Форма № Н-9.02

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі компанії ТОВ «Агрополіс»**

Виконав: студент VI курсу, групи КІ-602

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ Богдан КОЛИНЯК

(ім'я та прізвище)

Керівник Надія ТХІР

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

Тернопіль – 2025

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

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

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"31" березня 2025 року

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

Колиняку Богдану Михайловичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі компанії ТОВ «Агрополіс»**

керівник роботи Тхір Надія Павлівна
(прізвище, ім'я, по батькові)

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

2. Строк подання студентом роботи: 13 червня 2025 року.

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

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

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

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

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

7. Дата видачі завдання: 01 квітня 2025 року

Студент _____ Богдан КОЛИНЯК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Надія ТХІР
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Колиняк Б.М. Розробка проєкту комп'ютерної мережі компанії ТОВ «Агрополіс»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр за спеціальністю «123 – Комп'ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2025. 110 с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі аграрної фірми «Агрополіс» 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 Cisco Packet Tracert.

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

ANNOTATION

Kolinyak B.M. Development of a computer network project for the company LLC "Agroservice": qualification work for obtaining a bachelor's degree in the specialty "123 – Computer Engineering". Ternopil: VSP "TFK TNTU", 2025. 110p.

The qualification work involves the development of a computer network project for the agricultural company "Agroservice" according to 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 subnets and network protection tools are developed. A virtual network model is created in the Cisco Packet Tracert program.

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

Розвиток сучасного бізнесу нерозривно пов'язаний з ефективним використанням інформаційних технологій. У динамічних умовах ринкової економіки, де конкуренція постійно зростає, швидкість та точність обробки інформації стають ключовими факторами успіху для будь-якого підприємства, незалежно від його галузі. Особливо це стосується агропромислового комплексу, де впровадження сучасних технологій може суттєво підвищити ефективність виробничих процесів, оптимізувати управління та логістику, а також забезпечити швидкий доступ до необхідних даних.

Актуальність теми: В умовах цифровізації економіки, створення надійної, масштабованої та безпечної комп'ютерної мережі є фундаментом для функціонування будь-якої організації. Для агрофірм, таких як ТОВ «Агрополіс», це означає можливість оптимізувати облік, управління ресурсами, контроль за виробничими циклами, а також забезпечити ефективну комунікацію між підрозділами та зовнішніми партнерами. Відсутність адекватно спроєктованої та реалізованої мережі призводить до низької продуктивності, втрати даних, високих операційних витрат та вразливості до кіберзагроз. Тому розробка проєкту комп’ютерної мережі, яка відповідає сучасним вимогам безпеки, продуктивності та масштабованості, є надзвичайно актуальним завданням.

Метою кваліфікаційної роботи є розробка проєкту комп’ютерної мережі для ТОВ «Агрополіс», яка забезпечить ефективний обмін інформацією, надійний доступ до ресурсів та високий рівень інформаційної безпеки.

Практична цінність роботи полягає в розробці готового проєкту комп’ютерної мережі, який може бути безпосередньо використаний ТОВ «Агрополіс» для модернізації своєї IT-інфраструктури. Результати роботи дозволять підвищити ефективність бізнес-процесів, забезпечити надійність та безпеку обміну даними, а також створити основу для подальшого впровадження інноваційних рішень в агропромисловому секторі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Завданням кваліфікаційної роботи є розробка проекту комп’ютерної мережі агропромислового підприємства ТОВ «Агрополіс» .

Основний вид діяльності ТОВ «Агрополіс» (ЄДРПОУ 30834410) у Чортківському районі Тернопільської області є вирощування зернових культур (крім рису), бобових культур і насіння олійних культур. Компанія спеціалізується на вирощуванні таких основних культур як пшениця (озима), кукурудза, соняшник, цукровий буряк. Окрім основної аграрної діяльності, компанія також займається оптовою торгівлею сільськогосподарською продукцією, наданням в оренду спецтехніки, а також має власні складські потужності. З огляду на обсяги діяльності та її диверсифікованість, ефективна та надійна комп'ютерна мережа є критично важливою для підтримки виробничих, логістичних та адміністративних процесів, забезпечуючи централізоване управління даними, координацію роботи підрозділів та оперативний обмін інформацією.

На тлі зростаючих вимог до ефективності бізнесу та необхідності оптимізації внутрішніх процесів, ТОВ «Агрополіс» має нагальну потребу у впровадженні сучасної комп'ютерної мережі. Ця потреба зумовлена низкою факторів:

- необхідність об'єднання інформації з різних підрозділів (бухгалтерія, агрономічна служба, склад, ремонтна база) у єдине сховище для оперативного доступу та аналізу;

- потреба у прискоренні обробки документів, автоматизації обліку та покращенні взаємодії між співробітниками та відділами;

- забезпечення керівництва актуальною інформацією для прийняття своєчасних та обґрунтованих рішень;

- можливість легкого розширення мережі з урахуванням зростання компанії, впровадження нових технологій (наприклад, IoT в агросекторі, GPS-моніторинг техніки) та підключення додаткових робочих місць;

- захист конфіденційних даних компанії (фінансових, комерційних, персональних) від несанкціонованого доступу, втрат та кіберзагроз.

- потреба у раціональному використанні ресурсів, мінімізації витрат на папір, телефонний зв'язок та ручну обробку даних.

- забезпечення швидкого та надійного обміну інформацією між співробітниками та відділами, у тому числі віддаленими..

1.1.2 Призначення розробки

Розробка проєкту комп'ютерної мережі для ТОВ «Агрополіс» має на меті створення сучасної, ефективної, надійної та безпечної інформаційної інфраструктури, яка відповідатиме поточним та майбутнім потребам підприємства. Основне призначення цієї розробки полягає у:

- створення всебічного та детального опису архітектури, топології, конфігурації та принципів функціонування комп'ютерної мережі ТОВ «Агрополіс». Це забезпечить чітке розуміння структури мережі, спростить її адміністрування, обслуговування та подальший розвиток;

- визначення та вибір найбільш підходящих апаратних і програмних засобів (мережеве обладнання, операційні системи, сервіси) для побудови мережі, враховуючи специфіку діяльності агрофірми, її масштаби, бюджетні обмеження та вимоги до продуктивності й безпеки;

- проєктування мережі, здатної ефективно підтримувати всі бізнес-процеси ТОВ «Агрополіс», включаючи роботу з офісними застосунками, бухгалтерським програмним забезпеченням, системами управління підприємством, а також забезпечувати високу швидкість обміну даними між користувачами та серверами;

- впровадження комплексних заходів захисту, спрямованих на забезпечення конфіденційності, цілісності та доступності корпоративної інформації. Це включає розробку політик безпеки, налаштування мережевих екранів, систем виявлення вторгнень та механізмів авторизації/аутентифікації.

- проєктування мережі з урахуванням можливості її легкого розширення та модернізації у майбутньому без кардинальних змін архітектури, що дозволить інтегрувати нові технології та підключати додаткові робочі місця у відповідності до росту компанії;

- розроблений проєкт слугуватиме детальним керівництвом для технічних спеціалістів ТОВ «Агрополіс» або підрядної організації щодо реалізації та налаштування мережевої інфраструктури.

Таким чином, дана розробка спрямована на створення міцного IT-фундаменту для ТОВ «Агрополіс», що дозволить компанії підвищити свою операційну ефективність, конкурентоспроможність та забезпечити стійкий розвиток у довгостроковій перспективі.

Впровадження сучасної та добре спроєктованої комп'ютерної мережі забезпечить ТОВ «Агрополіс» низку значних переваг, які позитивно вплинуть на всі аспекти діяльності компанії:

- автоматизація рутинних операцій, швидкий доступ до інформації та спільна робота над документами дозволять співробітникам зосередитися на більш важливих завданнях, зменшуючи час на виконання операцій;

- можливість зберігати всі дані на центральному сервері, що забезпечує їхню цілісність, резервне копіювання та легкий доступ з будь-якого авторизованого робочого місця;

- створення єдиного інформаційного простору сприяє більш ефективній взаємодії між відділами та співробітниками, прискорюючи обмін інформацією та прийняття рішень;

- реалізація комплексних заходів захисту даних від несанкціонованого доступу, вірусів, шпигунських програм та зовнішніх загроз, забезпечуючи конфіденційність та цілісність корпоративної інформації;

- можливість легкого додавання нових робочих місць, інтеграції сучасних технологій (наприклад, систем GPS-моніторингу сільгосптехніки, датчиків полів) та розширення функціоналу мережі у майбутньому без значних додаткових інвестицій;

- ефективне використання ресурсів: Спільний доступ до периферійних пристроїв (принтерів, сканерів, плотерів), що зменшує потребу в придбанні окремого обладнання для кожного робочого місця;

- модернізація IT-інфраструктури дозволить ТОВ «Агрополіс» більш ефективно реагувати на зміни ринку, впроваджувати інновації та підвищувати свою конкурентоспроможність у агропромисловому секторі.

Розробка проєкту комп'ютерної мережі для ТОВ «Агрополіс» має на меті створення сучасної, ефективної, надійної та безпечної інформаційної інфраструктури, яка відповідатиме поточним та майбутнім потребам підприємства. Основне призначення цієї розробки полягає у:

- створення всебічного та детального опису архітектури, топології, конфігурації та принципів функціонування комп'ютерної мережі ТОВ «Агрополіс». Це забезпечить чітке розуміння структури мережі, спростить її адміністрування, обслуговування та подальший розвиток;

- визначення та вибір найбільш підходящих апаратних і програмних засобів (мережеве обладнання, операційні системи, сервіси) для побудови мережі, враховуючи специфіку діяльності агрофірми, її масштаби, бюджетні обмеження та вимоги до продуктивності й безпеки;

- проєктування мережі, здатної ефективно підтримувати всі бізнес-процеси ТОВ «Агрополіс», включаючи роботу з офісними застосунками, бухгалтерським програмним забезпеченням, системами управління підприємством, а також забезпечувати високу швидкість обміну даними між користувачами та серверами;

- впровадження комплексних заходів захисту, спрямованих на забезпечення конфіденційності, цілісності та доступності корпоративної

інформації. Це включає розробку політик безпеки, налаштування мережевих екранів, систем виявлення вторгнень та механізмів авторизації/аутентифікації.

- проєктування мережі з урахуванням можливості її легкого розширення та модернізації у майбутньому без кардинальних змін архітектури, що дозволить інтегрувати нові технології та підключати додаткові робочі місця у відповідності до росту компанії;

- розроблений проєкт слугуватиме детальним керівництвом для технічних спеціалістів ТОВ «Агрополіс» або підрядної організації щодо реалізації та налаштування мережевої інфраструктури.

Таким чином, дана розробка спрямована на створення міцного IT-фундаменту для ТОВ «Агрополіс», що дозволить компанії підвищити свою операційну ефективність, конкурентоспроможність та забезпечити стійкий розвиток у довгостроковій перспективі.

Впровадження сучасної та добре спроєктованої комп'ютерної мережі забезпечить ТОВ «Агрополіс» низку значних переваг, які позитивно вплинуть на всі аспекти діяльності компанії:

- автоматизація рутинних операцій, швидкий доступ до інформації та спільна робота над документами дозволять співробітникам зосередитися на більш важливих завданнях, зменшуючи час на виконання операцій;

- можливість зберігати всі дані на центральному сервері, що забезпечує їхню цілісність, резервне копіювання та легкий доступ з будь-якого авторизованого робочого місця;

- створення єдиного інформаційного простору сприяє більш ефективній взаємодії між відділами та співробітниками, прискорюючи обмін інформацією та прийняття рішень;

- реалізація комплексних заходів захисту даних від несанкціонованого доступу, вірусів, шпигунських програм та зовнішніх загроз, забезпечуючи конфіденційність та цілісність корпоративної інформації;

- можливість легкого додавання нових робочих місць, інтеграції сучасних технологій (наприклад, систем GPS-моніторингу сільгосптехніки, датчиків

полів) та розширення функціоналу мережі у майбутньому без значних додаткових інвестицій;

- ефективне використання ресурсів: Спільний доступ до периферійних пристроїв (принтерів, сканерів, плотерів), що зменшує потребу в придбанні окремого обладнання для кожного робочого місця;

- модернізація IT-інфраструктури дозволить ТОВ «Агрополіс» більш ефективно реагувати на зміни ринку, впроваджувати інновації та підвищувати свою конкурентоспроможність у агропромисловому секторі.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для реалізації проєкту локальної комп'ютерної мережі передбачається використання наступного ключового обладнання:

- головний комутатор – пристрій стандарту Gigabit Ethernet з функціоналом третього рівня моделі OSI, оснащений 16 портами;

- комутатори робочих груп – комутатори стандарту Gigabit Ethernet на 16 портів;

- маршрутизатор-шлюз – пристрій для забезпечення зв'язку між мережами та доступу до зовнішніх ресурсів;

- мережевий кабель – основа фізичного середовища передачі даних;

- мережеві розетки стандарту 8P8C – призначені для підключення кінцевих пристроїв;

- роз'єми (конектори) – для термінування сегментів кабелю стандарту 8P8C;

- патч-корди використовуватимуться для під'єднання кінцевих пристроїв до мережевих розеток структурованої кабельної систем;

- комутаційна шафа – для організації та захисту мережевого обладнанн;

- патчпанель – для зручного та впорядкованого підключення кабельних ліній.

Мережа функціонуватиме на основі стеку протоколів TCP/IP версії 4..

1.1.4 Вимоги до документації

Для забезпечення ефективного та своєчасного обслуговування локальної мережі ТОВ «Агрополіс» критично важливо мати повний комплект належним чином оформленої технічної документації. Ця документація є обов'язковим елементом для будь-якої комп'ютерної мережі і для проєкту ТОВ «Агрополіс» включає:

- план приміщення;
- логічна топологія;
- схема зв’язків між вузлами перенесена на план приміщення (фізична топологія);
- специфікації обладнання – детальний список всіх комутаторів (з їх моделями, кількістю портів, можливо, серійними номерами), маршрутизатора, сервера;
- система маркування, яка використовується для ідентифікації кожного кабелю та розетки;
- таблиця IP-адрес;
- опис застосованих заходів безпеки (правила брандмауера на маршрутизаторі, політики доступу на комутаторах.

1.1.5 Техніко-економічні показники

Проєктована локальна мережа ТОВ «Агрополіс» демонструє наступні ключові техніко-економічні характеристики [2]:

- основний провідний сегмент реалізовано за стандартом Gigabit Ethernet (IEEE 802.3ab).
- розрахована на обслуговування 45 робочих станцій;
- використовує кабель "вита пара" категорії 6 як середовище передачі даних;
- загальна вартість мережі не перевищує 500 тис. грн.

