесених змін у енергонезалежній пам’яті пристроїв. Для цього в привілейованому режимі виконання застосовується команда copy running-config startup-config, яка переносить активний набір інструкцій з оперативної пам’яті (RAM) до пам’яті NVRAM. Такий крок гарантує збереження всіх налаштувань безпеки, параметрів VLAN та режимів роботи інтерфейсів, забезпечуючи стабільне відновлення функціонування мережі після будь-якого технічного переривання живлення.

3.1.2 Інструкції з налаштування головного комутатора

Конфігурування центрального вузла комутації розпочинається з етапу ідентифікації пристрою шляхом призначення йому унікального системного імені. Для реалізації цього завдання застосовується набір термінальних інструкцій, ідентичних тим, що використовувалися під час налаштування периферійних комутаторів (див. рисунок 3.1). Наступним кроком є впровадження комплексної системи безпеки, що включає встановлення парольного захисту для різних рівнів доступу та створення облікового запису для дистанційного керування через захищений протокол SSH. Процедура налаштування засобів автентифікації на головному комутаторі повністю дублює алгоритм дій, розроблений для комутаторів робочих груп (згідно з рисунками 3.2–3.4).

З огляду на те, що головний комутатор відіграє ключову роль у розподілі трафіку між віртуальними сегментами, на ньому необхідно розгорнути аналогічну базу даних VLAN. Для цього ініціалізуються відповідні ідентифікатори та назви підмереж із використанням команд, що представлені на рисунку 3.5. Це забезпечує логічну цілісність усієї мережевої структури та дозволяє пристрою коректно опрацьовувати тегований трафік, що надходить від інших вузлів інфраструктури.

Особливістю конфігурування інтерфейсів головного комутатора є необхідність врахування безпосередньо підключених до нього критично

важливих вузлів, а саме файлового сервера та основного маршрутизатора. Відповідні фізичні порти, що забезпечують зв'язок із цими пристроями, переводяться в режим доступу (access mode) для роботи в конкретних сегментах. Натомість усі інші активні інтерфейси, які виконують роль магістральних каналів зв'язку з іншими комутаторами мережі, потребують налаштування в транковому режимі. Повний перелік конфігураційних команд для коректного переведення портів у відповідні режими роботи наведено на рисунку 3.7.

```
SwG(config)#interface range gigabitethernet1/0/1-2
SwG(config-if-range)#switchport mode access
SwG(config-if-range)#interface range gigabitethernet1/0/3-8
SwG(config-if-range)#switchport mode trunk
SwG(config-if-range)#interface gigabitethernet1/0/1
SwG(config-if)#switchport access vlan 110
SwG(config-if)#interface gigabitethernet1/0/2
SwG(config-if)#switchport access vlan 111
SwG(config-if)#interface gigabitethernet1/0/3
SwG(config-if)#switchport trunk allowed vlan 106,107
SwG(config-if)#interface gigabitethernet1/0/4
SwG(config-if)#switchport trunk allowed vlan 102
SwG(config-if)#interface gigabitethernet1/0/5
SwG(config-if)#switchport trunk allowed vlan 101
SwG(config-if)#interface gigabitethernet1/0/6
SwG(config-if)#switchport trunk allowed vlan 104,105
SwG(config-if)#interface gigabitethernet1/0/7
SwG(config-if)#switchport trunk allowed vlan 103
SwG(config-if)#
```

Рисунок 3.7 – Специфікація параметрів конфігурування інтерфейсів центрального комутаційного вузла.

Завершальним етапом підготовки ядра мережі є активація функцій маршрутизації на центральному комутаторі. Для переведення пристрою в режим роботи на третьому рівні моделі OSI (Layer 3) застосовується директива ip routing, що дозволяє комутатору здійснювати обробку та пересилання пакетів між різними сегментами мережі.

Центральним елементом міжмережевої взаємодії є створення віртуальних інтерфейсів комутатора для кожної з наявних VLAN. Згідно з розробленим планом адресації, наведеним у таблиці 2.5, кожному такому інтерфейсу призначається роль шлюзу за замовчуванням. Як ідентифікатор

шлюзу використовується остання доступна IP-адреса у відповідному адресному просторі підмережі.

Повний перелік термінальних команд для ініціалізації SVI та призначення адрес шлюзів систематизовано на рисунку 3.8.

```
SwG(config)#ip routing
SwG(config)#interface vlan101
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan101, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up

SwG(config-if)#ip address 192.168.1.14 255.255.255.240
SwG(config-if)#interface vlan102
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan102, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up

SwG(config-if)#ip address 192.168.1.30 255.255.255.240
SwG(config-if)#interface vlan103
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan103, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan103, changed state to up

SwG(config-if)#ip address 192.168.1.38 255.255.255.248
SwG(config-if)#interface vlan104
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan104, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan104, changed state to up

SwG(config-if)#ip address 192.168.1.46 255.255.255.248
SwG(config-if)#interface vlan105
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan105, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan105, changed state to up

SwG(config-if)#ip address 192.168.1.54 255.255.255.248
SwG(config-if)#interface vlan106
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan106, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan106, changed state to up

SwG(config-if)#ip address 192.168.1.62 255.255.255.248
SwG(config-if)#interface vlan107
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan107, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan107, changed state to up

SwG(config-if)#ip address 192.168.1.70 255.255.255.248
```

Рисунок 3.8 – Процедура ініціалізації логічних інтерфейсів та конфігурування адрес шлюзів на центральному комутаторі

```
SwG(config-if)#interface vlan108
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan108, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan108, changed state to up

SwG(config-if)#ip address 192.168.1.78 255.255.255.248
SwG(config-if)#interface vlan109
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan109, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan109, changed state to up

SwG(config-if)#ip address 192.168.1.86 255.255.255.248
SwG(config-if)#interface vlan110
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan110, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan110, changed state to up

SwG(config-if)#ip address 192.168.1.90 255.255.255.252
SwG(config-if)#interface vlan111
SwG(config-if)#
%LINK-5-CHANGED: Interface Vlan111, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan111, changed state to up

SwG(config-if)#ip address 192.168.1.93 255.255.255.252
SwG(config-if)#exit
SwG(config)#
```

Рисунок 3.8 – Процедура ініціалізації логічних інтерфейсів та конфігурування адрес шлюзів на центральному комутаторі (продовження)

Наступним кроком є налаштування статичного маршруту за замовчуванням (Default Route). Цей параметр визначає шлях для всього мережевого трафіку, адреса призначення якого відсутня в поточній таблиці маршрутизації комутатора.

У даній топології роль «шлюзу останньої надії» виконує внутрішній інтерфейс маршрутизатора з IP-адресою 192.168.0.94. Саме на цю адресу головний комутатор SwG пересилатиме всі запити, що спрямовані у зовнішні мережі або інтернет.

Для реалізації цієї логіки в режимі глобальної конфігурації використовується наступна команда:

SwG(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.94

Це забезпечує цілісність маршрутизації та гарантує, що пристрої локальної мережі зможуть виходити за межі власних підмереж.

3.1.3 Інструкції з налаштування маршрутизатора

Завершальним етапом підготовки активної мережевої інфраструктури є конфігурування маршрутизатора, який виступає основним шлюзом для виходу в глобальну мережу Інтернет.

Процес налаштування розпочинається з базових параметрів ідентифікації та безпеки. Маршрутизатору присвоюється унікальне ім'я хоста (за алгоритмом, наведеним на рисунку 3.1), після чого впроваджується багаторівневий парольний захист і створюється обліковий запис адміністратора для шифрованого віддаленого доступу за протоколом SSH. Усі команди для захисту термінальних ліній та привілейованого режиму ідентичні тим, що застосовувалися для комутаторів (див. рисунки 3.2 – 3.4).

Основна частина конфігурації полягає у визначенні параметрів мережевих інтерфейсів:

- внутрішній інтерфейс (LAN). Для зв'язку з головним комутатором SwG призначається IP-адреса 192.168.0.94 (згідно з планом адресації у таблиці 2.5). Ця адреса стає точкою виходу для всього трафіку локальної мережі;

- зовнішній інтерфейс (WAN). Для взаємодії з обладнанням провайдера (ISP) на відповідному порту встановлюється публічна IP-адреса 161.12.9.10 із маскою підмережі /16.

Повний перелік команд для активації інтерфейсів та призначення відповідних адресних параметрів наочно представлено на рисунку 3.9.

Останнім кроком у забезпеченні повної мережевої зв’язності є налаштування логіки пересилання пакетів на маршрутизаторі. Це охоплює як вихід у глобальну мережу, так і зворотний зв’язок із внутрішніми сегментами.