1.1.6 Стадії та етапи розробки

Проєктування локальної комп'ютерної мережі здійснюється згідно з наступною послідовністю кроків [3]:

- визначення основних етапів розробки мережевого проєкту;
- формування логічної схеми мережі;
- розробка фізичної топології та детального плану кабельної системи;
- вибір необхідного активного та пасивного обладнання для забезпечення функціонування мережі;
- здійснення фізичного прокладання кабельних ліній;
- встановлення точок підключення (мережевих розеток);
- монтаж та комутація мережевого обладнання в комутаційній шафі;
- налаштування центрального комутатора;
- конфігурування комутаторів робочих груп;
- налаштування маршрутизатора для забезпечення міжмережевого зв'язку;
- проведення тестування функціональності та стабільності мережі;
- складання повного комплекту технічної документації.".

1.1.7 Порядок контролю та прийому

Для ефективної оцінки якості мережі критично важливим є етап перевірки її функціональних параметрів. Це включає аналіз наступних технічних показників локальної мережі [5]:

- виявлення помилок у передачі/прийомі пакетів;
- аналіз системних журналів ОС для виявлення проблем;
- огляд звітів системи моніторингу для виявлення аномалій;
- вимірювання фактичної швидкості передачі пакетів між мережевими комутаторами та вузлами;
- перевірка цілісності фізичного середовища за допомогою кабельного тестера.

1.2 Опис задачі та характеристика підприємства ТОВ «Агрополіс»

ТОВ «Агрополіс», зареєстроване та здійснює свою діяльність у Чортківському районі Тернопільської області (ЄДРПОУ 30834410), є значним та динамічно розвиваючим агропромисловим підприємством. Основні види діяльності:

- вирощування зернових культур (крім рису), бобових культур і насіння олійних культур. Це включає повний цикл сільськогосподарського виробництва від підготовки ґрунту, посіву, догляду за посівами до збирання та первинної обробки врожаю. Ймовірно, компанія спеціалізується на вирощуванні таких культур як пшениця, кукурудза, соняшник, цукровий буряк.;
- оптова торгівля зерном, насінням, кормами;
- надання в оренду сільськогосподарської техніки та обладнання;
- післяурожайна діяльність (власні елеватори або зерносховища);
- транспортні послуги (перевезення власної продукції та надання послуг);
- виробництво цукру (якщо є власний цукровий завод або пайова участь)..

У своїй діяльності підприємство охоплює широкий спектр робіт по виготовленню та встановленню виробів із дерева і металу. Крім цього, ТОВ «Агрополіс» займається переробкою зернових культур (пшениці, жита, кукурудзи, гречки, рису, ячменю, вівса тощо) на борошно та крупи різних видів і сортів.

Діяльність підприємства поширюється на сільськогосподарські угіддя в Чортківському районі Тернопільської області, що включає декілька виробничих майданчиків, полів, складських приміщень та офісних будівель, які потенційно потребують об'єднання в єдину мереж. Розглянемо детально структуру підприємства із зазначенням кількості комп’ютерів і кожному підрозділі для об’єднання в мережу.

Отже, підприємство ТОВ «Агрополіс» структурно поділене на підрозділи вищого менеджменту (керівництво підприємства) та функціональний та комерційний відділи.

На підприємстві ТОВ «Агрополіс» працює 135 осіб із них робота 45 працівників пов’язана із використанням комп’ютерної техніки.

До керівництва підприємства ТОВ «Агрополіс» входять:

- директор – генеральне керівництво підприємством, стратегічний розвиток, взаємодія із зовнішніми партнерами. В кабінеті директора розташовано 1 персональний комп'ютер;
- секретар керівника – адміністративна підтримка. Розташовано 1 ПК;
- заступник директора з виробництва (нагляд за виробничими процесами, технічною базою). В кабінеті заступник директора з виробництва розташовано 1 вузол, що необхідно об'єднати в мережу;
- заступник директора з комерційних питань – нагляд за продажами, логістикою, закупівлями). Не має окремого ПК, працює через Відділ продажів/логістики;
- заступник директора з фінансових питань – нагляд за фінансовою діяльністю, обліком. Не має окремого ПК, працює через бухгалтерію;
- заступник директора з персоналу та безпеки – нагляд за кадрами, охороною праці, внутрішньою безпекою. Не має окремого ПК, працює через Відділ кадрів/ОП.

Виробничий підрозділ підпорядковується заступнику директора з виробництва і поділений на:

- виробничий відділ / диспетчерська – підпорядковується заступнику директора з виробництва. В його склад входять працівники: керівник виробничого відділу, диспетчери та оператори оперативного обліку. Всього у відділі встановлено 4 ПК;
- агрономічний відділ складається із працівників – головний агроном та агрономи. Всього у відділі встановлено 3 ПК;
- інженерно-технічний відділ складається із посад головного інженера, інженерів, технічних спеціалістів. Всього у відділі 4 ПК.

Комерційний відділ підпорядковується заступнику директора з комерційних питань і складається із підрозділів:

- відділ продажів, що складається із посад керівника відділу продажів та менеджерів з продажів. Всього у відділі 11 комп'ютерів;

- відділ логістики, куди входять керівник відділу логістики, логісти та фахівці з транспортування та складського обліку. Всього у відділі 10 ПК;

- відділ закупівель та постачання, куди входять керівник відділу закупівель, фахівці із закупівель, спеціалісти з постачання. Всього у відділі 3 ПК.

Фінансово-економічний підрозділ підпорядковується заступнику директора з фінансових питань. До складу цього підрозділу входить бухгалтерія, куди входять головний бухгалтер, бухгалтери за ділянками (розрахунки, зарплата, основні засоби, тощо) та касир. Всього у бухгалтерії розташовано 5 комп'ютерів.

Адміністративний підрозділ підпорядковується напряму директору і складається із відділе 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. Всього в адміністративному підрозділі розташовано 3 комп'ютери.

Всього на підприємстві встановлено 45 комп'ютерів які необхідно об'єднати в єдину мережу.

Для централізованого зберігання даних в проектованій мережі слід передбачити використання файлового сервера. Який повинен здійснювати:

- зберігання комерційної інформації. Бази даних клієнтів, прайс-листи, договори з постачальниками та покупцями, маркетингові матеріали, звіти;

- зберігання фінансової та бухгалтерської інформації. Бухгалтерські звіти, фінансові плани, платіжні відомості, податкова документація;

- спільний доступ до файлів. Співробітники різних відділів можуть легко отримувати доступ до необхідних документів та обмінюватися ними, що підвищує ефективність співпраці та усуває необхідність дублювання інформації.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Обґрунтування вибору логічного типу мережі

При проєктуванні комп'ютерних мереж критично важливо правильно обрати фізичне середовище передачі даних, топологію мережі та мережеву технологію. Кожен тип топології має свої переваги та недоліки, які впливають на надійність, масштабованість, швидкість та вартість мережі. Як вже було зазначено в розділах 1.1.3 та 1.1.4, мережа ТОВ «Агрополіс» використовуватиме кабельне фізичне середовище.

Серед основних топологій виділяють шинну, кільцеву, зіркоподібну, деревоподібну та завершену.

У шинній топології (Bus) всі пристрої підключаються до одного спільного кабелю, що слугує "шиною" для передачі даних. Це одна з найпростіших і найдешевших топологій для невеликих мереж. Однак її головний недолік полягає в низькій надійності: будь-який обрив або пошкодження центрального кабелю призводить до відмови всієї мережі. Локалізація несправностей також є складною, оскільки збій може бути викликаний будь-яким пристроєм, підключеним до шини. Для підприємства масштабу ТОВ «Агрополіс» з великою кількістю користувачів та критичними бізнес-процесами шинна топологія є абсолютно неприйнятною через її вразливість та складнощі масштабування.

У кільцевій топології (Ring) пристрої з'єднані послідовно, утворюючи замкнуте коло, по якому дані передаються в одному напрямку. Хоча ця топологія може забезпечувати досить високу швидкість передачі даних і в деяких реалізаціях (подвійне кільце) має певний рівень відмовостійкості, вона вкрай чутлива до пошкодження кабелю: один обрив може паралізувати всю мережу (у випадку простого кільця). Додавання або видалення пристроїв зазвичай вимагає тимчасового переривання роботи мережі, що є неприпустимим для активно функціонуючого підприємства.

Зіркоподібна (Star) топологія передбачає, що кожен пристрій підключається окремим кабелем до центрального вузла, яким зазвичай є комутатор або концентратор. Зіркоподібна топологія є дуже надійною, оскільки вихід з ладу одного пристрою або кабелю впливає лише на цей конкретний пристрій, а не на всю мережу. Локалізація несправностей значно спрощується, оскільки можна легко ідентифікувати проблемний сегмент. Це також робить її легкою для розширення. Однак, її критичним недоліком є повна залежність від центрального вузла: відмова комутатора призведе до зупинки роботи всього сегмента мережі. Ця топологія формує базові "зірки", які є складовими для більш складних структур.

У завершеній топології кожен пристрій підключається до кожного іншого пристрою в мережі, створюючи надлишкове з'єднання. Це забезпечує максимальну надійність та відмовостійкість, оскільки існує безліч альтернативних шляхів для передачі даних. Однак комірчаста топологія є надзвичайно дорогою в реалізації через величезну кількість необхідних кабелів та мережевих портів. Її використання практично обмежене для невеликих висококритичних сегментів мережі або для глобальних мереж, але є абсолютно непрактичною для локальних корпоративних мереж такого масштабу, як у «Агрополіс», через надмірну складність та вартість.

При проєктуванні сучасних комп'ютерних мереж, особливо для середніх та великих підприємств, рідко використовуються прості топології (шина, кільце) через їхні обмеження. Натомість, перевага надається більш складним, але гнучким та масштабованим структурам, таким як розширена зірка та деревоподібна топологія. Ці дві концепції тісно пов'язані і часто можуть бути інтерпретовані як варіанти одна одної, представляючи собою ієрархічні структури на базі зіркоподібних сегментів.

Розширена зірка є розвитком базової зіркоподібної топології. Якщо в простій зірці всі пристрої підключаються безпосередньо до одного центрального комутатора (або концентратора), то в розширеній зірці цей центральний комутатор (ядро) з'єднується з іншими, другорядними комутаторами, до яких

вже підключаються кінцеві пристрої (робочі станції, сервери тощо). Таким чином, формується дво- або багаторівнева структура, де кожен комутатор нижчого рівня сам по собі є центром для "зірки" з підключеними до нього пристроями.

Структура розширеної зірки [3]:

- центральний (головний) комутатор (Core Switch) – виступає як центральний вузол мережі, до якого підключаються всі інші комутатори. Це точка агрегації трафіку;
- розподільчі комутатори та комутатори рівня доступу (Distribution/Access Switches) – це комутатори, які підключаються до центрального комутатора. До них, у свою чергу, підключаються кінцеві пристрої. Ці комутатори можуть бути розташовані у різних відділах, на різних поверхах або у різних будівлях, об'єднуючи локальні групи пристроїв.

Основні переваги розширеної зірки [3]:

- масштабованість – дуже легко розширювати мережу, додаючи нові розподільчі комутатори або нові кінцеві пристрої до вже існуючих комутаторів;
- висока надійність – відмова одного кінцевого пристрою або кабелю до нього не впливає на роботу інших. Відмова розподільчого комутатора вплине лише на сегмент, який він обслуговує, а не на всю мережу. Це забезпечує локалізацію збоїв;
- ефективне усунення несправностей – завдяки централізованій структурі легко ідентифікувати місце виникнення проблеми. Якщо пристрій втрачає зв'язок, можна перевірити його кабель, потім порт на комутаторі, а потім з'єднання цього комутатора з ядром;
- простота управління – централізоване управління трафіком та налаштуваннями мережі, особливо якщо використовуються керовані комутатори, що дозволяють налаштовувати VLAN (Virtual Local Area Networks).

Недоліки розширеної зірки [3]:

- залежність від центрального комутатора. Якщо центральний комутатор виходить з ладу, вся мережа або її значна частина перестає функціонувати. Для

критичних мереж це може бути вирішено за допомогою резервування (кластеризація або використання декількох центральних комутаторів);

- витрата кабелю. Потребує більше кабелю, ніж, наприклад, шинна топологія, оскільки кожен пристрій має окремий кабель до комутатора, а комутатори – до центрального комутатора.

Деревоподібна топологія є ще більш ієрархічною формою розширеної зірки, яка часто використовується для опису структури великих та складних мереж. Вона характеризується тим, що кожен вузол (комутатор) може мати лише одного "батька" (висхідний комутатор), але може мати кілька "дітей" (низхідних комутаторів або кінцевих пристроїв). Таким чином, формується структура, що нагадує дерево з коренем (центральний комутатор), гілками (комутатори середнього рівня) та листям (кінцеві пристрої).

Розширена зірка є по суті дво- або трирівневою деревоподібною топологією. Термін "деревоподібна" часто підкреслює саме ієрархічну природу мережі з чітким поділом на рівні ядра, розподілу та доступу, що є стандартом у великих корпоративних мережах (наприклад, модель Cisco Hierarchical Network Design).

Переваги деревоподібної топології (додатково до переваг розширеної зірки) [2]:

- оптимізація трафіку та продуктивність. Чітке розділення на рівні дозволяє оптимізувати потік даних. Трафік між кінцевими пристроями одного сегмента обробляється на рівні доступу, а між сегментами – на рівні розподілу, зменшуючи навантаження на ядро;

- покращена безпека. Можливість впровадження складніших політик безпеки на кожному рівні ієрархії (наприклад, на рівні розподілу можуть бути налаштовані міжсегментні брандмауери або списки контролю доступу);

- легкість розширення та модернізації. Оскільки мережа модульна, можна легко оновлювати або замінювати обладнання на одному рівні, не впливаючи на інші.

Недоліки деревоподібної топології [3]:

- складність реалізації. Вимагає ретельного планування та проєктування через свою багатошаровість;

- залежність від центрального вузла. Якщо "корінь" дерева (комутатор ядра) виходить з ладу, це може призвести до повного колапсу мережі;

- вимагає більшої кількості мережевого обладнання (комутаторів) та кабелю порівняно з простими топологіями.

Мережа ТОВ «Агрополіс» є яскравим прикладом реалізації деревоподібної логічної топології, яка ефективно інтегрує принципи розширеної зірки.

- рівень ядра – це Switch SwG, розташований у кімнаті №4а (серверна), виконує функцію ядра мережі. До нього підключені всі інші комутатори, а також маршрутизатор R1 та сервер, що робить його центральною точкою агрегації та маршрутизації трафіку;

- рівень доступу/розподілу – комутатори Switch Sw1, Sw2 на першому поверсі та Switch Sw3, Sw4, Sw5 та Sw6 на другому поверсі відіграють роль як розподільчих комутаторів (для трафіку між відділами), так і комутаторів доступу (для підключення кінцевих пристроїв). До них підключаються ПК різних відділів (додаток А):

- Switch Sw1 – директор (Кімната №1), секретар (Кімната №2), заступник директора (Кімната №3), інженер з охорони праці (Кімната №4), відділ кадрів (Кімната №8);
- Switch Sw2 – відділ закупівель та постачання (Кімната №6), агрономічний відділ (Кімната №7);
- Switch Sw3 – відділ продажів (Кімната №13);
- Switch S4 – інженерно-технічний відділ (Кімната №12), оператори оперативного обліку (Кімната №11);
- Switch S5 – бухгалтерія (Кімната №10), головний бухгалтер (кімната №9), каса (Кімната №15);
- Switch S6 – відділ логістики (Кімната №14).

Крім цього, в кімнаті №5, де розташовано зал для нарад. Пропонується додати безпровідну точку доступу із гостьовим доступом для підключення мобільних пристроїв під час нарад.

Ця ієрархічна структура дозволяє «Агрополіс» повною мірою скористатися перевагами:

- висока масштабованість для майбутнього розширення;
- надійність за рахунок локалізації несправностей та чіткої сегментації;
- ефективне управління з використанням VLANs для ізоляції відділів та оптимізації трафіку;
- оптимальне використання кабельного середовища шляхом логічного групування пристроїв навколо комутаторів на кожному поверсі.

Таким чином, розширена зірка, що є базовою структурою для деревоподібної топології, є ідеальним вибором для «Агрополіс», забезпечуючи гнучку, надійну та високопродуктивну мережеву інфраструктуру.

Візуальне представлення спроектованої топології мережі можна знайти на рисунку 2.1.

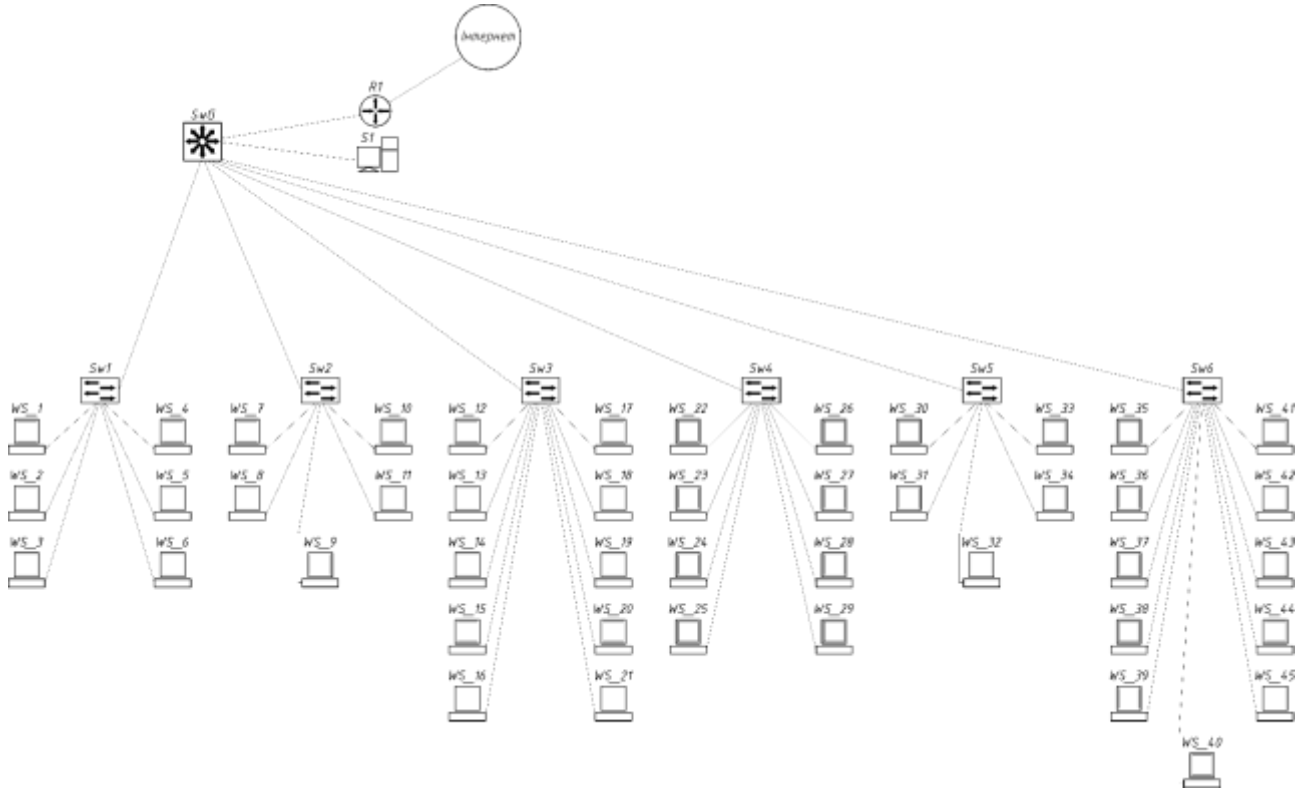


Рисунок 2.1 – Топологія мережі сервісного центру

Для комп'ютерної мережі ТОВ «Агрополіс» обрано мережеву технологію Gigabit Ethernet (1000BASE-T). Цей вибір є оптимальним і повністю обґрунтованим, виходячи з поточних потреб підприємства, вимог до продуктивності, масштабованості та економічної доцільності.

Стандарт 1000BASE-T розроблений спеціально для передачі даних зі швидкістю 1 Гбіт/с по мідній крученій парі (кабелі категорії 5e, 6 або вище) на відстань до 100 метрів [3]. Його висока популярність обумовлена економічністю та можливістю використання існуючої кабельної інфраструктури, що робить 1000BASE-T основним вибором для більшості локальних мереж.

Gigabit Ethernet забезпечує швидкість передачі даних до 1 Гбіт/с (1000 Мбіт/с). Ця пропускна здатність є достатньою для задоволення потреб сучасного офісного та виробничого середовища, такого як ТОВ «Агрополіс». Вона дозволяє:

- сервер, розташований у Кімнаті №4а (серверна), буде забезпечувати роботу баз даних, файлових сховищ та інших критично важливих сервісів. Gigabit Ethernet гарантує швидке завантаження та збереження великих файлів, оперативний доступ до даних для всіх 45 ПК в мережі;

- відділи, такі як агрономічний, інженерно-технічний, виробничий/диспетчерська, можуть працювати з графіками, картами полів, технічною документацією та іншими об'ємними даними. Швидкість 1 Гбіт/с забезпечує комфортну роботу з ними;

- сучасні підприємства часто використовують IP-телефонію та відеоконференції. Gigabit Ethernet забезпечує необхідну якість обслуговування (QoS) та пропускну здатність для безперебійної роботи цих сервісів.

Мережеве обладнання з підтримкою Gigabit Ethernet (комутатори, мережеві адаптери, маршрутизатори) є широко доступним на ринку від багатьох виробників. Це забезпечує конкурентні ціни, легкість у пошуку запасних частин та широку підтримку.

Вибір технології Gigabit Ethernet для мережі ТОВ «Агрополіс» є зваженим рішенням, яке забезпечує оптимальний баланс між продуктивністю, надійністю, економічною ефективністю та масштабованістю. Вона повною мірою відповідає вимогам деревоподібної топології та кабельного фізичного середовища, дозволяючи підприємству ефективно функціонувати та розвиватися.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

Для реалізації локальної комп'ютерної мережі ТОВ «Агрополіс» необхідний комплекс активного та пасивного комунікаційного обладнання. Серед пасивних елементів виділяються кабельні системи, комутаційні шафи, патч-панелі, патчкорди, роз'єми та мережеві розетки.

Якість і стабільність передачі даних у мережі безпосередньо залежать від належного функціонування кабельної системи – фундаментального елемента, що забезпечує зв'язок між мережевими пристроями. Різноманітність типів кабелів вимагає ретельного вибору та строгого дотримання технічних вимог під час монтажу для гарантії заявлених характеристик.

Вибір типу кабельної системи для ТОВ 'Агрополіс' зумовлений обраною технологією мережі та її топологією. Як уже зазначалося у розділі 2.1, проєктована мережа використовує специфікацію 1000Base-T, що логічно передбачає застосування кабелю типу «кручена пара».

У розробленій локальній комп'ютерній мережі ТОВ «Агрополіс» передбачається використання структурованої кабельної системи (СКС), яка базується на трьох основних типах кабельних з'єднань, що забезпечують її функціональність, масштабованість та надійність:

- патчкорди – короткі, гнучкі кабелі слугуватимуть для з'єднання кінцевих мережевих пристроїв (таких як персональні комп'ютери, IP-телефони, принтери) з мережевими розетками у робочих зонах. Додатково, патчкорди будуть

використовуватися в комутаційних шафах для гнучкого підключення портів патч-панелей до відповідних портів комутаторів. Це дозволяє легко змінювати підключення та реконфігурувати мережу за необхідності. Патчкорди є витратним матеріалом і можуть бути легко замінені, що спрощує обслуговування та усунення несправностей на кінцевих точка;

- горизонтальний кабель – цей тип кабелю є базовим компонентом СКС і відповідає за з'єднання мережевих розеток, розташованих у робочих зонах (офісних приміщеннях, відділах), безпосередньо з портами комутаторів рівня доступу (або агрегації), які знаходяться у комутаційних вузлах, як правило, в телекомунікаційних шафах на відповідних поверхах. Таким чином, кожен кінцевий пристрій отримує свій індивідуальний канал зв'язку до найближчого комутатора. У мережі ТОВ «Агрополіс» кабелі горизонтальної кабельної системи з’єднуватимуть мережеві розетки безпосередньо з комутаторами рівня доступу/агрегації (Switch Sw1, Sw2, на першому поверсі та Sw3, Sw4, Sw5, Sw6 на другому поверсі), які агрегують трафік для своїх зон. Також до горизонтальної абельної системи відноситься кабель, що з’єднує сервер із комутатором SwG та безпровідну точку доступу в залі засідань із комутатором SwG (додаток Б);

вертикальний кабель – утворює магістральну підсистему мережі, забезпечуючи високошвидкісні канали зв'язку між комутаторами, розташованими на різних рівнях ієрархії (наприклад, між поверхами або різними телекомунікаційними шафами), та центральним комутатором ядра мережі. Його головна функція полягає у створенні цих високошвидкісних «магістралей». У мережі ТОВ «Агрополіс» кабелі вертикальної кабельної системи з’єднуватимуть комутатори робочих груп (Switch S2, S3, S4, S5, S6) з головним комутатором мережі (Switch S1), що розташований у серверній кімнаті (Кімната №4). Це забезпечить ефективний та швидкий обмін даними між усіма сегментами мережі та її ядром.

Вибір конкретного типу кабелю для магістральних з'єднань у мережі ТОВ «Агрополіс» – чи то мідний, чи то оптоволоконний – буде визначатися декількома ключовими факторами: фактичною відстанню між комутаційними

вузлами, необхідною агрегованою пропускною здатністю (оскільки сукупний трафік від кінцевих пристроїв, що працюють на 1 Гбіт/с, може бути значно вищим), а також наявними бюджетними обмеженнями. Незважаючи на це, принципово важливим залишається забезпечення високошвидкісних каналів зв'язку, здатних ефективно агрегувати трафік від усіх підключених сегментів.

Саме тому сучасні мережі переважно будуються з використанням неекранованої крученої пари (UTP) та волоконно-оптичних кабелів. Їхня відповідність мережевим стандартам гарантується фізичними характеристиками, які закладаються ще на етапі виробництва та відображаються у маркуванні, забезпечуючи високу якість та надійність передачі даних.

Після ретельного аналізу технічних вимог, відповідності запитам замовника, а також зважаючи на вартість та перспективи подальшої модернізації, для локальної мережі було обрано кабель U/UTP Cat.6 4Pr виробництва «Одескабель». Його конструктивні особливості деталізовано далі [11]:

- струмопровідна жила – виконана з мідного м'якого провідника;
- діаметр жили – 0,57 мм (що відповідає стандарту 23 AWG).
- ізоляція – використовується поліетилен;
- діаметр провідника (з ізоляцією) – 1,05 мм.
- відповідність стандартам: Кабель відповідає вимогам ISO/IEC 11801:2002, EN 50173-1:2002, ANSI/TIA/EIA-568-B.2-1-2002, IEC 61156-5:2002.

Для підключення кабелю типу «кручена пара» до мережевих пристроїв використовуються конектори стандарту 8P8C, широко відомі як RJ45. Для потреб даної мережі було обрано конектори ATCOM RJ45 CAT.6 UTP 8P8C.

З метою оптимізації кабельної системи та спрощення підключення кінцевих пристроїв, у всіх точках підключення передбачається встановлення мережевих розеток стандарту 8P8C. Взаємозв'язок між цими розетками та персональними комп'ютерами здійснюватиметься за допомогою спеціалізованих патч-кордів.

Сучасний ринок мережевого обладнання пропонує широкий асортимент готових з'єднувальних кабелів різної довжини. Для потреб даної мережі,

оптимальним вибором є патч-корди довжиною 1,5 метра. Зокрема, для проєкту ТОВ «Агрополіс» обрано модель 2E CAT6 UTP RJ-45 26AWG, зовнішній вигляд якої представлено на рисунку 2.2

Рисунок 2.2 – Патч-корд 2E CAT6 UTP RJ-45 26AWG

Для забезпечення можливості підключення патч-кордів до стаціонарних кабельних ліній мережі обов'язковим є використання мережевих розеток. У проєктованій мережі було обрано зовнішню модель Cablexpert RJ45x1 UTP Cat.6 (див. рис. 2.3). Перевага цієї моделі полягає в її високій практичності та зручності монтажу. Це рішення є особливо доречним для офісних приміщень, де існує потреба у швидкому та простому підключенні кінцевих пристроїв, без необхідності інсталяції розеток безпосередньо в стіни/ [12].

Рисунок 2.3 – Мережева розетка Cablexpert RJ45x1 UTP cat.6

Однопортові мережеві розетки сприяють створенню організованого та естетично привабливого робочого простору. Їхня відповідність категорії Cat.6 забезпечує повну сумісність з обраною кабельною інфраструктурою та гарантує стабільну підтримку швидкості Gigabit Ethernet.

Підприємство «Агрополіс» функціонує у двоповерховій будівлі. Ця будівля об'єднує п’ятнадцять основних приміщень, а також додаткову кімнату

№4а, яка має ключове значення для мережевої інфраструктури. Детальний план цієї будівлі представлений на рисунках А.1 та А.2, додатку А.

Прокладка кабельної системи в двоповерховій будівлі ТОВ «Агрополіс» буде здійснюватися з урахуванням ієрархічної зіркової топології мережі та центрального розташування серверної кімнати (Кімната №4а) на першому поверсі.

Кабельні траси прокладаються таким чином, щоб мінімізувати довжину кабелю, але при цьому забезпечити доступність до робочих місць та мережевого обладнання. Всі кабелі повинні бути захищені від механічних пошкоджень, електромагнітних перешкод (від силових кабелів, великих електродвигунів), перегинів та надмірного натягу.

Кабелі прокладаються організовано, з використанням кабельних лотків, коробів або гофрованих труб у коридорах над півісною стелею, особливо у місцях переходу через стіни та у комутаційних шафах.

Кожен кабель та мережева розетка повинні бути чітко промарковані згідно з розробленою схемою маркування, що значно спрощує обслуговування та діагностику.