Для того, щоб користувачі мали доступ до ресурсів Інтернету, на маршрутизаторі встановлюється «шлюз останньої надії». Будь-який пакет, адреса якого не належить до локальної мережі, автоматично пересилається на IP-адресу обладнання інтернет-провайдера (ISP). Це дозволяє пристрою

обробляти запити до зовнішніх серверів, не маючи повної картини адрес усього Інтернету.

```
R1(config)#interface gigabitethernet0/0
R1(config-if)#ip address 161.12.9.10 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#interface gigabitethernet0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up

R1(config-if)#interface gigabitethernet1/0
R1(config-if)#ip address 192.168.1.94 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Рисунок 3.9 – Конфігурування мережевих інтерфейсів маршрутизатора для внутрішнього та зовнішнього сегментів

Оскільки маршрутизатор безпосередньо не «бачить» окремі VLAN, створені на комутаторах, йому необхідно вказати шлях до них. Для цього прописуються статичні маршрути до кожної підмережі, описаної в таблиці 2.5:

- IP-адреси та маски відповідних VLAN;
- наступний стрибок (Next Hop) – усі запити спрямовуються на віртуальний інтерфейс головного комутатора з адресою 192.168.0.93.

Саме цей інтерфейс виступає в ролі «вхідних воріт» до внутрішньої інфраструктури компанії. Повна послідовність команд, що реалізує цей механізм взаємодії між зовнішнім шлюзом та ядром мережі, наведена на рисунку 3.10.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 161.12.1.0
R1(config)#ip route 192.168.1.0 255.255.255.240 192.168.1.93
R1(config)#ip route 192.168.1.16 255.255.255.240 192.168.1.93
R1(config)#ip route 192.168.1.32 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.40 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.48 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.56 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.64 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.72 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.80 255.255.255.248 192.168.1.93
R1(config)#ip route 192.168.1.88 255.255.255.252 192.168.1.93
R1(config)#
```

Рисунок 3.10 – Конфігурування статичних маршрутів до внутрішніх VLAN та зовнішнього шлюзу провайдера

Завершальним етапом конфігурування шлюзу є налаштування механізму трансляції мережевих адрес (NAT). Ця технологія відіграє критичну роль у сучасних мережах, оскільки дозволяє приховати внутрішню структуру адресного простору та забезпечити вихід у глобальну мережу багатьом пристроям через одну публічну IP-адресу. Окрім вирішення проблеми дефіциту IPv4-адрес, NAT слугує додатковим бар'єром безпеки, оскільки робить внутрішні вузли невидимими для прямих запитів іззовні.

Процес впровадження NAT складається з кількох послідовних кроків:

- маркування інтерфейсів. Необхідно чітко розмежувати ролі портів маршрутизатора, визначивши внутрішню сторону мережі (ip nat inside) та зовнішню сторону, що дивляться в бік провайдера (ip nat outside);

- визначення дозволеного трафіку. Створюється список контролю доступу (ACL), який ідентифікує діапазони внутрішніх IP-адрес, що мають право на трансляцію;

- активація трансляції. Встановлюється логічний зв'язок між визначеним ACL та зовнішнім інтерфейсом, найчастіше з використанням ключового слова overload (технологія PAT), що дозволяє підтримувати тисячі одночасних сесій.

Повна послідовність термінальних команд, що включає налаштування списків доступу та активацію динамічної трансляції для всіх внутрішніх підмереж, детально проілюстрована на рисунку 3.11.

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip nat outside
R1(config-if)#interface gigabitethernet 1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface gigabitethernet 0/0 overload
R1(config)#
```

Рисунок 3.11 – Конфігурування механізму трансляції мережевих адрес (NAT) та списків контролю доступу (ACL) на маршрутизатор

Для автоматизації процесу підключення бездротових клієнтів до мережі необхідно розгорнути службу DHCP на базі маршрутизатора. Це дозволить

мобільним пристроям, що працюють у сегменті VLAN 12, отримувати мережеві параметри без ручного втручання адміністратора.

Оскільки інтерфейс GigabitEthernet0/0/1 функціонує в режимі магістрального каналу (trunk), він здатен обробляти трафік від бездротових точок доступу, зберігаючи відповідні мітки VLAN. Процес конфігурування DHCP-сервера включає створення виділеного пулу адрес під назвою AP.

Основні етапи налаштування пулу AP:

- визначення мережі: Встановлення діапазону адрес, що відповідає підмережі VLAN 12 (згідно з таблицею адресації);
- призначення шлюзу (Default Router). Вказання IP-адреси віртуального інтерфейсу, через який пристрої виходитимуть за межі своєї підмережі;
- конфігурація DNS. Надання адрес серверів імен для коректного розв'язання доменних назв у мережі Інтернет;
- виключення адрес. Зарезервування статичних IP (наприклад, для самих точок доступу або шлюзу), щоб запобігти конфліктам адрес у мережі.

Деталізований перелік команд для створення та активації пулу DHCP наведено на рисунку 3.12.