На першому поверсі у приміщеннях «Відділ продажів», керівництва, «Відділ кадрів», «Інженер з охорони праці» кабелі від мережевих розеток у цих приміщеннях прокладатимуться до комутатора Sw1 розташованого у серверній.

Кабелі від мережевих розеток комп’ютерів розташованих у «Відділі закупівель та постачання» та «Агрономічного відділу» прокладаються в коробах закріплених на станах до комутатора Sw2, розташованого в приміщені кімнати №6.

Кабелі горизонтальної системи прокладаються в пластикових кабель-каналах (коробах) із профілем 50х35 вздовж стін або під плінтусами для забезпечення естетичного вигляду та захисту. У деяких зонах, де це можливо та передбачено конструкцією будівлі, може використовуватися прихована прокладка (наприклад, за гіпсокартонними стінами, під фальшстелею або фальшпідлогою), що забезпечить максимальну невидимість кабельних трас.

Для протягування кабелю через стіну необхідно просвердлити отвір діаметром 16 мм і прокласти кабель в гофрованій трубці відповідного діаметру.

Кабель в коридорі між відділом кадрів та кабінетом директора і між «Відділ закупівель та постачання» і серверною прокладається у гофрованій трубці діаметром 16 мм над підвісною стелею.

На другому поверсі будівлі кабелі до мережевих розеток «Відділу логістики» та «Відділу продажів» прокладаються у спеціальних металічних підлгових коробах під фальшпідлогою. Це спеціальна конструкція, яка створює порожнину між основною підлогою та покриттям, дозволяючи легко прокладати та обслуговувати кабелі.

Прокладання під підлогою має свої специфічні вимоги та норми. В Україні ці вимоги регулюються низкою нормативних документів, зокрема ПУЕ (Правила улаштування електроустановок), ДБН В.2.5-56:2014 (Державні будівельні норми), а також відповідні стандарти (ДСТУ EN 50085-2-2:2015:) [4].

Для забезпечення точок підключення у мережі використовуються підлогові розетки. Процес їх монтажу передбачає наступні етапи [8]:

- за допомогою спеціалізованого інструменту (коронки або пили) у плиті фальшпідлоги вирізається отвір відповідного діаметру або розміру, призначений для монтажного лючка розетки. Важливо, щоб краї отвору були чистими та рівними;
- кінець кабелю виводиться через захисну трубу до місця встановлення лючка, залишаючи необхідний запас для подальшого монтажу;
- монтажний лючок підлогової розетки встановлюється у підготовлений отвір та надійно закріплюється (зазвичай за допомогою гвинтів або спеціальних затискачів);
- кабель зачищається, а його жили розкладаються та підключаються до відповідних контактів модуля RJ45 згідно з обраною схемою розкладки (T568A або T568B). Залишки жил обрізаються;
- модуль RJ45 встановлюється у рамку лючка.

Вимоги до кабелів включають високі показники пожежної безпеки (негорючість, низьке димоутворення та токсичність продуктів горіння), особливо в місцях скупчення людей. Такий кабель має маркування LSZH або аналогічне.

Для прокладки кабелів будуть використані металеві (перфоровані або неперфоровані) лотки, що забезпечують вентиляцію, механічний захист та зручність обслуговування. З огляду на ризик пошкодження гризунами, обрано саме металеві лотки для додаткового захисту.

Кабелепроводи необхідно надійно кріпити до конструкцій опор фальшпідлоги, щоб уникнути провисання та зміщення.

Також, під час монтажу слід суворо дотримуватися мінімальних радіусів вигину кабелів (для витої пари це 4-8 зовнішніх діаметрів), щоб запобігти пошкодженню жил та зберегти працездатність системи."

2.2.2 Будова вузлів та необхідність їх застосування

Вибір відповідного приміщення для розміщення серверної кімнати є одним з ключових рішень при проєктуванні локальної комп'ютерної мережі, оскільки саме тут концентрується критично важливе мережеве обладнання, включаючи маршрутизатор та центральний комутатор. Для мережі ТОВ «Агрополіс» в якості серверної кімнати було обрано кімнату №4а, що обґрунтовується такими факторами:

- кімната №4а займає стратегічно зручне місце у плані будівлі. Це дозволяє мінімізувати загальну довжину кабельних трас від центрального мережевого обладнання (Switch SwG, Switch Sw1, Router R1, Server S1), розташованого у цій кімнаті, до всіх інших мережевих комутаторів (Sw2, Sw3, Sw4, Sw5, Sw6) та, відповідно, до кінцевих користувачів. Коротші кабелі сприяють зменшенню втрат сигналу, підвищенню надійності зв'язку та зниженню витрат на прокладку. Таке розташування також спрощує реалізацію деревоподібної топології мережі;

- обрана кімната №4а дозволяє ефективно впровадити необхідні заходи фізичної безпеки. До них належать обмеження доступу (шляхом встановлення замків), що забезпечує захист дорогого обладнання та конфіденційних даних від несанкціонованого доступу та потенційного пошкодження. Відсутність вікно в цій кімнаті є теж додатковим фактором підвищення безпеки. Також до цієї кімнати немає прямого доступу із коридору. Потрапити в серверну можна лише через кабінет інженера з охорони праці;

- серверна розташована найближче до точки введення комунікацій Інтернет-провайдера.

Розміщення серверної кімнати в кімнаті №4а є ключовим стратегічним кроком, що забезпечує підвищену безпеку, ефективну роботу та економічну доцільність мережевої інфраструктури.

Для забезпечення належного функціонування мережі, критично важливим є правильне обладнання серверної кімнати. Серед ключових вимог до такого приміщення виділяють:

- доступ до серверної кімнати повинен бути суворо обмежений для переважної більшості відвідувачів та співробітників підприємства. Це гарантує фізичну безпеку дорогого мережевого обладнання та конфіденційних даних;

- розташування серверної кімнати має бути таким, щоб мінімізувати витрати на прокладання структурованої кабельної системи з усіх сегментів мережі. Це означає її географічно зручне розміщення відносно інших приміщень, що забезпечує ефективність кабельних трас.

В серверній кімнаті буде розміщено телекомунікаційну шафу, для впорядкування головного активного мережевого обладнання.

Шафа повинна мати достатню висоту (вимірюється в юнітах, U) та глибину, щоб вмістити все заплановане обладнання (патч-панелі, комутатори, блок безперебійного живлення, кабельні організатори) із запасом для майбутнього розширення. Відповіно до цих вимог пропонується обраної шафу WMNC-9U-FLAT (див. рис. 2.4) це 9U висоти та габарити 600x450x380 мм, що вже підтверджує її відповідність потребам поточного проєкту.

Рисунок 2.4 – Комутаційна шафа WMNC-9U-FLAT

У шафу WMNC-9U-FLAT буде поміщено патч-панелі, головний комутатор SwG, сенментуючий комутатор Sw1, маршрутизатор блок безперебійного живлення (APC 1500VA) та кабельні організатори.

Для ефективної організації та кросування кабельних з'єднань у комутаційній шафі буде використано патч-панель Panduit 19" на 24 порти, категорії 6 [15]. Ця патч-панель призначена для встановлення у серверні шафи та стійки. Вона комплектується конекторами RJ-45, які не потребують спеціальних інструментів для підключення завдяки системі автоматичного прорізання ізоляції провідників, що значно спрощує монтаж. Патч-панель постачається з необхідними кріпильними деталями та хомутами Colring і повністю відповідає стандарту EIA/TIA 568 B.2-1.

Для підтримання порядку та систематизації кабелів у шафі передбачено встановлення спеціального кабельного організатора. Крім того, блок безперебійного живлення (ДБЖ) APC Back-UPS Pro 1500VA забезпечить безперервну подачу електроенергії на всі мережеві вузли, надійно захищаючи їх від можливих перебоїв у зовнішній електромереж

Робочі місця у всіх приміщеннях розташовані вздовж стін, що значно спрощує прокладання структурованої кабельної системи. Це дозволить підключати робочі станції до мережевих розеток, встановлених у настінних коробах.

Загалом, у провідній мережі буде 45 комп'ютерів, що функціонуватимуть як робочі станції. Найбільша їх концентрація спостерігається у приміщенні

номер «Відділу логістики», як показано на додатку Б. Десять ПК також розташовано у приміщенні відділу продажів.

По чотири ПК розміщено у кімнатах «Інженерно-технічного відділу», «Операторів оперативного обліку» (ще одне приміщення ремонтного відділу), а також у відділах логістики та постачання (див. додаток Б).

По три комп'ютери знаходяться в бухгалтерії кімнаті «Відділу закупівель та посатчання» (див. додаток Б).

2.3 Обґрунтування вибору комунікаційного обладнання

Проєктування локальної комп'ютерної мережі ТОВ «Агрополіс» вимагає ретельного підбору активного мережевого обладнання, яке є базою всієї інфраструктури. Правильний вибір забезпечує високу продуктивність, надійність, безпеку та масштабованість системи. Для мережі «Агрополіс» було обрано компоненти від провідного виробника Cisco, що гарантує корпоративний рівень якості та підтримки.

Згідно із топологією представленою на рсиунку 2.1 в мережі ТОВ «Агрополіс» буде використовуватись наступне активне мережеве обладнання: один головний комутатор, шість комутаторів робочих груп, маршрутизатор та безпровідна точка доступу.

Головний комутатор виконує роль центрального елемента мережевої інфраструктури, забезпечуючи інтеграцію всіх пристроїв шляхом об'єднання сегментованих підмереж через відповідні комутатори. Безпосередньо до цього головного комутатора буде також підключено маршрутизатор, який надає доступ до глобальної мережі Інтернет. Обидва ці ключові мережеві пристрої розміщуються в серверній кімнаті.

Оснвоними критеріями вибору головного комутатора буде висока комутаційна пропускна здатність, підтримка L3-маршрутизації, достатня кількість Gigabit Ethernet портів для підключення серверів та аплінк-портів

Gigabit Ethernet для магістральних з'єднань. Підтримка інтелектуальних мережевих послуг (QoS, ACL, управління мультикастом).

Вибір головного комутатора вимагає особливо ретельного підходу, оскільки він є центральним вузлом в архітектурі розширеної зірки. До цього ключового пристрою передбачається підключення таких компонентів:

- шість комутаторів робочих груп;
- один сервер;
- одна безпровідна точка доступу;
- маршрутизатор, який є шлюзом доступу до мережі Інтернет.

Отже, для забезпечення всіх перерахованих підключень, головний комутатор повинен мати мінімум 9 інтерфейсів."

При виборі головного комутатора, який є центральним вузлом мережевої інфраструктури, необхідно враховувати низку критично важливих параметрів.

Оскільки аплінк-інтерфейси комутаторів робочих груп функціонують на швидкості 1 Гбіт/с, порти LAN головного комутатора, до яких підключаються ці комутатори, а також сервер, також повинні підтримувати швидкість 1 Гбіт/с.

Для коректного визначення мінімальної внутрішньої комутаційної спроможності (backplane bandwidth) головного комутатора, слід врахувати загальну кількість усіх кінцевих вузлів мережі. Згідно із завданням, їх нараховується 46 одиниць (45 користувачів та 1 сервер, який також генерує трафік). Розрахунок мінімальної необхідної пропускної здатності, що забезпечує повнодуплексну передачу даних для кожного користувача, виконується за формулою:

(45 користувачів+1 сервер)×1 Гбіт/с (на користувача)×2 (дуплекс)=92 Гбіт/с

Таким чином, мінімальна внутрішня комутаційна спроможність головного комутатора повинна становити не менше 92 Гбіт/с.

Окрім вимог до кількості та пропускної здатності портів, головний комутатор має підтримувати розширені функції керування мережею. Належність до третього рівня моделі OSI (L3) є критично важливою для ефективного поділу мережі на логічні сегменти (VLAN). Лише L3-комутатори здатні здійснювати

маршрутизацію між VLAN-ами (inter-VLAN routing), що неможливо для комутаторів лише рівня L2. Це забезпечує гнучке управління мережевими потоками, ефективну ізоляцію сегментів та оптимальне використання ресурсів, перетворюючи головний комутатор на повноцінний центральний вузол корпоративної мережі.

Для забезпечення надійної, високопродуктивної та керованої роботи всієї корпоративної мережі, до вибору головного комутатора було підійдено з особливою увагою, Достатня кількість портів [3]:

- мінімум 9 інтерфейсів для підключення шести комутаторів робочих груп, сервера, безпровідної точки доступу та маршрутизатора;
- підтримка 1 Гбіт/с на всіх LAN-портах для взаємодії з комутаторами робочих груп та сервером;
- внутрішня комутаційна спроможність не менше 92 Гбіт/с для ефективної обробки трафіку від усіх 46 вузлів мережі;
- належність до рівня керування L3;
- можливість розширення в майбутньому: Забезпечення масштабованості мережі.

Після всебічного аналізу вимог, було визначено, що Cisco Catalyst WS-C3560CX-12XPD-S є ідеальним вибором головного комутатора. Це сучасне рішення корпоративного класу не лише відповідає потребам у пропускній здатності, але й надає розширений функціонал маршрутизації, керування та безпеки, необхідний для ефективного функціонування центрального вузла корпоративної мережі [14]. Зовнішній вигляд обраного головного комутатора Cisco Catalyst WS-C3560CX-12XPD-S представлено на рисунку 2.5.

Рисунок 2.5 – Комутатор Cisco Catalyst WS-C3560CX-12XPD-S

Обрана модель L3-комутатора, Cisco Catalyst 3560CX-12XPD-S, ідеально підходить для ролі головного комутатора завдяки своїй здатності до централізованої обробки даних та розширених можливостей маршрутизації.

Цей комутатор оснащений 12 портами Gigabit Ethernet (RJ-45) для підключення серверів та ключових пристроїв, а також чотирма оптичними 10 Gigabit Ethernet (SFP+) аплінк-портами. Останні є критично важливими для забезпечення високошвидкісного зв'язку з маршрутизатором, гарантуючи достатню агреговану пропускну здатність для всього зовнішнього трафіку.

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

Cisco Catalyst 3560CX-12XPD-S також вирізняється низкою інтелектуальних функцій, таких як [14]:

- QoS (Quality of Service): для пріоритезації чутливого до затримок трафіку (наприклад, голосових та відеоданих);
- обмеження швидкості: для гнучкого контролю пропускної здатності для різних сегментів;
- ACL (Access Control Lists): для посилення безпеки та управління доступом до мережевих ресурсів;
- управління мультикастом: для оптимізації багатоадресної передачі даних;
- функція Cisco Auto SmartPorts, забезпечує автоматичну конфігурацію порту з урахуванням типу підключеного до нього пристрою, спрощуючи розгортання та адміністрування;
- підтримують також агрегування лінків, що дає збільшення пропускної спроможності та підсумовування бюджету PoE з двох і більше портів;
- високошвидкісна IP-маршрутизація (Cisco Express Forwarding - CEF): для ефективної взаємодії між віртуальними локальними мережами (VLAN-ами).

Детальні технічні параметри цього комутатора представлені у таблиці 2.1 [14], надаючи вичерпну інформацію про його функціональні можливості."

Таблиця 2.1 – Технічні характеристик Cisco WS-C3560CX-12XPD-S [14]

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.

Як вузли доступу до мережі, комутатори робочих груп відіграють центральну роль у своїх сегментах, збираючи трафік від кінцевих вузлів (робочих станцій, принтерів) та направляючи його до спільних ресурсів та головного комутатора.

Для цієї мережі передбачено шість таких комутаторів. Вибір цих пристроїв ґрунтується на двох основних вимогах: достатня кількість портів та відповідна пропускна здатність. З огляду на необхідність гарантованої пропускної здатності

1 Гбіт/с для кожного користувача, всі порти комутаторів робочих груп повинні підтримувати стандарт Gigabit Ethernet.

Для визначення необхідної кількості портів та технічних характеристик комутаторів робочих груп (рівня доступу), ми орієнтуємося на найбільший сегмент мережі. Згідно зі схемою логічної топології (представленої, наприклад, у Додатку Б), максимальне навантаження припадає на комутатор у кімнаті міжнародної логістики, до якого підключається 11 кінцевих вузлів (хостів). Отже, цей комутатор повинен мати мінімум 12 портів: 11 для підключення кінцевих вузлів та 1 для висхідного (uplink) підключення до головного комутатора.

Щоб кожен користувач дійсно мав доступ до мережі зі швидкістю 1 Гбіт/с, усі порти комутаторів робочих груп повинні відповідати стандарту Gigabit Ethernet. Цей стандарт забезпечує номінальну швидкість передачі даних 1 Гбіт/с на кожен порт, що є ключовим для сучасних вимог до пропускної здатності.

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

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

Кількість вузлів × Пропускна здатність на вузол × 2 (для дуплексу)

Отже, для найбільш завантаженого сегменту мережі (11 вузлів) буде:

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

Таким чином, комутатор робочої групи повинен мати внутрішню комутаційну матрицю з пропускною здатністю не менше 22 Гбіт/с.

Цей керований комутатор другого рівня (L2) ідеально відповідає поставленим завданням, забезпечуючи:

- завдяки підтримці Gigabit Ethernet на всіх портах, гарантується швидке з'єднання для користувачів;
- через виділені аплінк-порти, що формують стабільні магістральні з'єднання;
- для ефективної обробки всього трафіку без затримок.

Комутатор оснащений 16 LAN-інтерфейсами Gigabit Ethernet (RJ-45, 10/100/1000 Мбіт/с), що забезпечує високошвидкісне підключення для всіх кінцевих вузлів сегмента [15]. Додатково, він має два виділені аплінк-порти Gigabit Ethernet (RJ-45, 1000 Мбіт/с), призначені для надійного та високошвидкісного зв'язку з головним комутатором мережі або іншими мережевими пристроями, формуючи ключові магістральні з'єднання.

З комутаційною пропускною здатністю 32 Гбіт/с, пристрій значно перевершує мінімальні потреби мережі (22 Гбіт/с). Це забезпечує високу продуктивність та запобігає перевантаженням. Повний перелік характеристик представлено в таблиці 2.2.

Таблиця 2.2 – Технінчі характеристики Cisco Catalyst C1000-16T-2G-L [13]

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

Зовнішній вигляд комутатора Cisco Catalyst C1000-16T-2G-L представлено на рисунку 2.6.

Рисунок 2.6 – Комутатор Cisco Catalyst C1000-16T-2G-L

Вибір маршрутизатора, який є шлюзом для доступу локальної мережі до Інтернету, є наступним кроком у виборі активного мережевого обладнання. Враховуючи, що з'єднання з Інтернет-провайдером буде реалізовано за допомогою оптоволокна, маршрутизатор обов'язково повинен мати оптичний SFP-слот. Це забезпечить пряме, високошвидкісне та надійне підключення до волоконно-оптичного каналу провайдера.

Зважаючи на цю ключову вимогу, а також необхідність забезпечення стабільного та захищеного доступу до Інтернету, було прийнято рішення обрати маршрутизатор Cisco ISR4221/K9, зовнішній вигляд якого представлено на рисунку 2.7.

Рисунок 2.7 – Маршрутизатор Cisco ISR4221/K9

Детальний огляд технічних характеристик доступний у 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.

Маршрутизатор Cisco ISR4221/K9 є високоефективним рішенням, здатним підтримувати інтенсивний інтернет-трафік та забезпечувати стабільний доступ. Його потужність дозволяє не тільки здійснювати маршрутизацію, а й обробляти VPN-шифрування, що розширює можливості безпечного зв'язку.

Ключова функція моделі ISR4221/K9 – ефективне спрямування пакетів даних. Вона забезпечує безперебійний трафік між локальною мережею ТОВ «Агрополіс» (включаючи VLANs) та Інтернетом, підтримуючи як прості статичні налаштування, так і складні динамічні протоколи маршрутизації (такі як OSPF, EIGRP, BGP) для автоматичної оптимізації шляхів передачі.

Додатково, маршрутизатор виконує роль міжмережевого екрана, контролюючи мережевий потік за допомогою ACL, тим самим захищаючи локальну мережу від несанкціонованого доступу та зовнішніх загроз

Згідно з проєктом, бездротовий сегмент мережі передбачає розгортання точки доступу TP-LINK EAP225 (див. рис. 2.8). Її стратегічне розташування в коридорі, прилеглому до офісу прийому відвідувачів, забезпечить ефективне покриття. Вибір даної моделі зумовлений її оптимальним співвідношенням ціни та функціональності для невеликого офісу, а також зручністю встановлення на вертикальні або горизонтальні поверхні.

Рисунок 2.8 – Точка доступу TP-LINK EAP225

Цей бездротовий пристрій є високоефективною дводіапазонною точкою доступу, що підтримує стандарт Wi-Fi 5 (802.11ac). Вона забезпечує швидкість до 867 Мбіт/с у діапазоні 5 ГГц та 450 Мбіт/с у діапазоні 2.4 ГГц.

TP-LINK EAP225 оснащена одним Gigabit Ethernet портом (RJ45) з підтримкою технології Power over Ethernet (PoE) за стандартом 802.3af/at. Це означає, що пристрій отримує живлення безпосередньо через мережевий кабель, що усуває потребу в окремому кабелі живлення та значно спрощує розміщення точки доступу. Завдяки елегантному дизайну, що нагадує світильник, TP-Link EAP225 легко інтегрується в будь-яке офісне середовище, дозволяючи монтувати її на стіні чи підвішувати до стелі.

EAP225 є ідеальним рішенням для середовищ з високою щільністю клієнтів, таких як офіси, готелі або комп'ютерні клуби, забезпечуючи стабільну

та високу продуктивність. Вона пропонує оптимальний баланс між можливостями Wi-Fi 5, наявністю гігабітного порту та доступною ціною.

Однією з ключових переваг EAP225 є підтримка аутентифікації користувачів, що дозволяє адміністраторам ефективно контролювати доступ до бездротової мережі, забезпечуючи високий рівень безпеки.

2.4 Особливості монтажу мережі

Монтаж мережі ТОВ «Агрополіс» є критично важливим етапом, що забезпечує перетворення проєктних рішень у функціонуючу інфраструктуру. З огляду на обране обладнання та топологію, цей процес має низку особливостей, спрямованих на забезпечення надійності, продуктивності, безпеки та зручності подальшого обслуговування.

Перед монтажем мережевого обладнання серверної кімнати №4а потрібно забезпечити заходи фізичної безпеки – встановлення систем обмеження доступу (замки, можлива карткова система) та, за потреби, відеоспостереження, для захисту критично важливого обладнання.

Встановлюється комутаційна шафа WMNC-9U-FLAT розміром 600x450x380 мм. Вона надійно фіксується на стіні. У шафі організовано розміщується все активне та пасивне обладнання:

- головний комутатор Cisco Catalyst 3560CX-12XPD-S;
- комутатор Cisco Catalyst C1000-16T-2G-L для підмережі керівництва підприємства;
- маршрутизатор Cisco ISR4221/K9;
- блок безперебійного живлення APC Back-UPS Pro 1500VA;
- патч-панель Panduit 19" на 24 порти, Категорії 6.
- кабельні організатори для упорядкування кабелів.

Кабелі всередині шафи акуратно укладаються та фіксуються за допомогою кабельних організаторів, стяжок, маркується кожне з'єднання для легкого обслуговування та діагностики.

Основною складовою горизонтальної кабельної системи є кабель витої пари Категорії 6 (UTP), що забезпечує швидкість 1 Гбіт/с для кінцевих вузлів.

Для мережі, розташованої на одному поверсі, буде використана горизонтальна кабельна система, прокладена у спеціальних коробах IBOCO. Таке рішення забезпечує не лише естетичний вигляд, але й надійний захист кабелів від механічних пошкоджень, а також зручність подальшого обслуговування. Проходи кабелів крізь стіни виконуються у ПВХ трубках (діаметром 16 мм), тоді як ділянки, розташовані під підвісною стелею, захищені гофрованими ПВХ шлангами (діаметром 25 мм). Це відповідає чинним нормам пожежної безпеки та вимогам електромонтажу [1].

Для підключення кінцевих пристроїв на робочих місцях (біля ПК) передбачено встановлення зовнішніх мережевих розеток Cablexpert RJ45x1 UTP cat.6 на настінних коробах. Застосування конекторів ATCOM RJ45 CAT.6 UTP 8P8C, які відповідають стандарту TIA/EIA-568-B.2-1, гарантує високу продуктивність каналу передачі даних від користувача до комутатора.

Ці розетки розміщуються у легкодоступних місцях. Для сервісного центру, де робочі місця прилягають до стін, розетки встановлюються безпосередньо над кабельними коробами. Рекомендована висота монтажу – 60-90 см від підлоги, що забезпечує зручність підключення різноманітних пристроїв (телефонів, ноутбуків) та не перешкоджає проведенню прибирання."

У приміщеннях «Вдділу логістики» та «Відділу продажів» під фальшпідлогою у металічних коробах.

У місцях, де це передбачено проєктом, у плиті фальшпідлоги вирізаються отвори відповідного діаметру/розміру для монтажних лючків підлогових розеток. Важливо, щоб краї отворів були чистими та рівними. Кабель виводиться через трубу до лючка із запасом.

Жили кабелю Cat 6 зачищаються та розкладаються до відповідних контактів модулів RJ45 згідно з обраною схемою (T568B). Використовується спеціальний ударний інструмент для надійного контакту. Краї жил обрізаються.

Модулі RJ45 надійно встановлюються у рамки монтажних лючків (для підлогових розеток) або в настінні розетки.

Мережеві кабелі прокладаються окремо від силових ліній електроживлення для уникнення електромагнітних наведень та забезпечення стабільності сигналу.

Суворе дотримання допустимих радіусів вигину кабелів (не менше 4-8 зовнішніх діаметрів) під час прокладки, щоб уникнути пошкоджень та деградації характеристик кабелю.

Монтаж точки доступу TP-LINK EAP225 значно спрощується завдяки підтримці Power over Ethernet (PoE) за стандартом 802.3af/at. Це дозволяє живити пристрій безпосередньо через мережевий кабель, виключаючи необхідність прокладання окремих силових кабелів. Точка доступу розміщуються таким чином, щоб забезпечити оптимальне покриття Wi-Fi у залі для засідань.

Маршрутизатор Cisco ISR4221/K9 обрано з урахуванням наявності оптичного SFP-слота, що дозволяє здійснити пряме підключення до оптоволоконного кабелю Інтернет-провайдера. Це є ключовим для високошвидкісного та надійного зовнішнього зв'язку.

Усі металеві елементи комутаційної шафи та мережевого обладнання обов'язково заземлюються згідно з вимогами безпеки та стандартів.

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

2.5 Обґрунтування вибору програмного забезпечення

Вибір програмного забезпечення для мережі підприємтва ТОВ «Агрополіс» здійснюється з метою забезпечення стабільного функціонування, ефективного управління, високого рівня безпеки даних та продуктивної роботи співробітників, враховуючи як серверні, так і клієнтські потреби.

Для забезпечення стабільного функціонування та надійної роботи мережі ТОВ «Агрополіс» необхідно ретельно підібрати відповідне програмне забезпечення. Цей процес вибору має враховувати вимоги до ефективного керування мережею, високого рівня безпеки, постійного моніторингу та загальної оптимізації всіх мережевих процесів.

Одним із ключових та фундаментальних рішень при розгортанні IT-інфраструктури будь-якого підприємства, зокрема ТОВ «Агрополіс», є вибір серверної операційної системи (ОС). Саме ця ОС формує основу для розміщення всіх мережевих сервісів, додатків та управління даними. Для прийняття обґрунтованого рішення буде проведено огляд основних типів серверних ОС. Важливо зазначити, що критерії оцінки різняться: для серверних ОС пріоритетними є показники надійності, стійкості до зовнішніх загроз (безпека), періодичності оновлень та універсальності наданих сервісів. Натомість для операційних систем робочих станцій на перший план виходять простота використання, зручність для кінцевих користувачів та сумісність з необхідним прикладним програмним забезпеченням.

Вибір операційної системи (ОС) для серверної інфраструктури ТОВ «Агрополіс» є стратегічним рішенням, що безпосередньо впливає на стабільність, безпеку, ефективність управління та загальну продуктивність роботи підприємства. Метою цього вибору є забезпечення надійної платформи для файлового сервера, з потенціалом для розширення функціоналу, враховуючи як поточні, так і майбутні потреби компанії.

Для розгортання файлового сервера розглядалися наступні ключові серверні операційні системи: Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), Debian та Ubuntu Server. Кожна з цих ОС має свої унікальні переваги та недоліки, що робить їх придатними для різних сценаріїв використання.

Microsoft Windows Server – це універсальна серверна ОС, широко застосовується в корпоративних середовищах. Пропонує тісну інтеграцію з продуктами Microsoft (Active Directory, Exchange, SQL Server) [10].

Серед її переваг можна відзначити звичний графічний інтерфейс (GUI) для адміністраторів Windows, велика кількість сумісного програмного забезпечення та обладнання, покращені механізми безпеки в нових версіях.

Серед недоліків: висока комерційна вартість ліцензій (включаючи клієнтські ліцензії CALs), що суттєво збільшує загальні витрати на володіння (TCO); потенційно вищі вимоги до апаратних ресурсів [9].

Операційна система Red Hat Enterprise Linux (RHEL) – це комерційний дистрибутив Linux, лідер серед корпоративних рішень для великих підприємств та критично важливих інфраструктур.

Основними її первагами є виняткова стабільність та надійність, підвищена безпека завдяки інтегрованим механізмам (наприклад, SELinux) та регулярним оновленням, професійна довгострокова підтримка (до 10 років) від розробника, що спрощує довгострокове планування [9].