```
R1(config)#ip dhcp pool AP
R1(dhcp-config)#network 192.168.1.96 255.255.255.128
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#exit
```

Рисунок 3.12 – творення та параметризація DHCP-пулу для бездротового сегмента мережі

3.2 Інструкції з налаштування засобів захисту мережі

Питання захисту мережевих пристроїв визначається як пріоритетне завдання як на етапі проектування, так і впродовж усього періоду експлуатації інформаційної системи. Нехтування засобами безпеки створює умови для виникнення руйнівних наслідків, що охоплюють широкий спектр загроз: від перехоплення контролю над комутаційним обладнанням до витоку

конфіденційних корпоративних даних. Такі інциденти призводять не лише до значних фінансових збитків, а й до втрати репутації та порушення безперервності критичних бізнес-процесів підприємства.

Ефективна модель захисту проектованої мережі базується на інтеграції низки взаємопов'язаних технічних механізмів:

- реалізація надійної автентифікації та авторизації. Передбачено встановлення складних та унікальних комбінацій паролів для доступу до всіх вузлів мережі. В основу доступу покладено принцип мінімальних привілеїв, згідно з яким персоналу та сервісам надається лише той обсяг повноважень, що є абсолютно необхідним для виконання конкретних обов'язків;

- мінімізація поверхні потенційної атаки. Основним методом є деактивація всіх протоколів та служб, що не використовуються в роботі. Оскільки кожен активний, але зайвий сервіс створює додатковий вектор для несанкціонованого входу, вимкнення надлишкових функцій суттєво підвищує загальну стійкість інфраструктури;

- автоматизація захисних функцій. Впровадження механізмів автоматичного підключення засобів безпеки гарантує їх постійну працездатність, що дозволяє нівелювати негативний вплив людського фактора;

- часовий контроль та моніторинг – встановлення лімітів на тривалість активних сесій забезпечує додатковий рівень нагляду. Окрім того, налаштування автоматичного інформування про підозрілу активність дозволяє адміністраторам здійснювати оперативне реагування на будь-які аномалії;

- у проекті мережі філії агрохолдингу «Контінентал Фармерз Груп» особливу увагу приділено активному обладнанню. Для комутаторів та маршрутизаторів розроблено багаторівневий захист;

- консольний пароль забезпечує безпеку при безпосередньому фізичному підключенні до пристрою через консольний порт;

- пароль віддаленого доступу (SSH) – захищає термінальні лінії під час дистанційного адміністрування. Використання протоколу SSH є обов'язковим,

оскільки він, на відміну від Telnet, забезпечує повне шифрування трафіку керування;

- пароль привілейованого режиму – створює додатковий бар'єр для доступу до глобальних налаштувань обладнання, дозволяючи вносити зміни лише авторизованим фахівцям.

Для створення всебічного захисту інфраструктури філії впроваджуються додаткові заходи безпеки. Управління обліковими записами передбачає регулярну ревізію прав доступу, видалення профілів звільнених співробітників та впровадження двофакторної автентифікації (2FA/MFA) для входу в критично важливі системи, такі як файловий сервер або фінансові бази даних.

Захист робочих станцій реалізується через розгортання актуального антивірусного програмного забезпечення з функцією автоматичного оновлення баз. На кожному хості та сервері активуються брандмауери для блокування небажаного вхідного трафіку.

Обов'язковим є системне оновлення операційних систем та прикладного ПЗ для усунення відомих вразливостей. Додатково встановлюється контроль над використанням зовнішніх USB-носіїв для запобігання поширенню шкідливого коду.

Керування мережевим трафіком базується на логічному розділенні мережі на VLAN, що локалізує можливі загрози в межах одного сегмента. На маршрутизаторі застосовуються списки контролю доступу (ACL), які фільтрують потоки даних між підмережами та зовнішнім світом за принципом «заборони всього, що не дозволено явно». Також розглядається можливість інтеграції систем IDS/IPS для виявлення вторгнень у реальному часі.

Стійкість до втрати інформації забезпечується автоматизованим резервним копіюванням за стратегією 3-2-1 (три копії, два типи носіїв, одна копія поза межами офісу). Цілісність бекапів підтверджується шляхом регулярних тестових відновлень. Для раннього виявлення загроз налаштовується централізований збір логів (журналів подій) з усіх вузлів мережі.

Завершальним елементом безпеки є впровадження чіткої політики використання ресурсів та навчання персоналу основам кібергігієни. Це включає розпізнавання фішингових розсилок та суворе дотримання плану дій у разі виявлення інцидентів. Впровадження цих заходів дозволяє філії агрохолдингу «Контінентал Фармерз Груп» забезпечити стабільну роботу та захистити корпоративні дані від сучасних кіберзагроз.

3.3 Моделювання мережі d Cisco Packet Tracer

Після завершення етапу проєктування здійснюється перехід до безпосереднього налаштування обраних мережевих компонентів через термінальний доступ або інтерфейс командного рядка (CLI). Для відпрацювання архітектури мережі та перевірки її працездатності використовується програмний комплекс Packet Tracer, який забезпечує імітацію функціонування широкого переліку пристроїв: робочих станцій, серверів, Ethernet-комутаторів та маршрутизаторів.

Процес моделювання розпочинається з розміщення мережевих елементів на робочій області та їх з’єднання згідно з логічною схемою (рисунок 2.1). Під час вибору середовища передачі даних дотримується правило: пристрої, що функціонують на одному рівні моделі OSI, з’єднуються перехресним (crossover) кабелем, тоді як пристрої різних рівнів — прямим кабелем.