Серед недоліків можна відзначити високу початкова вартість ліцензій та підтримки; вимагає певних навичок роботи з командним рядком Linux, може повільніше інтегрувати новітні технології через акцент на перевіреній стабільності [9].

Linux Debian – це один з найстаріших і найавторитетніших дистрибутивів Linux, відомий своєю прихильністю до вільного ПЗ та надзвичайною стабільністю. Можна відзначити високу стабільність та надійність роботи цієї операційної системи завдяки ретельному тестуванню, широка сумісність з більшістю апаратних архітектур, повністю безкоштовний доступ до величезної кількості програмних пакетів.

Серед недоліків можна відзначити пвільне впровадження нових технологій через тривалий цикл тестування, комерційна підтримка надається сторонніми компаніями, а не безпосередньо розробником.

Ubuntu Server – це популярний дистрибутив Linux, що базується на Debian, розроблений компанією Canonical. Забезпечує відмінний баланс між функціональністю, зручністю та вартістю.

Серед переваг можна відзначити простоту встановлення та налаштування; широкий вибір програмного забезпечення, регулярні оновлення, включаючи LTS-релізи з п'ятирічною підтримкою, що гарантує довгострокову стабільність та безпеку, безкоштовний дистрибутив з активною спільнотою, що надає широку підтримку, висока гнучкість та безпека, придатний для широкого спектра завдань.

Після ретельного аналізу всіх представлених серверних операційних систем, для мережі ТОВ «Агрополіс» було прийнято рішення про впровадження операційної системи Ubuntu Server. Цей вибір є найбільш обґрунтованим з огляду на специфічні потреби та стратегічні цілі компанії:

Ubuntu Server є повністю безкоштовним дистрибутивом. Це забезпечує значну економію на ліцензійних платежах у порівнянні з комерційними операційними системами, такими як Microsoft Windows Server або RHEL, що суттєво знижує загальну вартість володіння інфраструктурою.

Незважаючи на те, що персонал «Агрополіс» може не мати глибокого досвіду роботи з Linux, Ubuntu Server вирізняється відносно простим процесом встановлення та інтуїтивно зрозумілими початковими налаштуваннями. Широка доступність онлайн-ресурсів, докладних посібників та активна спільнота користувачів дозволяють швидко розгорнути та підтримувати файловий сервер без необхідності постійного залучення дорогих зовнішніх IT-спеціалістів, що додатково оптимізує витрати на адміністрування.

ТОВ «Агрополіс» потребує постійного та безперебійного доступу до інформації. Ubuntu Server відомий своєю високою стабільністю. Зокрема, випуски LTS (Long Term Support) гарантують п'ятирічну підтримку та регулярні оновлення безпеки, що забезпечує довгострокову надійність функціонування системи. Це мінімізує ризики простоїв, які можуть призвести до затримок у роботі з клієнтами, зниження продуктивності та, як наслідок, втрати репутації та фінансових збитків.

З огляду на плани «Агрополіс» щодо розширення діяльності та впровадження нових сервісів, масштабованість Ubuntu Server є ключовою

перевагою. Він може ефективно слугувати не лише файловим сервером, а й розміщувати інші внутрішні служби, такі як база даних для обліку замовлень, внутрішній веб-сервер для інструкцій, або навіть прості CRM-системи. Ця гнучкість дозволяє адаптувати інфраструктуру до зростаючих потреб бізнесу без необхідності міграції на абсолютно нову платформу та значних капітальних вкладень.

Для забезпечення безперебійної роботи співробітників ТОВ «Агрополіс» та підтримки їхньої специфічної діяльності (аналітика, бухгалтерія, офісні завдання), ключовими критеріями вибору ОС для робочих станцій стали рівень підготовки персоналу та вимоги до програмного забезпечення. Враховуючи ці аспекти, було прийнято рішення стандартизувати робочі місця на базі операційної системи Microsoft Windows 11 Pro.

Вибір Windows 11 Pro забезпечує низку значних переваг [10]:

- сучасний та інтуїтивно зрозумілий дизайн системи спрощує адаптацію користувачів, які не мають глибоких IT-знань, мінімізуючи час на навчання та підвищуючи комфорт роботи;

- гарантована сумісність додатків. ОС надає надійну підтримку для всього спектра використовуваного прикладного програмного забезпечення, від стандартних офісних пакетів до спеціалізованих галузевих рішень для аналітики та фінансової звітності, що є критично важливим для безперервності бізнес-процесів;

- завдяки ефективному використанню ресурсів сучасного апаратного забезпечення, Windows 11 Pro забезпечує високу швидкість роботи системи, швидке завантаження та плавну багатозадачність, сприяючи підвищенню загальної продуктивності праці;

- вбудовані механізми автоматичних оновлень (через Центр оновлення Windows) гарантують своєчасне отримання патчів безпеки та функціональних поліпшень, а потужна підтримка драйверів та системна діагностика забезпечують стабільну роботу та захист від потенційних збоїв. Система також виконує непомітну фонову діагностику для превентивного виявлення проблем;

- висока сумісність з попередніми версіями додатків та вдосконалені алгоритми пошуку файлів і програм дозволяють користувачам ефективно працювати з існуючими даними та швидко знаходити необхідну інформацію, забезпечуючи безперервність робочих процесів.

2.6 Визначення функцій серверів

В мережі ТОВ "Агрополіс" сервер буде виконувати декілька ключових функцій. Основні послуги, що надаються центральним сервером:

- управління файлами та спільний доступ (Файловий Сервер). Забезпечить єдиний централізований репозиторій для всіх корпоративних документів та файлів, що забезпечує контрольований спільний доступ для всіх співробітників. Завдяки використанню Samba на Ubuntu Server, робочі станції (особливо Windows-клієнти) легко інтегруються з мережевими теками. Це гарантує порядок у зберіганні документів відділів (клієнтське обслуговування, бухгалтерія, логістика, кадри), проектних матеріалів, шаблонів та іншої оперативної інформації. Це спрощує документообіг, посилює контроль над версіями та доступом до даних, а також є основою для ефективного резервного копіювання, що знижує ризики втрати важливої інформації;

- сервер резервного копіювання здійснює автоматизоване та надійне резервування всіх критичних даних з робочих станцій та файлового сервера, що дозволяє миттєве відновлення у випадку непередбачених ситуацій. Використовуючи вбудовані можливості Linux (BorgBackup). Це включає користувацькі файли, конфігурації програм та інші важливі компоненти. Безкомпромісний захист від втрати даних через апаратні збої, випадкові видалення чи шкідливі програми (наприклад, віруси-шифрувальники). Гарантує безперервність бізнес-процесів через оперативне відновлення інформації, мінімізуючи фінансові та репутаційні втрати;

- моніторинг інфраструктури (Сервер Моніторингу) – здійснює безперервний збір та аналіз ключових метрик про стан мережевого обладнання

та серверів для раннього виявлення потенційних проблем. Інтеграція таких інструментів, як Prometheus (з Node Exporter) для серверних метрик, SNMP для мережевого обладнання, та Grafana для інтуїтивної візуалізації даних. Це дозволяє відстежувати навантаження CPU, використання пам'яті, дискового простору, мережевий трафік, температуру та інші життєво важливі показники.

2.7 Розподіл адресного простору мережевих вузлів

З метою ефективної та безпечної адресації пристроїв у локальній мережі сервісного центру було вирішено використовувати приватний адресний простір IPv4 класу C, а саме мережу 192.168.1.0/24. Цей вибір є оптимальним, оскільки він забезпечує до 254 унікальних IP-адрес, що з великим запасом покриває поточні потреби мережі, яка налічує 45 кінцевих пристроїв. Для подальшої логічної сегментації, покращення безпеки та оптимізації трафіку, мережу підприємства розділено на дев’ять віртуальних підмереж (VLAN), у відповідності із складом структурних підрозділів підприємства:

- Direct – керівництво підприємства, куди входять по 1 ПК директора, заступника директора із виробництва, офіс-менеджер (секретар). Всього 3 ком-п’ютери;
- Kadry – відділ кадрів із 2 ПК та інженер з охорони праці (1 ПК). Разом 3 комп’ютери;
- Bughal – бухгалтерія ТОВ “Агрополіс” із 5 комп’ютерів. Серед низх один комп’ютер рохташовано в кабіеті головного бухгалтера, 1 – в приміщенні каси та 3 – в самій бухгалтерії;
- Prodag – відділ продажів із 10 ПК;
- Logist – відділ логістики із 11 робочих станцій;
- Zakup – відділ закупівель та постачання із 3 комп’ютерів;
- Agronom – агрономічний відділ із 2 ПК;
- Techn – інженерно-технічний відділ із 4 комп’ютерів;
- Oper – відділ операторів оперативного обліку із 4 притроїв.

Ще одна десята підмережа із одного пристрою – це мережа сервера.

Потрібно врахувати, що при виділені діапазону IP-адрес необхідно додаи до кожної підмережі ще одну IP-адресу для мережевого шлюзу, який буде призначатись віртуальному інтерфейсу головного комутатора.

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

Ми використовуємо приватний IP-діапазон 192.168.1.0/24, який надає 256 адрес для розподілу. Для кожної віртуальної підмережі (VLAN) необхідно виділити:

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

На першому етапі потрібно відсортувати список підрозділів та необхідна кількість IP-адрес (включаючи шлюз). Це дозволяє уникнути "фрагментації" адресного простору та забезпечити можливість виділення менших підмереж з залишків великих блоків:

- Logist (Логістика): 11 ПК + 1 шлюз = 12 адрес;
- Prodag (продажі): 10 ПК + 1 шлюз = 11 адрес;
- Buhgal (бухгалтерія): 5 ПК + 1 шлюз = 6 адрес;
- Techn (інженерно-технічний): 4 ПК + 1 шлюз = 5 адрес;
- Oper (Оператори оперативного обліку): 4 пристрої + 1 шлюз = 5 адрес;
- Direct (дирекція): 3 ПК + 1 шлюз = 4 адреси;

- Kadry (відділ кадрів та інженер з охорони праці): 3 ПК + 1 шлюз = 4 адреси;
- Zakup (закупівлі та постачання): 3 ПК + 1 шлюз = 4 адреси;
- Agronom (Агрономічний відділ): 2 ПК + 1 шлюз = 3 адреси
- Serv (сервер): 1 пристрій + 1 шлюз = 2 адреси;
- Sw-Rout: 1 пристрій + 1 шлюз = 2 адреси.

Остання підмережа Sw-Rout створюється додатково для забезпечення обміну інформацією між головним комутатором та маршрутизатором мережі.

Для кожної підмережі необхідно визначити найменшу степінь двійки (2^n), яка вміщує необхідну кількість адрес (включаючи мережеву та широкомовну адреси, які не використовуються для хостів). Маска підмережі виводиться з кількості бітів для хостів (n), де загальна довжина IPv4 адреси – 32 біти, а довжина маски – 32−n:

- Logist (Логістика): 12 хостів. Найменший блок, що вміщує 12 адрес – 16 адрес (2^4). Кількість бітів для хостів = 4. Маска: 32−4=/28;
- Prodag (продажі): 11 хостів. Найменший блок: 16 адрес (2^4). Маска: /28;
- Buhgal (бухгалтерія): 6 хостів. Найменший блок: 8 адрес (2^3). Маска: /29;
- Techn (інженерно-технічний): 5 хостів. Найменший блок: 8 адрес (2^3). Маска: /29;
- Oper (Оператори оперативного обліку): 5 хостів. Найменший блок: 8 адрес (2^3). Маска: /29;
- Direct (дирекція): 4 хости. Найменший блок: 8 адрес (2^3). Маска: /29;
- Kadry (відділ кадрів та інженер з охорони праці): 4 хости. Найменший блок: 8 адрес (2^3). Маска: /29;
- Zakup (закупівлі та постачання): 4 хости. Найменший блок: 8 адрес (2^3). Маска: /29;
- Agronom (Агрономічний відділ): 3 хости. Найменший блок: 8 адрес (2^3). Маска: /29;
- Serv (сервер): 2 хости. Найменший блок: 4 адреси (22). Маска: /30;
- Sw-Rout: 2 хости. Найменший блок: 4 адреси (22). Маска: /30.

На третьому кроці потрібно послідовно призначити адресні блоки, починаючи з 192.168.1.0/24. Для першої підмережі Prodag IP-адреса 192.168.1.0/28. В діапазон входить 14 адрес від 192.168.1.1 до 192.168.1.14. Наступна адреса 192.168.1.15 буде бродкестом ціє підмережі.

Після цієї адреси, наступна буде IP-адресою другої підмережі Sales 192.168.1.16/28. В діапазон цієї підмережі входить 14 адрес від 192.168.1.17 до 192.168.1.30. Наступна адреса 192.168.1.31 буде бродкестом ціє підмережі. Результати поділу всіх підмереж на адресні блоки за цим алгоритмом представлено в таблиці 2.4.

Таблиця 2.4 – Розрахунок адресного простору для підмереж

Підме-режа	К-сть хост	Адреса мережі	Діапазон хостів	Адреса шлюзу	Бродкест
Logist	11+1	192.168.1.0/28	192.168.1.1 - 192.168.1.13	192.168.1.14	192.168.1.15
Prodag	10+1	192.168.1.16/28	192.168.1.17 - 192.168.1.29	192.168.1.30	192.168.1.31
Buhgal	5+1	192.168.1.32/29	192.168.1.33 - 192.168.1.37	192.168.1.38	192.168.1.39
Techn	4+1	192.168.1.40/29	192.168.1.41 - 192.168.1.45	192.168.1.46	192.168.1.47
Oper	4+1	192.168.1.48/29	192.168.1.49 - 192.168.1.53	192.168.1.54	192.168.1.55
Direct	3+1	192.168.1.56/29	192.168.1.57 - 192.168.1.61	192.168.1.62	192.168.1.63
Kadry	3+1	192.168.1.64/29	192.168.1.65 - 192.168.1.69	192.168.1.70	192.168.1.71
Zakup	3+1	192.168.1.72/29	192.168.1.73 - 192.168.1.77	192.168.1.78	192.168.1.79
Agronom	2+1	192.168.1.80/29	192.168.1.81 - 192.168.1.85	192.168.1.86	192.168.10.87
Serv	1+1	192.168.1.88/30	192.168.1.89	192.168.1.90	192.168.10.91
Sw-Rout	1+1	192.168.1.92/30	192.168.1.93	192.168.1.94	192.168.1.95

Кожна підмережа отримала свій унікальний діапазон IP-адрес та окремий шлюз, що призначений віртуальному інтерфейсу головного комутатора, який виконує функцію маршрутизатора між VLAN-ами.

Після розподілу IP-адрес для 10 підмереж, робочий адресний простір обмежується адресою 192.168.1.95. Таким чином, значна частина виділеного діапазону, а саме 159 IP-адрес від 192.168.1.96 до 192.168.10.255, залишається вільною. Цей невикористаний сегмент може бути ефективно зарезервований для створення окремої гостьової підмережі Wi-Fi, яка буде розгорнута в залі для засідань із номером кімнати №5 (див. додаток Б).