Комутаційні порти задіюються відповідно до схеми фізичних з’єднань та розподілу по VLAN, наведених у таблиці 3.1. Для обладнання, що працює через бездротові канали зв’язку, передбачено встановлення Wi-Fi-адаптерів. Такі пристрої не потребують фізичного кабельного підключення до комутатора, проте для них здійснюється програмне резервування відповідного порту.

Наступна стадія передбачає призначення статичних IP-адрес кінцевим вузлам згідно з розробленим планом адресації. Конфігурування мережевих параметрів виконується у налаштуваннях кожного ПК (вкладка "Desktop", застосунок "IP Configuration"). Для кожного пристрою вказується унікальна IP-

адреса, відповідна маска підмережі та адреса шлюзу за замовчуванням. Як адресу DNS-сервера для всієї мережі встановлено значення 8.8.8.8 (сервер S1), що продемонстровано на рисунку 3.13.

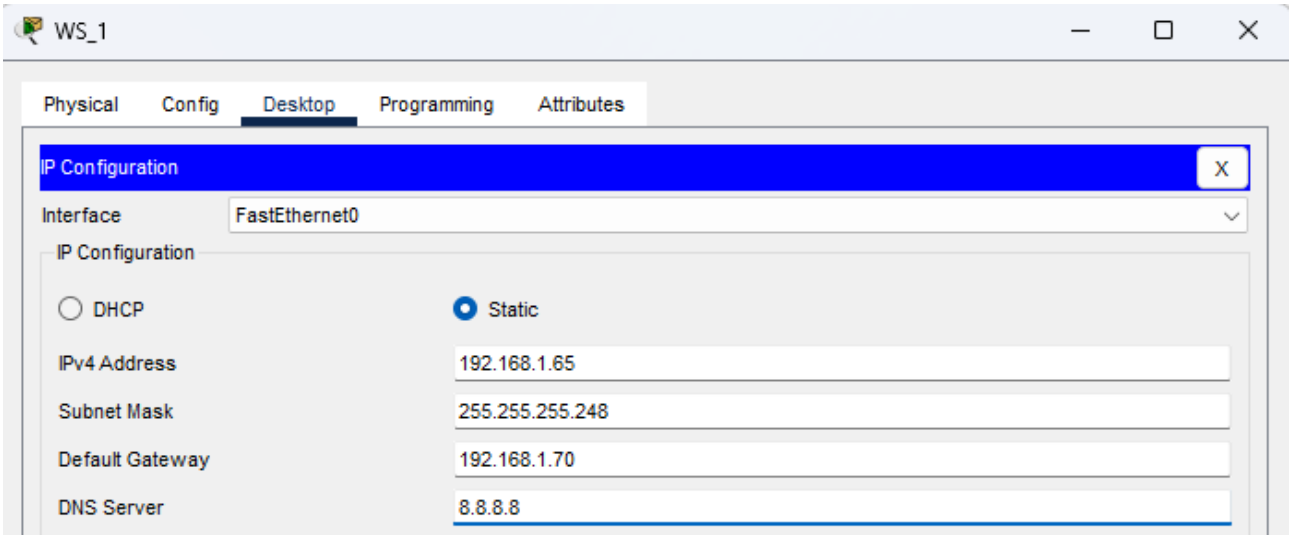

Рисунок 3.13 – Конфігурування статичних мережевих параметрів на прикладі робочої станції WS_1

Налаштування бездротових точок доступу здійснюється через графічний інтерфейс конфігурування у вкладці «Config». У підрозділі «Port 1» виконується введення ідентифікатора бездротової мережі, а також вибір параметрів безпеки.

Для захисту каналу зв’язку встановлюється тип автентифікації WPA2-PSK, вказується пароль та обирається алгоритм шифрування. Приклад заповнення відповідних параметрів для точки доступу AP1 наведено на рисунку 3.14.

Завершальним етапом підготовки клієнтського обладнання є конфігурування бездротових адаптерів на кінцевих пристроях. Для кожного такого вузла вказується відповідний ідентифікатор SSID та пароль доступу, що забезпечує їхнє з'єднання з визначеною точкою доступу згідно із загальною схемою мережі.

Після завершення налаштування кінцевих точок здійснюється перехід до конфігурування активного обладнання. Процес розпочинається з комутаторів окремих сегментів. Основні завдання на цьому етапі охоплюють:

- призначення ідентифікаторів пристроїв (Hostname);
- розподіл фізичних портів за відповідними віртуальними мережами;
- впровадження засобів безпеки через встановлення паролів автентифікації.

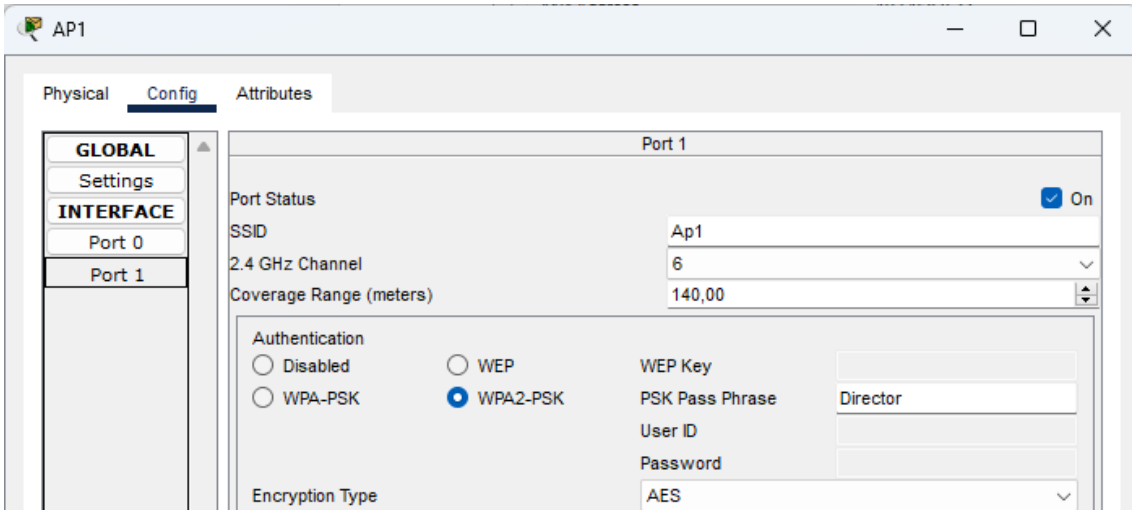

Рисунок 3.14 – Налаштування параметрів безпеки та ідентифікації бездротової мережі на точці доступу AP1

Для реалізації цих налаштувань використовується вкладка CLI (Command Line Interface), де вводиться послідовність команд операційної системи Cisco IOS, що була детально описана в розділі 3.1. За аналогічним принципом здійснюється конфігурування інтерфейсів маршрутизатора.

Важливим елементом мережевої логіки є встановлення маршруту за замовчуванням. Це дозволяє спрямовувати весь трафік, адресати якого знаходяться поза межами локальної інфраструктури, на інтерфейс обладнання інтернет-провайдера. Повна візуалізація готового проекту мережі наведена у додатку В.

3.4 Тестування роботи побудованої моделі мережі

Для верифікації коректності налаштувань та аналізу взаємодії компонентів системи у програмному комплексі Cisco Packet Tracer передбачено перехід до режиму симуляції. Активація цього режиму здійснюється натисканням кнопки Simulation у правому нижньому куті робочого простору, після чого запускається процес візуалізації пакетів за допомогою клавіші Play.

Перевірка мережевої зв'язності між різними сегментами інфраструктури виконується шляхом тестування з'єднань із комп'ютерами, які розподілені по іншим шести підмережам. Для реалізації цього сценарію задіюється одна з робочих станцій — наприклад, вузол PC61, що функціонує у межах підмережі Net 4. У вікні конфігурації обраного пристрою на вкладці Desktop запускається термінальний додаток Command Prompt.

Діагностика здійснюється шляхом послідовного введення команди ping для кожної цільової адреси кінцевих пристроїв та серверної платформи. Процес тестування розпочинається з відправки ICMP-запитів на адресу сервера — 192.168.0.89. Приклад виконання цієї процедури та фіксації успішного обміну пакетами між різними підмережами наочно представлено на рисунку 3.15.

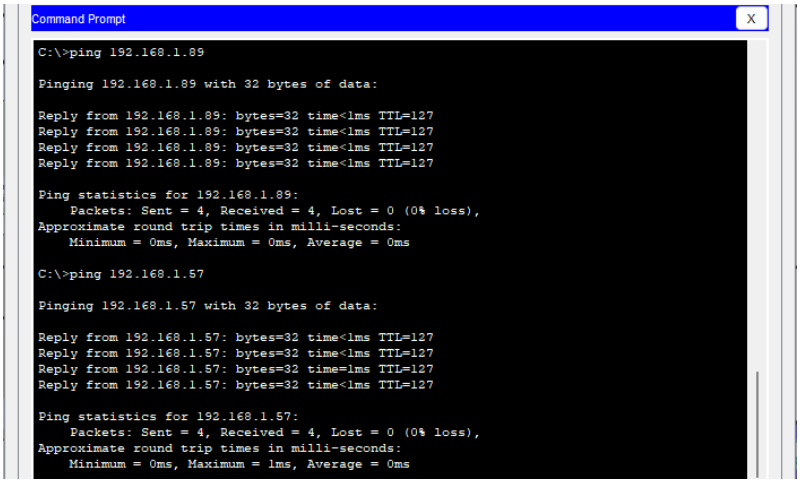

Рисунок 3.15 – Тестування міжмережевої взаємодії за допомогою утиліти ping на прикладі вузла PC61

Для детального аналізу всього шляху проходження інформаційних пакетів у межах створеної інфраструктури та фіксації часових затримок на кожному проміжному вузлі застосовується утиліта трасування маршруту.

Запуск команди tracert у командному рядку кінцевого пристрою дозволяє поетапно відстежити всі переходи (хопи) від початкової робочої станції через комутатори ядра та маршрутизатор до цільового вузла. Цей інструмент дає змогу наочно перевірити коректність відпрацювання налаштованих статичних маршрутів та виявити потенційні проблеми з доставкою пакетів на конкретних ділянках мережі.

Приклад успішного виконання трасування та фіксації всіх проміжних адрес на шляху до віддаленої підмережі наведено на рисунку 3.16.

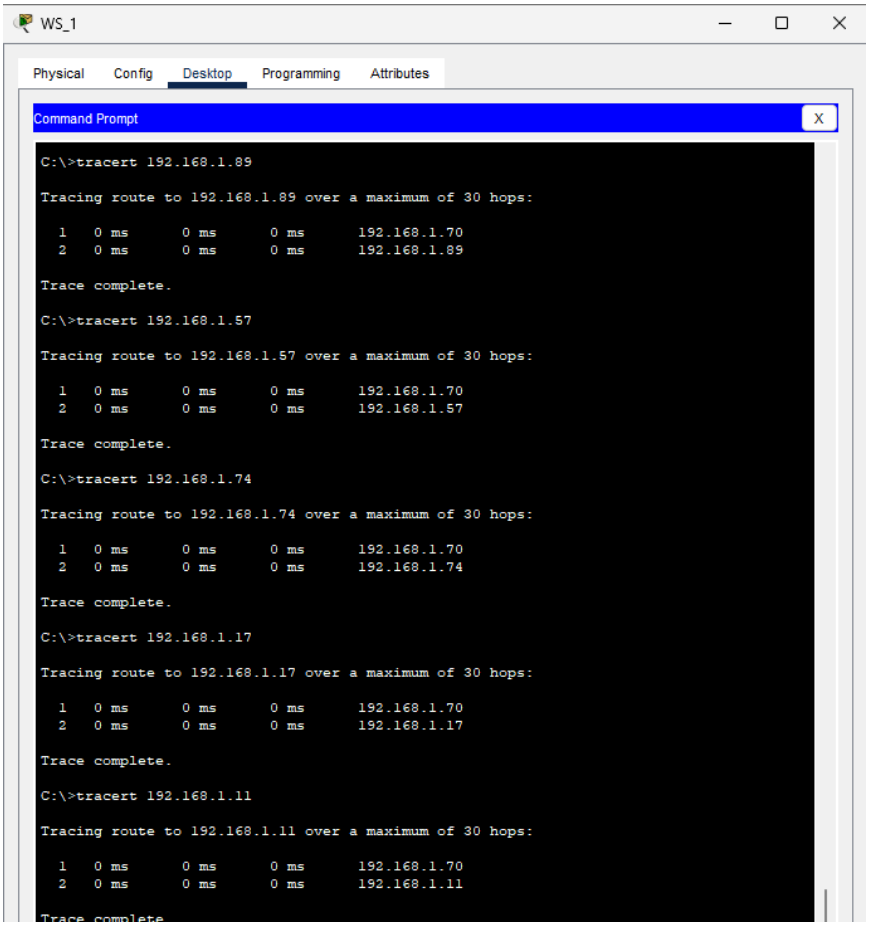

Рисунок 3.16 – Визначення маршруту проходження пакетів за допомогою команди tracert

Результати проведеного тестування мережевої інфраструктури філії агрохолдингу «Континентал Фармерз Груп» підтвердили повну працездатність системи. Успішне проходження всіх діагностичних команд свідчить про коректність побудови логічної схеми та безпомилкове налаштування статичної маршрутизації.

Для поглибленого аналізу стану мережевих таблиць та верифікації шляхів передачі даних використовується системна команда show ip route. Її виконання здійснюється безпосередньо на маршрутизаторі у привілейованому режимі адміністрування. Ця операція дозволяє вивести на екран актуальну таблицю маршрутизації, де відображаються всі безпосередньо підключені підмережі (C — connected) та маршрути, встановлені адміністратором вручну (S — static).