Оскільки, для Wi-Fi підмережі достатньо буде виділити 50 динамічно змінюваних адрес, то найменший блок, що вміщує 100 адрес – 128 адрес (2^7). Кількість бітів для хостів = 7. Маска: 32−7=/25.

Отже, адреса гостьової Wi-Fi-мережі буде 192.168.1.96/25/ В діапазон цієї підмережі входить 126 адрес від 192.168.1.97 до 192.168.1.222. Наступна адреса 192.168.1.223 буде бродкестом цієї підмережі. Шлюзом цієї підмережі буде адреса 192.168.1.222.

Для забезпечення постійної доступності та передбачуваності, IP-адреси всім стаціонарним пристроям будуть призначені статично.

DHCP-сервер буде налаштовано безпосередньо на комутаторі SwG, що дозволить централізовано керувати розподілом IP-адрес для мобільних пристроїв та спростить загальну конфігурацію мережі.

2.8 Тестування та налагодження мережі

Тестування та налагодження є заключним, але одним із найважливіших етапів після фізичного монтажу та базового налаштування мережі. Метою цього етапу є не лише перевірка відповідності розгорнутої інфраструктури проєктній документації, а й виявлення та усунення потенційних несправностей, а також оптимізація її роботи для забезпечення стабільного, ефективного та безпечного функціонування всіх сервісів.

Процес тестування та налагодження буде включати послідовну перевірку на трьох основних рівнях моделі OSI: фізичному, канальному та мережевому.

Тестування фізичного рівня включає [2]:

- ретельний огляд усіх прокладених кабелів, коробів, мережевих розеток та патч-панелей на предмет механічних пошкоджень, правильного кріплення та загальної акуратності монтажу. Обов'язкова перевірка коректності маркування всіх точок підключення для зручності подальшого обслуговування;
- використання професійного кабельного тестера (аналізатора СКС), що відповідає вимогам Категорії 6. Цей прилад виконує комплексне тестування кожної кабельної лінії на відповідність стандартам (включаючи перевірку цілісності, відсутність обривів/коротких замикань, правильність розшивки, загасання сигналу та перехресні наведення);
- звіти про тестування кожної кабельної лінії (зазвичай у цифровому вигляді) зберігаються як офіційне підтвердження відповідності структурованої кабельної системи стандартам та її готовності до експлуатації.

Тестування канального рівня включає [2]:

- після підключення робочих станцій та інших пристроїв перевіряється індикація Link/Activity на портах комутаторів (SwG, Sw1, Sw2, Sw3, Sw4, Sw5, Sw6) для підтвердження фізичного з'єднання;
- перевірка правильності налаштування всіх 10 віртуальних підмереж (VLAN ID, назви, асоціація з відповідними портами) на всіх комутаторах та маршрутизаторі (R1);
- тестування коректності передачі даних між пристроями, що знаходяться в межах однієї VLAN, а також підтвердження блокування трафіку між різними VLAN без проходження через маршрутизатор;
- перевірка коректної роботи транкових портів (з 802.1Q тегуванням) між усіма комутаторами та між головним комутатором (SwG) і маршрутизатором (R1), що забезпечує проходження трафіку для всіх VLAN.

Тестування мережевого рівня та вище включає [3]:

- перевірка, чи всі бездротові пристрої коректно отримують IP-адреси, маски підмереж, шлюзи за замовчуванням та адреси DNS-серверів від DHCP-сервера, налаштованого на кмутаторі третього рівня SwG;

- перевірка коректності налаштування статичних IP-адрес для файлового сервера (192.168.1.89) та робочих станцій, яким адреси призначаються статично;

- тестування доступу до файлового сервера з усіх робочих станцій, що знаходяться в різних VLAN. Це включає перевірку коректності маршрутизації трафіку між підмережами через маршрутизатор R1;

- перевірка з'єднання всіх робочих станцій з Інтернетом. Тестування функціональності DNS-сервера (перевірка розв'язання доменних імен, наприклад, через публічний DNS Google 8.8.8.8) та оцінка пропускної здатності каналу;

- перевірка доступу до спільних папок та файлів на файловому сервері (Samba) з усіх робочих станцій. Це включає тестування операцій читання, запису та видалення файлів з різними обліковими записами та їхніми дозволами;

- проведення базового тестування швидкості копіювання файлів для оцінки загальної продуктивності файлового сервера та мережі в цілому.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування активного комутаційного обладнання

3.1.1 Інструкції з налаштування комутаторів робочих груп

Налаштування активного комутаційного обладнання розпочинається з конфігурації комутаторів, які обслуговують окремі сегменти мережі. Цей процес включає виконання ключових завдань:

- присвоєння унікальних імен для ідентифікації пристроїв;
- встановлення параметрів безпеки, зокрема паролів аутентифікації для захищеного доступу до управління;
- налаштування інтерфейсів для підтримки VLAN з метою логічної сегментації мережі згідно з проектом.

Першим кроком є налаштування комутатора робочих груп, розташованого у серверній (див. Додаток Б). Для цього необхідно встановити консольне з'єднання з пристроєм. Після підключення система автоматично переходить у користувацький режим комутатора. Для присвоєння імені комутатору потрібно ввести команди 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 – Налаштування імені комутатора

Далі потрібно налаштувати парольний захист пристрою. Існує кілька типів паролів, які слід налаштувати для повного захисту комутатора [3]:

- пароль консолі (Console Password) – захищає фізичний доступ через консольний порт;
- пароль VTY (Virtual Teletype) або Telnet/SSH Password – захищає віддалений доступ до комутатора через Telnet або SSH;

- пароль режиму привілейованого виконання (Privileged EXEC Mode Password) – захищає доступ до режиму з розширеними правами (enable mode), де можна змінювати конфігурацію;

- команда, яка шифрує всі незашифровані паролі у конфігурації.

Налаштування пароля режиму привілейованого виконання здійснюється командою:

enable Secret <пароль>

Ця команда дозволяє зберігати пароль у зашифрованому вигляді.

Для встановлення паролю на консольний спочатку потрібно імьпвим консольний інтерфейс, а тоді встановити пароль для консолі командою password. Команда активує login запит пароля при підключенні до консолі. На рисунку 3.2 представлено налаштування паролю консольного доступу та режиму привілейованого виконання.

```
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 – Призначення паролів на привілейований режим та консоль

В даному випадку, в якості прикладу паролю вказано пароль “agropolis”.

Паролі VTY (Telnet/SSH) захищають віддалений доступ до комутатора через Telnet або SSH. Зазвичай існує кілька VTY-ліній (наприклад, 0 4), що дозволяє одночасно підключатися кільком адміністраторам. Повний набір команд для встановлення паролів на віддалений доступ представлено на рисунку 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 – Встановлення парою на відділений доступ по SSH

Для забезпечення захищеного віддаленого доступу додатково налаштовується протокол SSH. Крім того, з метою підвищення безпеки, усі паролі в конфігурації пристрою шифруються командою service password-encryption. Важливо зазначити, що у наведених прикладах використовується умовний пароль " agropolis ", який слід замінити на реальний, надійний пароль доступу.

Після цього необхідно створити користувача для SSH ввівши команди представлені 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 – Створення користувача SSH

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

Таблиця 3.1 – Назви та ідентифікатори підмереж VLAN

Кімната	Під'єднано до комутатора	Назва VLAN	Номер VLAN
Відділ логістики	Sw6	Logist	101
Відділ продажів	Sw3	Prodag	102
Бухгалтерія, головний бухгалтер, каса	Sw5	Buhgal	103
Інженерно-технічний відділ	Sw4	Techn	104
Оператори операторного обліку	Sw5	Oper	105
Директор, прийомна, заступник дирек.	Sw1	Direct	106
Відділ кадрів	Sw1	Kadry	107
Відділ закупівель та постачання	Sw2	Zakup	108
Агрономічний відділ	Sw2	Agronom	109
Сервер	SwG	Serv	110
Мережа із маршрутизатором	SwG	Sw-Rout	111

Створення віртуальних локальних мереж (VLAN) на комутаторі вимагає переходу в режим глобальної конфігурації. Далі, використовуючи команду vlan <номер>, де <номер> є унікальним ідентифікатором, створюється нова VLAN. Після цього за допомогою команди name <назва> [3] їй присвоюється зрозуміла назва. Відповідні команди проілюстровано на рисунку 3.5.

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

Рисунок 3.5 – Створення бази даних VLAN

Після створення VLAN необхідно перейти до налаштування типів портів комутатора, які забезпечуватимуть їх функціонування. Розрізняють два ключові типи:

- Access-порти – призначені для кінцевих пристроїв (ПК), передають нетегований трафік лише однієї VLAN;

- Trunk-порти – використовуються для міжкомутаторних з'єднань або підключення до маршрутизатора, передаючи тегований трафік кількох VLAN через одне фізичне з'єднання.

Згідно зі схемою топології (Додаток Б), для налаштування інтерфейсів комутатора Sw1 у режимі глобального конфігурування необхідно виконати наступні дії. Зокрема, останній інтерфейс Sw1 слід конфігурувати як транковий,

оскільки він з'єднуватиметься з головним комутатором SwG. Відповідні команди налаштування інтерфейсів для Sw1 ілюструє рисунок 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 – Налаштування інтерфейсів комутатора Sw1

Подібним чином потрібно налаштувати комутатори Sw2 – Sw6 вказуючи лише інші назви інтерфейсів та номери VLAN, відпоідно до даних таблиці 3.2.

Таблиця 3.2 – Визначення інтерфейсів комутаторів робочих груп

Назва комутатора	Інтерфейси комутатора	Типи порпів	Команда визначення інтферйсу
1	2	3	4
Sw1	GigabitEthernet0/1 - GigabitEthernet2/1	access	switchport access vlan 106
	GigabitEthernet3/1 – GigabitEthernet5/1	access	switchport access vlan 107
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 106,107
Sw2	GigabitEthernet0/1 - GigabitEthernet2/1	access	switchport access vlan 108
	GigabitEthernet3/1– GigabitEthernet4/1	access	switchport access vlan 109
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 108,109

Продовження таблиці 3.2

1	2	3	4
Sw3	GigabitEthernet0/1 – GigabitEthernet9/1	access	switchport access vlan 102
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 102
Sw4	GigabitEthernet0/1 – GigabitEthernet3/1	access	switchport access vlan 104
	GigabitEthernet4/1– GigabitEthernet6/1	access	switchport access vlan 105
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 104,105
Sw5	GigabitEthernet0/1 – GigabitEthernet4/1	access	switchport access vlan 103
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 103
Sw6	GigabitEthernet0/1 – GigabitEthernet4/1	access	switchport access vlan 101
	GigabitEthernet16/1	trunk	switchport trunk allowed vlan 101

Після налаштування комутаторів потрібно зберегти їх конфігурацію командою “copy running-config startup-config” [5].

3.1.2 Інструкції з налаштування головного комутаторів

Налаштування головного комутатора необхідно розпочтаи із призначеня його імені. При цьому необхідно виконати команди аналогічні до представлених на рисунку 3.1. Після цього на головному комутаторі необхідно налаштувтаи парольний захист та створити SSH-користувача. При цьому виконуються такі ж самі команди як і для комутаторів робочих груп (див. рисунки 3.2-3.4).

Оскільки, головний комутатор буде теж виконувати комутацію віртуальних підмереж, то на ньому також необхідно створити базу даних

віртуальних мереж. При цьому необхідно ввести команди представлені на рисунку 3.5

До головного комутатора безпосередньо будуть під'єднані підмережі сервера та з'єднання із маршрутизатором. Тому необхідно налаштувати інтерфейси до яких під'єднано сервер та маршрутизатор як access-порти. Всі інші інтерфейси необхідно перевести в транковий режим. Для цього необхідно ввести команди представлені на рискну 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 – Налаштування інтерфейсів головного комутатора

Після налаштування інтерфейсів головного комутатора необхідно активувати режим маршрутизації. Це виконується командою «ip routing» [3].

Наступним кроком є створення віртуальних інтерфейсів VLAN (SVI - Switched Virtual Interfaces) для кожної підмережі та призначення їм IP-адрес шлюзів. Відповідно до плану IP-адрес (Таблиця 2.4), цією адресою є остання доступна IP-адреса хоста у відповідній підмережі.

SVI є логічними інтерфейсами, тісно пов'язаними з конкретними VLAN, і відіграють ключову роль у забезпеченні функціональності комутатора на мережевому рівні (рівень 3). Кожен SVI функціонує як шлюз за замовчуванням (Default Gateway) для пристроїв, що знаходяться у відповідній VLAN. Це дозволяє трафіку, призначеному для переходу між різними VLAN, направлятися на IP-адресу SVI цієї VLAN. Оскільки комутатор має IP-адреси на різних SVI,

він отримує можливість маршрутизувати пакети між ними. Крім того, SVI може слугувати як IP-адресний інтерфейс для віддаленого управління комутатором (наприклад, через Telnet, SSH, SNMP, HTTP/HTTPS), при цьому для управління зазвичай використовується SVI Management VLAN [3].

Команди для виконання цих налаштувань представлені на рисунку 3.8 [4].

```
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 – Створення віртуальних інтерфейсів головного комутатора

```
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 – Створення віртуальних інтерфейсів головного комутатора (продовження)

Далі необхідно сконфігурувати статичний маршрут за замовчуванням. Цей маршрут відправляє весь трафік, що не відповідає жодному іншому запису в таблиці маршрутизації, у вказаний напрямок. Адресою наступного переходу для цього маршруту буде внутрішній IP-адрес маршрутизатора – 192.168.1.94,:

SwG(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.94

3.1.3 Інструкції з налаштування маршрутизатора

Конфігурація активного мережевого обладнання завершується налаштуванням маршрутизатора, який виконуватиме функцію шлюзу до Інтернету.

Для реалізації зазначеної функціональності, на фізичному інтерфейсі маршрутизатора, що підключений до головного комутатора, буде необхідно

налаштувати IP-адресу шлюзу із мережі між головним комутатором та маршрутизатором.

Проте, перш ніж перейти до конфігурації інтерфейсів, маршрутизатору слід призначити унікальне ім'я, використовуючи команди, ідентичні тим, що застосовувалися для комутаторів робочих груп (див. рис. 3.1). Аналогічно, необхідно налаштувати парольний захист маршрутизатора та створити обліковий запис користувача для захищеного віддаленого доступу через SSH. Відповідні команди для цих налаштувань представлені на рисунках 3.2 – 3.4.

Далі слід сконфігурувати інтерфейс маршрутизатора, під'єднаний до головного комутатора, призначивши йому IP-адресу 192.168.1.94 відповідно до даних таблиці 2.4. На іншому інтерфейсі, призначеному для під'єднання до провайдера Інтернет-послуг (ISP), необхідно встановити IP-адресу 161.12.9.10/16. Команди налаштування цих інтерфейсів проілюстровано на рисунку 3.9.