Аналіз результатів, представлених на рисунку 3.17, підтверджує наявність записів про всі сегменти локальної мережі. Наявність цих даних у таблиці маршрутизації гарантує, що пристрій володіє необхідною інформацією для коректного пересилання пакетів між різними VLAN та зовнішніми мережами.

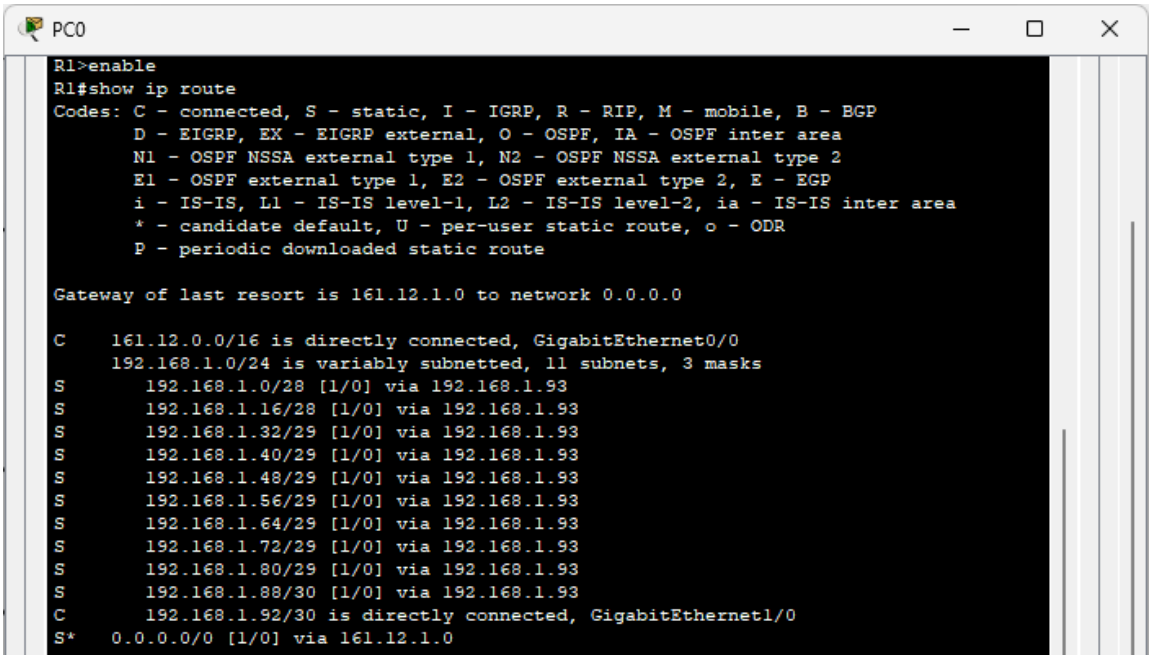

Рисунок 3.17 – Відображення таблиці маршрутизації пристрою для перевірки мережевих шляхів

4 ЕКОНОМІЧНИЙ РОЗДІЛ

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Для визначення загальної тривалості науково-дослідної роботи (НДР) потрібно зібрати дані про час, затрачений на кожну операцію технологічного процесу. Ця інформація буде відображена в Таблиці 4.1. Збором даних займатимуться керівник, інженер і технік.

У таблиці 4.1 відображено етапи технологічного процесу та середній час, необхідний для їхнього завершення.

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	10
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі філії агрохолдингу. Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури філія агрохолдингу «Контінентал Фармерз Груп» для сегментування локальної мережі на підмережі.	Інженер	15

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	25
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	20
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
		Разом	75

Сумарний час виконання операцій технологічного процесу проектування мережі становить 75 години, з них 10 годин – робота керівника проекту, 40 години – інженера, 25 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 обмежена.

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 – 220 грн, інженера – 180 грн./год. а для техніка – 150 грн./год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 10 \cdot 220 = 2200$ грн.
- інженера – $З_{осн2} = 40 \cdot 180 = 7200$ грн.
- техніка – $З_{осн3} = 25 \cdot 150 = 3750$ грн.

Сумарна основна заробітна плата становить

$$З_{осн}=2200 +7200 + 3750 =13150 \text{ грн.}$$

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 $З_{дод1}=2200 \cdot 0,13= 286$ грн.
- інженера $З_{дод1}=7200 \cdot 0,13= 936$ грн.
- техніка $З_{дод3}=3750 \cdot 0,13= 487,5$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=286 + 936 + 487,5 = 1709,5 \text{ грн.}$$

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:

$$В_{о.п.}= 13150 + 1709,5 = 14859,5 \text{ грн.}$$

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.

$$В_{с.з} = 14859{,}5 \cdot 0{,}22 = 3269{,}09 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п	Категорія працівників	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн
		Тариф ставка, грн.	К-сть відпрац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	220	10	2200	286		
2	Інженер	180	40	7200	936	-	-
3	Технік	150	25	3750	487,5	-	-
Разом				13150	1709,5	3269,09	18477,51

Отже, загальні витрати на оплату праці становлять 18477,51 грн.

4.3 Розрахунок матеріальних витрат

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

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

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	Комутаційна шафа Hypernet WMNC-6U-FLAT	шт.	1	3595	3595
2	Патчпанель 24 порти, кат. 6	шт.	1	1250	1250
3	Розетка RJ-45 (категорія 6)	шт.	32	118	3 776
4	Розетка підлогова RJ-45 (категорія 6)	шт.	15	195	2925
5.	Роз’єм 8P8C (100 шт)	шт.	1	595	595
6	Короб (середня ціна для різного січення)	м.	161	115	18515
7	Короб пілоговий	м.	16	195	3120
8	Кабель UTP (кат. 6) (бухта)	шт.	3	5353	16059
8	Патчкорди (кат. 6)	шт.	32	51	1632
9	Кабель опотоволоконний	м.	3	33	99
10	Конектор SC	шт.	2	38	76
11	Маршрутизатора Cisco ISR4221/K9	шт.	1	24706	24706
12	Головний комутатор Cisco Catalyst WS-C3560CX-12XPD-S	шт.	1	65345	65345
13	Комутатор робочих груп Cisco Catalyst C1000-16T-2G-L	шт.	4	27313,75	109255
14	Безпровідна точка доступу TP-LINK EAP225	шт.	1	2999	2999
14	Джерело безперебійного живлення APC Back-UPS Pro 1200VA	шт.	1	3680	3680
Р а з о м			-	-	257627

Отже, загальна сума матеріальних витрат на розробку мережі становить 257627 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,

$$Т_В = 257627 \cdot 0,08 = 20610,16 \text{ грн.}$$

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 - 26500 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{26500 \cdot 0{,}04}{150} \cdot 10 = 106 \text{ грн}$$

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.

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

де $Н_В$ – накладні витрати.

$$Н_В = 14859{,}5 \cdot 0{,}4 = 5943{,}8 \text{ грн.}$$

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)	14859,5	4,91
Відрахування на соціальні заходи	3269,09	1,08
Матеріальні витрати	257627	85,18
Витрати на електроенергію	35	0,01
Транспортні витрати	20610,16	6,81
Амортизаційні відрахування	106	0,04
Накладні витрати	5943,8	1,97
Собівартість	302450,55	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 $С_В$=302450,55 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:

$$Ц = 302450{,}55 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 471822{,}86 \quad грн$$

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;

$$П = 302450{,}55 - 299572{,}02 = 169372{,}31 \; грн.$$

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

$$E_p = \frac{П}{С_в} = \frac{167760{,}33}{299572{,}02} = 0{,}56 \quad (4.14)$$

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.	302450,55 грн.
2.	Плановий прибуток, грн.	169372,31 грн.
3.	Ціна, грн.	471822,86 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп'ютерної мережі для аграрного підприємства Філія агрохолдингу «Контінентал Фармерз Груп» становить 471822,86 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 Розрахунок системи штучного освітлення для приміщення філії агрохолдингу "Контінентал Фармерз Груп" в Тернопільській області, де міститься найбільше ПК

Для проведення розрахунку системи штучного освітлення обрано приміщення відділу логістики філії агрохолдингу "Контінентал Фармерз Груп". Згідно із фізичною топологією розміщення обладнання (див. додаток В), це приміщення характеризується найбільшою концентрацією комп'ютерної техніки (11 робочих станцій, ПК_35 – ПК_45), що вимагає створення комфортного світлового середовища для запобігання зоровій втомлюваності працівників.

Вихідні дані приміщення згідно з планом приміщення (див. додаток А):

- довжина приміщення А= 7,0 м (відстань між осями В та Е);
- ширина приміщення В= 8,0 м (відстань між осями 4 та 7);
- площа приміщення (S) визначається як:

$$S = A \times B = 7,0 \times 8,0 = 56,0 \text{ м}^2;$$

- висота приміщення Н=3,0 м;
- висота робочої поверхні $h_p = 0,8$ м (стандартна висота робочого столу).

Відповідно до ДБН В.2.5-28:2018 «Природне і штучне освітлення», для приміщень, де виконуються роботи з дисплеями та комп'ютерами, нормативна освітленість ($E_{норм}$) на робочій поверхні повинна становити не менше 500 лк [9].

Крім того, показник дискомфорту (UGR) не повинен перевищувати 19, а коефіцієнт пульсації світлового потоку – не більше 5%.

Враховуючи вимоги до енергоефективності та якості освітлення, для розрахунку обрано сучасні світлодіодні (LED) панелі розміром 600х600 мм, які вбудовуються в стелю типу «Армстронг» (див рис. 5.1). Характеристики обраного світильника: потужність Р = 40 Вт, світловий потік одного світильника $F_{св}$ = 4000 лм, колірна температура 4000 К (нейтральне біле світло).

Рисунок 5.1 – Світильник типу «Армстронг» 600х600

Оскільки освітлення має бути рівномірним по всій площі відділу логістики (робочі місця розташовані по всій площі кімнати), розрахунок проводимо методом коефіцієнта використання світлового потоку. Цей метод дозволяє визначити необхідну кількість світильників для забезпечення заданої освітленості з урахуванням відбиття світла від стін, стелі та підлоги.

Розрахунок освітлення здійснено методом коефіцієнта використання. Згідно із даною методикою на першому кроці необхідно визначити розрахункову висоту підвісу світильника ($h_{розр}$).

Розрахункова висота – це відстань від світного елемента до робочої поверхні. Оскільки світильники вбудовані в стелю, звис світильника дорівнює нулю.

$$h_{\text{розр}} = H - h_{\text{р}} \tag{5.1}$$

де

H – загальна висота приміщення (3,0 м);

h_p – висота робочої поверхні (0,8 м).

З формули (5.1):

$$h_{\text{розр}} = 3{,}0 - 0{,}8 = 2{,}2 \text{ м}$$

Другий крок полягає у визначені індексу приміщення (i). Індекс приміщення характеризує геометрію кімнати і впливає на частку світла, що досягає робочої поверхні і визначається за формулою:

$$i = \frac{A \cdot B}{h_{\text{розр}} \cdot (A + B)} \tag{5.2}$$

Звідси

$$i = \frac{7 \cdot 8}{2{,}2 \cdot (7 + 6)} = \frac{56}{2{,}2 \cdot 13} = 1{,}9$$

Наступний крок – визначення коефіцієнта використання світлового потоку (η), що знаходиться за довідниковими таблицями залежно від індексу приміщення (i = 1,90) та коефіцієнтів відбиття поверхонь [3]. Для стандартних умов світлого офісу приймаємо коефіцієнт відбиття стелі 70%, стін 50% та підлоги 30%. Згідно з довідниками, для заданих параметрів коефіцієнт використання становить 0,60 [3].

Після визначення коефіцієнта використання світлового потоку встановлюється необхідна кількість світильників за основною формулою методу коефіцієнта використання:

$$N = \frac{E_{\text{Н}} \cdot S \cdot K_{\text{з}} \cdot Z}{F_{\text{св}} \cdot \eta} \qquad (5.3)$$

де

$E_н$ – це нормативна освітленість у люксах (лк), встановлена державними будівельними нормами для конкретного типу діяльності (наприклад, 400 лк для роботи за комп'ютером) [9];

S – загальна площа приміщення в квадратних метрах, яку необхідно наситити штучним світлом. Згідно формули S = A x B = 7,0 x 8,0 = 56,0 м² ;

$K_з$ – коефіцієнт операційного запасу, який заздалегідь закладається в математичну модель для компенсації майбутнього старіння світлодіодних елементів, поступового вигорання люмінофору та неминучого запилення захисного скла світильника за роки експлуатації. Приймаємо $K_з$= 1,4;

Z – позначає коефіцієнт нерівномірності освітлення, який коригує розрахунок у більшу сторону, враховуючи, що безпосередньо під самою лампою світла завжди більше, ніж у проміжках між рядами чи у кутках кімнати;

$F_{св}$ – означає номінальний світловий потік одного обраного світильника в люменах, який показує повний об'єм світлової енергії, що її випромінює прилад у простір при підключенні до мережі. Для обраного світильника

$F_{св}$ = 4000 лм;

η – відображає коефіцієнт використання світлового потоку, який є відсотковою величиною, що показує, яка саме частина сукупного світла ламп реально долетить до робочих столів логістів після багаторазового відбиття від світлої стелі, стін та підлогового покриття. На основі обчисленого індексу приміщення і = 1,47 та заданих коефіцієнтів відбиття пиймаємо $\eta = 0{,}6$.

Відповідно до формули (5.2) необхідна кількості світильників:

$$N = \frac{500 \cdot 56 \cdot 1{,}4 \cdot 1{,}1}{4000 \cdot 0{,}60} = \frac{43120}{2400} = 17{,}96 \approx 18$$

Для забезпечення симетричного монтажу приладів у прямокутній кімнаті та досягнення абсолютно рівномірного розподілу світлових променів над комп'ютерними столами логістів, теоретичне число 17,96 округлюється в більшу сторону до найближчого оптимального парного числа, що становить 20 світильників. Отже,

$$N = 20 \text{ штук}$$

На четвертому етапі виконується обов'язковий перевірочний розрахунок фактичної освітленості, яку створюватиме спроектована система після фізичного встановлення п'ятнадцяти світильників. Розрахунок проводиться за зворотною формулою, де шуканою величиною є реальна освітленість:

$$E_{\text{фак}} = \frac{N \cdot F_{\text{св}} \cdot \eta}{S \cdot K_{\text{з}} \cdot \text{Z}} \qquad (5.4)$$

Підставимо у формулу прийняту цілу кількість світильників 15 та всі інші незмінні коефіцієнти:

$$E_{\text{фак}} = \frac{15 \cdot 4000 \cdot 0{,}6}{42 \cdot 1{,}4 \cdot 1.1} = \frac{36000}{64{,}68} \approx 556{,}6 \text{ лк}$$

Для перевірки відповідності будівельним нормам знайдемо відносне відхилення фактичної освітленості від норми за математичною формулою:

$$\Delta E = \frac{E_{\text{фак}} - E_{\text{Н}}}{E_{\text{Н}}} \cdot 100\% = \frac{556{,}6 \ - 500}{500} \cdot 100\% = 11{,}3\% \qquad (5.5)$$

Отримане відхилення вказує на те, що фактична освітленість перевищує норму на 11,3%. Згідно з вимогами ДБН В.2.5-28:2018, відхилення реальних рівнів освітленості від встановленого нормативу допускається в суворих межах

від мінус 10% до плюс 20% [9], що доводить повну відповідність розробленого проекту державним стандартам.

На етапі просторового проектування виконується розробка схеми розміщення п'ятнадцяти світлодіодних панелей на площині стелі відділу логістики відповідно до його реальних геометричних розмірів, які згідно з будівельним планом становлять 7,0 м уздовж довгої стіни (між осями В–Е) та 8,0 м уздовж короткої стіни (між осями 4–7) (див. додаток А).

Розрахунок геометричних параметрів для розміщення джерел світла вздовж довгої стіни приміщення, де довжина становить 7,0 м і передбачено розташування 5 світильників у кожному ряду, починається з обчислення відстані між осями сусідніх світильників у ряду, яка позначається як L_A. Ця величина визначається за математичною формулою:

$$L_A = \frac{7,0}{4} = 1,75 \text{ м} \quad (5.6)$$

Після цього розраховується точна відстань від крайніх світильників до торцевих стін приміщення, що позначається як l_A, яка за правилами світлотехніки становить половину кроку між приладами і обчислюється за формулою:

$$l_A = \frac{L_A}{2} = \frac{1,4}{2} = 0,875 \text{ м} \quad (5.7)$$

Наступним кроком є обчислення параметрів розміщення обладнання вздовж короткої стіни відділу логістики, яка має чисту ширину 6,0 м, де для забезпечення рівномірності світлового поля запроектовано 3 паралельні ряди світильників.

Відстань між паралельними рядами світильників позначається як L_B і визначається шляхом ділення загальної ширини на кількість рядів за формулою:

$$L_B = \frac{8,0}{5} = 1,6 \text{ м} \quad (5.8)$$

Для запобігання утворенню щільних тіней біля меж робочої зони розраховується відстань від крайніх рядів світильників до поздовжніх стін

приміщення, яка позначається як l_B і становить половину міжрядного простору згідно з формулою:

$$l_B = \frac{L_B}{2} = \frac{1{,}6}{2} = 0{,}8 \text{ м} \quad (5.9)$$

Такий чіткий лінійний розподіл дозволяє сформувати симетричну монтажну сітку на підвісній стелі «Армстронг», що повністю відповідає графічній план-схемі трасування електричних мереж та забезпечує оптимальні умови для тривалої роботи персоналу за комп'ютерами від PC_35 до PC_45. На рисунку 5.2 представлено схему розташування світильників у приміщенні відділу логістики філії агрохолдингу "Контінентал Фармерз Груп".

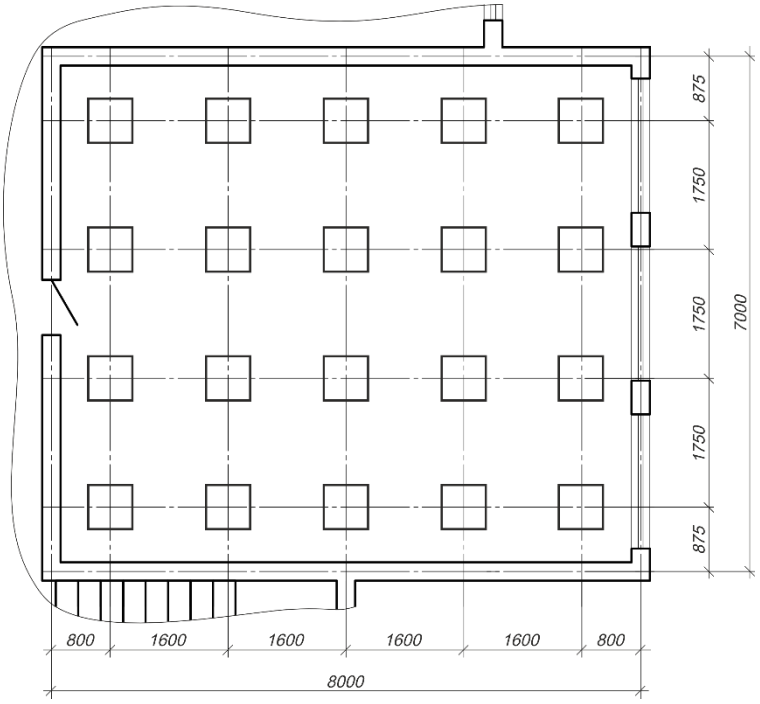

Рисунок 5.2 – Схема встановлення світильників в приміщенні відділу логістики

На заключному етапі обчислюються електричні характеристики проектованої системи освітлення відділу логістики. Загальна споживана електрична потужність усієї системи визначається як добуток кількості світильників на потужність одного приладу:

$$P_{\text{заг}} = N \cdot P = 20 \cdot 40 = 600 \text{ Вт} \quad (5.10)$$

Питома встановлена потужність штучного освітлення розраховується як відношення загальної електричної потужності до повної площі кімнати:

$$p = \frac{P_{\text{заг}}}{S} = \frac{600}{42} = 14{,}28 \text{ Вт/м}^2 \quad (5.11)$$

Отриманий показник питомої потужності, який після округлення становить 14,3 Вт/м², повністю задовольняє сучасні європейські та державні вимоги щодо раціонального використання паливно-енергетичних ресурсів та енергоефективності адміністративно-офісних будівель, що підтверджує інженерну та економічну доцільність розробленого проекту для філії агрохолдингу "Контінентал Фармерз Груп".

5.2 Особливості заходів електробезпеки в філії агрохолдингу "Контінентал Фармерз Груп" в Тернопільській області

Специфіка діяльності філії агрохолдингу передбачає наявність різнопланових об’єктів, кожен з яких має унікальні умови навколишнього середовища. Згідно з Правилами улаштування електроустановок (ПУЕ) та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів» [10], всі приміщення та території філії розділені на три категорії:Проте концентрація великої кількості комп'ютерної техніки формує специфічні техногенні ризики:

- приміщення без підвищеної небезпеки/ Сюди відносяться адміністративно-управлінський блок, кабінети відділу логістики, каса та диспетчерські. Тут відсутні агресивні середовища, висока вологість чи струмопровідний пил. Основна загроза – велика концентрація оргтехніки та ймовірність пошкодження ізоляції живильних шнурів;
- приміщення з підвищеною небезпекою. До цієї групи належать пункти технічного обслуговування (ПТО), ремонтно-механічні майстерні (РММ) для сільськогосподарської техніки та критих автостоянок. Небезпека обумовлена наявністю струмопровідної підлоги (бетон, земля), металевих конструкцій, сирості (відносна вологість повітря часто перевищує 75 %) та можливості

одночасного дотику людини до корпусу верстата чи трактора і заземлених металоконструкцій будови;

- особливо небезпечні приміщення та зони. Сюди відносяться відкриті майданчики (заправні станції, вагові комплекси), акумуляторні станції, а також елеваторні комплекси, зерносушарки та склади підлогового зберігання зерна. Останні, згідно з класифікацією, утворюють пожежо- та вибухонебезпечні зони (класи Зона 21 та Зона 22 через постійну присутність вибухонебезпечного органічного зернового пилу).

Враховуючи високу розгалуженість електричних мереж філії (0,4 кВ та 10 кВ) та роботу важкої техніки, на підприємстві реалізовано комплекс інженерно-технічних засобів захисту.

Для захисту від непрямого дотику (при пробої ізоляції на корпус) всі об'єкти філії переведені на сучасні схеми заземлення:

- в адміністративній будівлі та РММ застосовано систему TN-S, де нульовий робочий (N) і захисний (PE) провідники розділені по всій мережі;

- опір контуру заземлення для електроустановок напругою 380/220 В становить $R_{заз} \leq 4$ Ом;

- усі металеві частини обладнання (рампи елеваторів, металеві корпуси зерносушарок, станини верстатів у РММ) підключені до магістралей заземлення за допомогою системи вирівнювання потенціалів.

Залежно від технологічної зони філії, автоматичний захист налаштовано на різні рівні чутливості:

- побутова та офісна мережа. Розеточні групи захищені пристроями захисного вимкнення (ПЗВ) або дифавтоматами зі струмом спрацьовування 30 мА для гарантованого захисту життя людини при прямому дотику;

- ремонтні зони та вологі приміщення. Лінії живлення ручного електроінструменту верстатного парку обладнані ПЗВ зі струмом витоку 10-30 мА;

- елеватори та пожежонебезпечні зони. Встановлено протипожежні ПЗВ зі струмом спрацьовування 100-300 мА, які відсікають живлення при

пошкодженні кабелю, запобігаючи виникненню електричної дуги, що може підірвати зерновий пил.

Під час проведення ремонтних робіт усередині металевих бункерів елеваторів, силосів, силосних ям та в оглядових канавах РММ, використання напруги 220 В суворо заборонено. Живлення переносних світильників та ручного інструменту в цих зонах здійснюється через знижувальні трансформатори напругою 12 В або 36 В.

На елеваторі та сушильному комплексі філії "Контінентал Фармерз Груп" застосовується електрообладнання виключно у вибухозахищеному виконанні із високим ступенем захисту оболонки (не нижче IP64/IP65), що унеможливлює потрапляння пилу всередину пускачів, двигунів норій та конвеєрів. Кабельні лінії прокладені в сталевих герметичних трубах або суцільних металевих лотках.

Електробезпека на підприємстві підтримується чітким розподілом обов'язків та регулярним навчанням персоналу. Залежно від доступу до техніки, працівники філії діляться на три категорії:

- I група (неелектротехнічний персонал). Трактористи, водії, різноробочі та офісні працівники (включаючи відділ логістики). Проходять щорічний інструктаж на робочому місці із записом у журналі, без видачі посвідчень;
- II-III групи (електротехнологічний та персонал обслуговування). Зварювальники, оператори сушильних комплексів, верстатники. Мають право працювати з електроустановками та підключати ручний інструмент;
- IV-V групи (інженерно-технічний персонал). Головний енергетик філії та старші електрики. Мають право видавати наряди-допуски на виконання особливо небезпечних робіт в електромережах до і вище 1000 В.

Будь-які планові чи аварійні роботи в мережах філії (наприклад, заміна двигуна транспортера на елеваторі) виконуються виключно за нарядом-допуском після виконання п'яти обов'язкових технічних етапів: відключення напруги, вивішування заборонних плакатів («Не вмикати! Працюють люди»), перевірки відсутності напруги, встановлення переносних заземлень та огородження робочого місця.

Впровадження вищеописаних технічних заходів (зокрема вибухозахищеного виконання на токах зернообробки та диференційного розділення офісних мереж) разом із суворим організаційним контролем забезпечує нульовий рівень виробничого травматизму від дії електричного струму в філії агрохолдингу "Контінентал Фармерз Груп".

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проект локальної мережі аграрного підприємства філії агрохолдингу "Контінентал Фармерз Груп". Основні технічні характеристики розробленого проекту локальної мережі:

- фізична топологія – «гібридна», що поєднує «ієрархічну розширену зірку» та комірчасту безпровідну топології;
- технології використані для розробки мережі - IEEE 802.3ab, IEEE 802.11ac, IEEE 802.1Q;
- маршрутизатор-шлюз – Cisco ISR4221/K9;
- комутатори ядра локальної мережі – Cisco WS-C3560CX-8XPD-S;
- комутатори робочих груп – Cisco Catalyst C1000-16T-2G-L;
- 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.

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, 2011. – 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 2016 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: 5.06.2026.

11. ДСТУ EN 50110-1:2014. Експлуатація електроустановок. Частина 1: Загальні вимоги. URL: https://standards.ua/50110-1. (Дата звернення: 14.05.2026)

12. ДБН В.2.5-28-2018 "Природне і штучне освітлення". URL: https://e-construction.gov.ua/laws_detail/30749587325562408 33?doc_type=2. (Дата звернення: 14.05.2026)

13. App.Diagrams сайт для створення схем URL: https://app.diagrams.net. (Дата звернення: 14.05.2026)

14. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 16.05.2026)

15. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 16.05.2026)

ДОДАТКИ

Додаток А. План приміщення будівлі філії агрохолдингу "Континентал Фармерз Груп"

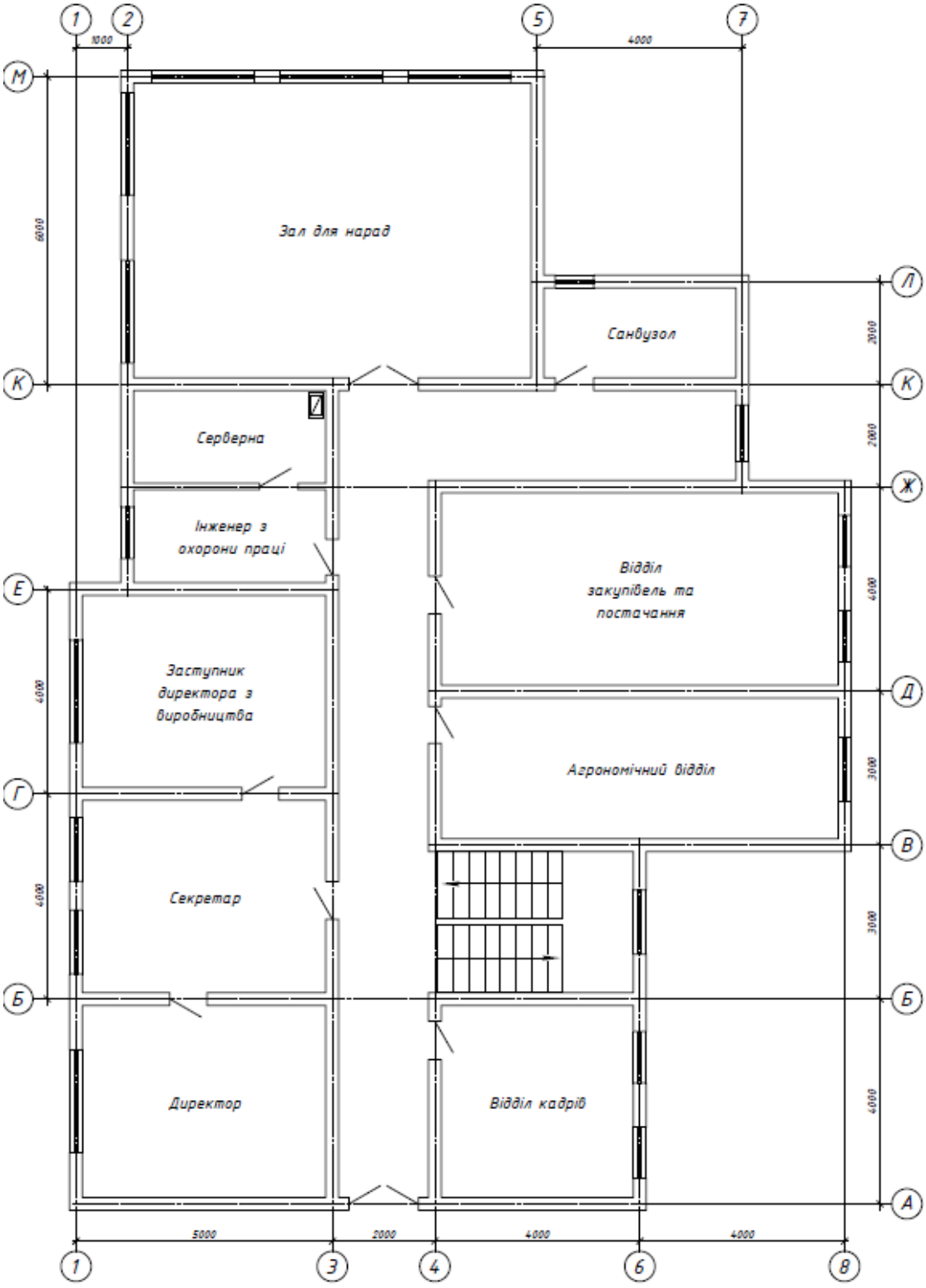

Рисунок А.1 – План першого поверху

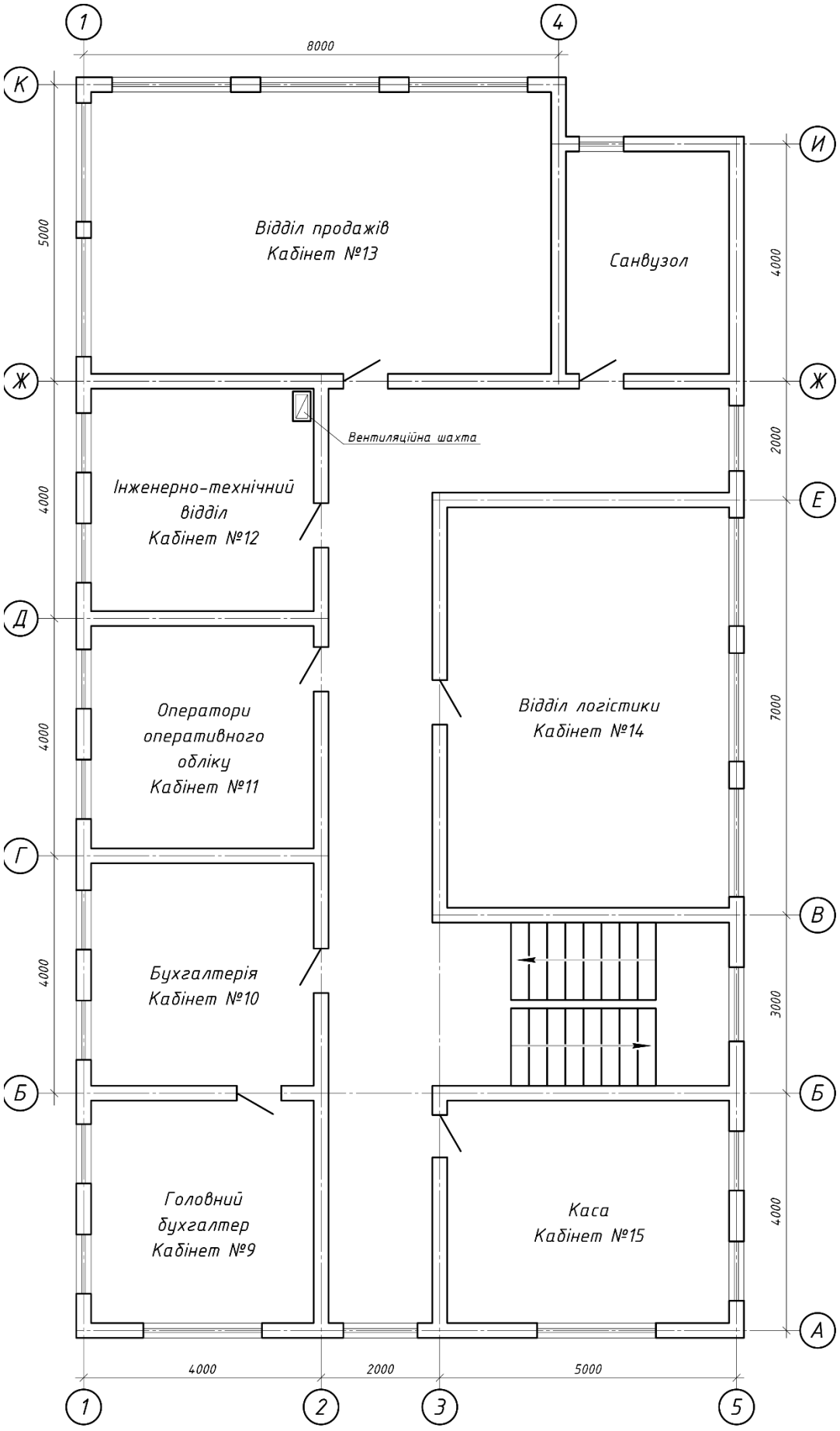

Рисунок А.2 – План другого поверху

Додаток Б. План прокладання кабелів СКС мережі філії агрохолдингу "Контінентал Фармерз Груп"

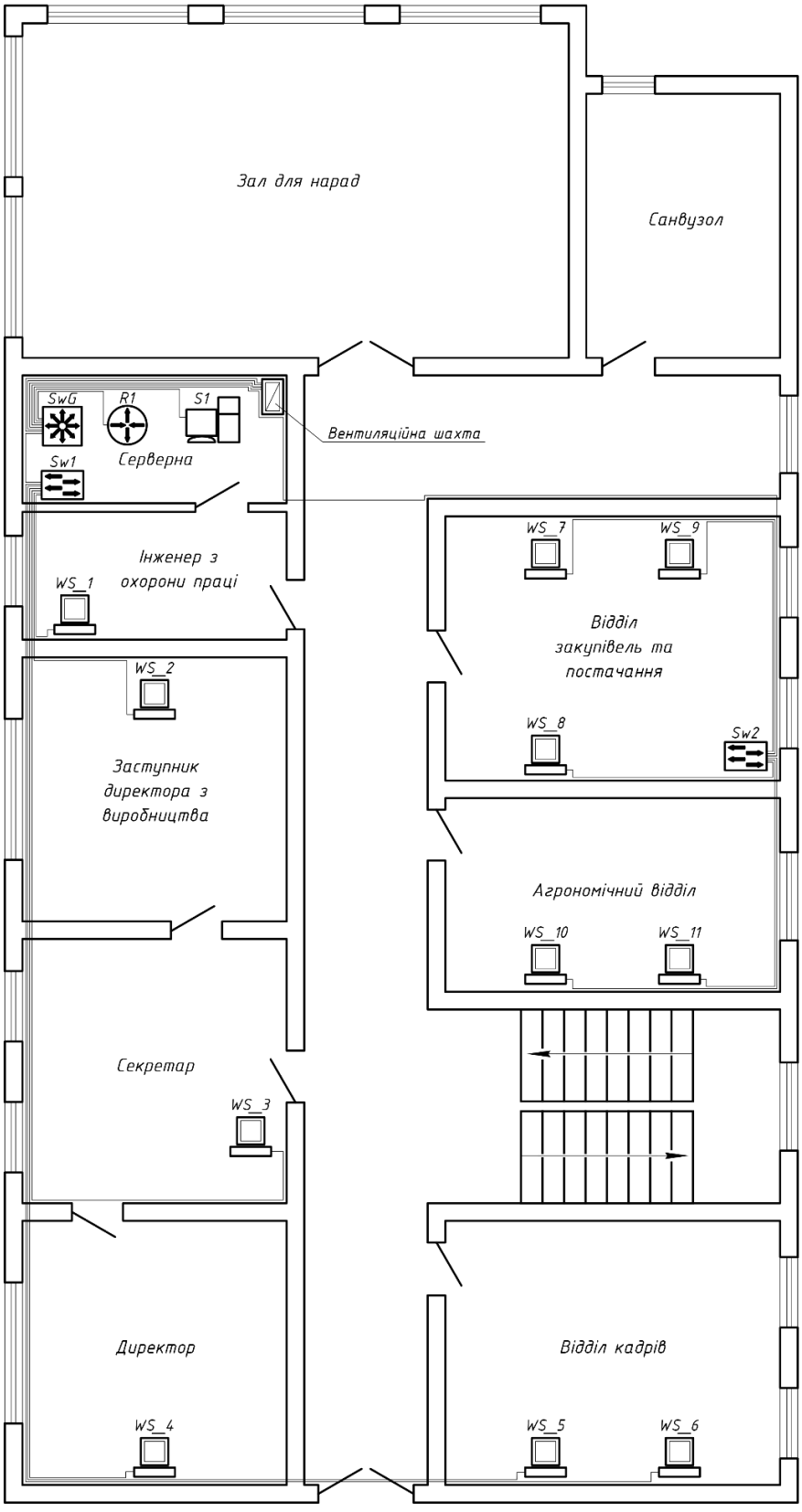

Рисунок Б.1 – План першого поверху

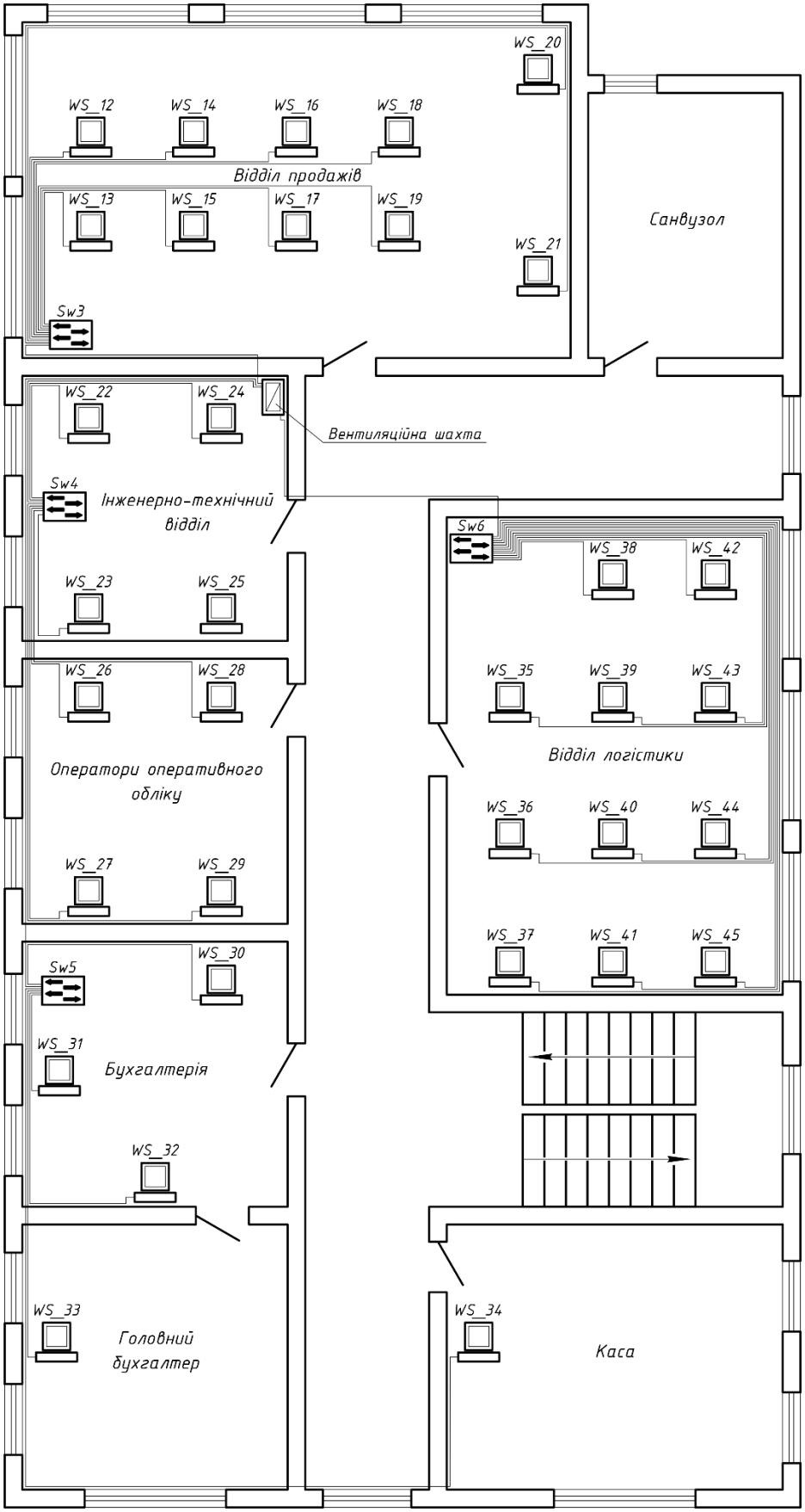

Рисунок Б.2 – План другого поверху