```
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 – Налаштування інтерфейсів маршрутизатора

Для забезпечення доступу до зовнішніх мереж, включаючи Інтернет, а також для обробки всього трафіку, який не має конкретного маршруту в таблиці маршрутизації, буде налаштовано статичний маршрут за замовчуванням. Весь немаршрутизований трафік буде спрямовуватися на IP-адресу шлюзу, наданого інтернет-провайдером.

Крім того, для забезпечення зв'язку маршрутизатора з усіма внутрішніми віртуальними підмережами, буде сконфігуровано статичні маршрути. Необхідна

інформація про IP-адреси та маски цих підмереж буде отримана з Таблиці 2.4. При цьому адресою наступного переходу (інтерфейсом доступу) для досягнення цих внутрішніх мереж слугуватиме IP-адреса віртуального інтерфейсу головного комутатора: 192.168.1.93/30. Відповідні команди для реалізації цих налаштувань представлені 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 – Налаштування маршрутизації на маршрутизаторі R1

Далі необхідно налаштувати трансляцію мережевих адрес (NAT). Ця функція є ключовою для забезпечення ефективного та безпечного доступу внутрішніх мереж до Інтернету, дозволяючи багатьом пристроям спільно використовувати одну публічну IP-адресу. Це не лише економить публічні IP-адреси, але й підвищує рівень безпеки мережі.

Для правильної роботи NAT спершу визначаються внутрішні та зовнішні інтерфейси маршрутизатора [5]. Потім створюється ACL для ідентифікації трафіку, який повинен бути трансляції, і цей ACL застосовується до відповідного інтерфейсу [5]. Детальні команди налаштування NAT наведено 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 – Налаштування NAT на маршрутизаторі

Для підмережі бездротових пристроїв (AP), що належить до VLAN ID 12, необхідно сконфігурувати DHCP-сервер. Цей сервер автоматично розподілятиме IP-адреси пристроям, які підключатимуться до мережі Wi-Fi. Фізичний інтерфейс маршрутизатора GigabitEthernet0/0/1 налаштований як транковий порт, що дозволяє передавати трафік усіх VLAN.

Спочатку потрібно створити окремий пулу DHCP, названого AP, спеціально для цієї VLAN. У налаштуваннях пулу слід вказати діапазон IP-адрес для видачі, адресу шлюзу за замовчуванням та адреси DNS-серверів, як це проілюстровано 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 – Налаштування DHCP-сервера на маршрутизаторі

3.2 Інструкції з налаштування засобів захисту мережі

Безпека мережевих пристроїв є дуже важливою як на стадії проєктування, так і протягом усього циклу експлуатації інформаційної системи. Ігнорування цього аспекту може призвести до руйнівних наслідків: від несанкціонованого керування мережевим обладнанням до витоку конфіденційної інформації. Подібні інциденти загрожують значними фінансовими збитками, репутаційними втратами та порушенням безперервності критичних бізнес-процесів.

Ефективний захист мережевої інфраструктури ґрунтується на впровадженні низки взаємопов'язаних механізмів [3]:

- надійна автентифікація та авторизація. Це передбачає встановлення складних, унікальних паролів для доступу до всіх мережевих пристроїв. Ключовим є також принцип мінімальних привілеїв: користувачам та сервісам надаються лише ті дозволи, які абсолютно необхідні для виконання їхніх функцій, що суттєво обмежує потенційні зловживання;

- мінімізація поверхні атаки. Одним із найефективніших методів є деактивація всіх невикористовуваних протоколів та сервісів. Кожен активний, але непотрібний сервіс або відкритий порт створює потенційний "вхід" для зловмисників. Деактивуючи надлишкові функції, ми значно зменшуємо кількість векторів для потенційних кібератак;

- автоматизація компонентів безпеки. Застосування функцій автоматичного підключення та активації захисних механізмів гарантує їхню постійну працездатність. Це мінімізує вплив людського фактора та підвищує загальну стійкість системи до загроз;

- контроль доступу за часом та оперативне реагування. Встановлення часових лімітів для підключення та активного використання мережевих ресурсів додає додатковий рівень контролю. Крім того, налаштування системи на автоматичне сповіщення про потенційні загрози дозволяє адміністраторам своєчасно реагувати на будь-які підозрілі дії або аномалії, запобігаючи можливим інцидентам.

У спроєктованій мережі "Агрополіс" особлива увага приділена безпеці активного мережевого обладнання – комутаторів та маршрутизатора. Для них передбачено багаторівневу систему парольного захисту:

- паролі для консольного доступу. Забезпечують безпеку при прямому (фізичному) підключенні до пристрою;

- паролі для віддаленого доступу через SSH. Захищають від несанкціонованого доступу під час віддаленого керування. Перевага надається SSH, оскільки він забезпечує шифрування трафіку, на відміну від незахищеного Telnet;

- паролі для входу до привілейованого режиму. Обмежують доступ до критично важливих налаштувань та функцій обладнання виключно авторизованим адміністраторам.

Детальні інструкції щодо налаштування цих паролів є невід'ємною частиною комплексних інструкцій з конфігурації комутаторів та маршрутизатора, представлених у розділі 3.1.

Для забезпечення всебічного та надійного захисту мережевої інфраструктури ТОВ "Агрополіс", окрім зазначених базових заходів, необхідно впровадити наступні ключові аспекти безпеки:

- управління обліковими записами користувачів та привілеями;
- захист кінцевих точок (робочих станцій);
- управління мережевим трафіком та доступом;
- резервне копіювання та відновлення даних;
- моніторинг та аудит;
- політика безпеки та навчання персоналу.

Управління обліковими записами користувачів та привілеями є фундаментом внутрішньої безпеки і полягає у наступному [2]:

- кожен користувач та сервіс повинні мати лише мінімально необхідні права доступу для виконання своїх функцій. Наприклад, майстрам не потрібен доступ до фінансової документації, а бухгалтерам – до операторів обробки;
- необхідно періодично переглядати всі облікові записи для видалення застарілих (наприклад, для колишніх співробітників) та перевірки відповідності прав доступу поточним обов'язкам користувачів;
- впровадження обов'язкової політики використання складних паролів (мінімум 12-14 символів, комбінація великих/малих літер, цифр, спецсимволів) та вимога їх регулярної зміни (наприклад, раз на 90 днів);
- для доступу до критично важливих систем (файловий сервер, система обліку клієнтів, віддалений доступ до мережі) запровадити 2FA/MFA. Це може бути реалізовано через SMS-коди, мобільні додатки-автентифікатори або апаратні ключі.

Основними етапами захисту робочих станцій є:

- встановлення та постійна підтримка актуального антивірусного ПЗ на всіх робочих станціях та серверах. Налаштування автоматичних оновлень та регулярного сканування;
- первеірка, що брандмауери активовані та налаштовані як на серверах, так і на кожній робочій станції для блокування небажаного трафіку;

- всі операційні системи, офісні пакети, браузери та інше прикладне ПЗ мають бути регулярно оновлені до останніх версій. Патчі безпеки виправляють відомі вразливості, які можуть бути використані зловмисниками;

- обмеження використання неперевірених USB-накопичувачів та інших знімних носіїв, оскільки вони є поширеним джерелом шкідливого ПЗ. Можливе впровадження політики, яка дозволяє використовувати лише авторизовані та попередньо просканові пристрої.

Ефективне управління мережевим трафіком та доступом передбачає [6]:

- мережу розділено на логічні сегменти (VLAN) (див. розділ 3.1). Це не лише обмежує поширення можливих атак, але й дозволяє застосовувати різні політики безпеки для кожного сегменту;

- конфігурація ACL на маршрутизаторі для контролю, який трафік може проходити між різними сегментами мережі, а також з/до Інтернету. Застосовувати принцип "заборонити все, що не дозволено явно";

- оцінка доцільності впровадження систем виявлення/запобігання вторгненням (IDS/IPS) для моніторингу мережевого трафіку на предмет підозрілої активності та блокування потенційних атак у реальному часі.

Резервне копіювання та відновлення даних є важливим для забезпечення стійкості до втрати даних [6]:

- впровадження автоматизованої системи для регулярного резервного копіювання всіх критично важливих даних (документів, баз даних, налаштувань серверів);

- дотримання стратегії 3-2-1:зберігати мінімум 3 копії даних, на 2 різних носіях, принаймні 1 копію зберігати поза офісом (наприклад, у хмарному сховищі або на зовнішньому диску, що зберігається в іншому безпечному місці);

- регулярне проведення тестового відновлення даних з резервних копій для підтвердження їхньої цілісності та здатності до відновлення у разі надзвичайної ситуації.

Моніторинг та аудит проводиться для раннього виявлення загроз [6]:

- налаштування збору та централізованого зберігання журналів подій з усіх мережевих пристроїв, серверів та робочих станцій. Журнали є неоціненним джерелом інформації для виявлення та розслідування інцидентів безпеки;

- впровадження системи моніторингу, яка відстежує стан мережевих пристроїв, завантаження каналів, активність користувачів та оперативно попереджає про аномалії.

Плітика безпеки та навчання персоналу [6]:

- розробка чіткого документу, що регламентує правила використання мережевих ресурсів, політику паролів, дії у разі виявлення підозрілої активності тощо;

- проведення регулярних тренінгів з кібербезпеки для всього персоналу "Агрополіс". Навчання має охоплювати розпізнавання фішингових листів, безпечне поводження з вкладеннями, неприпустимість розголошення паролів, та процедури повідомлення про будь-які підозрілі інциденти;

- розробка чіткого плану дій у разі виникнення інциденту безпеки (наприклад, зараження вірусом, несанкціонований доступ, витік даних). Цей план має включати кроки з ізоляції проблеми, її усунення, відновлення та аналізу першопричин;

Впровадження цих інструкцій дозволить "Агрополіс" створити надійний, багаторівневий захист своєї мережевої інфраструктури, що є життєво важливим для забезпечення безперебійної роботи, збереження даних клієнтів та підтримки високої репутації піжприємтсва.

3.3 Інструкція з використання тестових наборів та тестових програм

Ефективність та безпека комп'ютерної мережі не є статичними величинами; вони вимагають постійної уваги, починаючи від етапу впровадження і протягом усього життєвого циклу інфраструктури. Тестування – це не просто технічна рутина, а ключовий елемент стратегії забезпечення надійності та захищеності мережевих систем. Адже справжня безпека виходить

за рамки лише відбиття кібератак; вона охоплює гарантування безперебійної та оптимальної роботи. Навіть найменші конфігураційні помилки чи апаратні збої можуть призвести не тільки до повних відмов, але й до значного зниження продуктивності, що безпосередньо загрожує бізнес-процесам та фінансовій стабільності.

Для мінімізації ризиків, пов'язаних з непередбаченими збоями та падінням продуктивності, необхідно регулярно застосовувати комплексні діагностичні, тестові та профілактичні заходи. Для цих цілей існує широкий арсенал апаратних і програмних інструментів.

Серед найбільш доступних та широко застосовуваних є вбудовані утиліти операційних систем. В операційній системі Windows для діагностики мережі використовуються наступні потужні інструменти командного рядка [7]:

- ipconfig – ця команда надає швидкий знімок поточної конфігурації протоколу TCP/IP. Вона дозволяє миттєво перевірити IP-адресу пристрою, маску підмережі, шлюз за замовчуванням та DNS-сервери. Зокрема, функція ipconfig /flushdns незамінна для очищення кешу DNS, що часто вирішує проблеми з доступом до веб-ресурсів після змін у мережі;

- ping – невід'ємний інструмент для базової перевірки зв'язку між двома мережевими вузлами. Надсилаючи ICMP-запити до цільової IP-адреси або доменного імені, ping вимірює час відгуку, дозволяючи швидко оцінити наявність зв'язку та затримки в передачі даних;

- netstat – ця утиліта надає детальну інформацію про активні TCP/IP-з'єднання, відкриті (прослуховуючі) порти та загальну статистику мережевої активності. За допомогою netstat можна виявляти небажані або підозрілі з'єднання, ідентифікувати програми, що використовують мережу, та моніторити її безпековий стан;

- tracert (або traceroute) – дозволяє відстежити повний шлях, який проходить пакет даних від поточної робочої станції до віддаленого ресурсу. Відображаючи всі проміжні маршрутизатори ("хопи") та час, витрачений на

проходження кожного з них, tracert є незамінним для діагностики проблем з маршрутизацією та виявлення "вузьких місць" у мережевій інфраструктурі;

- route – ця команда використовується для перегляду та маніпулювання таблицями маршрутизації операційної системи. Вона надає можливість вручну додавати, видаляти або змінювати записи в таблиці маршрутизації, що є важливим для тонкого налаштування мережевого трафіку або вирішення проблем з доступом до певних мереж.

Тестування мережі "Агрополіс" буде здійснюватися у два послідовні етапи для забезпечення її як фізичної, так і логічної цілісності.

- етап 1 – перевірка фізичних з'єднань та кабельної системи;
- етап 2 – програмне тестування мережевої інфраструктури.

Етап перевірки фізичних з'єднань є фундаментальним, оскільки будь-які недоліки на цьому рівні унеможливлюють коректну роботу всієї мережі. Для діагностики фізичних з'єднань та електричних параметрів кабельної системи незамінним є кабельний тестер. Процедура тестування включає:

- візуальний огляд. Ретельна інспекція всіх роз'ємів на кабелях на предмет механічних пошкоджень (зламані контакти, пошкоджена ізоляція) або невідповідності колірній схемі розводки (стандарти T568A або T568B);
- підключення тестера. Один кінець мережевого кабелю (з роз'ємом RJ45) підключається до основного модуля кабельного тестера, а інший – до його віддаленого блоку (кінцевика);
- запуск тестування. Активація режиму тестування на кабельному тестері.
- аналіз індикації. Тестер послідовно перевіряє цілісність кожного провідника кабелю. У разі успішного з'єднання (для Ethernet зазвичай 8 провідників), на обох модулях тестера синхронно загоряються відповідні індикатори. Відсутність світлової індикації для певного провідника вказує на обрив або коротке замикання в цій лінії. У таких випадках для відновлення працездатності мережі може знадобитися заміна несправного відрізка кабелю або повторне обтискання роз'ємів.

На етапі програмного тестування мережі необхідно виконати наступні кроки, використовуючи системні утиліти.

Крок 1 – діагностика конфігурації за допомогою ipconfig:

- на кожному вузлі мережі (робочій станції, сервері) слід виконати команду ipconfig у командному рядку;
- ретельно перевірити отримані мережеві налаштування: IP-адресу вузла, маску підмережі, MAC-адресу, адресу шлюзу за замовчуванням та DNS-сервера;
- переконатися, що всі параметри точно відповідають проєкту мережі та її логічній структурі;
- у разі виникнення проблем з резолвінгом доменних імен (DNS-проблеми) необхідно спробувати очистити кеш DNS за допомогою команди: ipconfig /flushdns.

Після цих дій рекомендується перезавантажити вузол для повного оновлення мережевих налаштувань.

Крок 2 – перевірка зв'язку за допомогою ping:

- з однієї робочої станції послідовно "пропінгувати" шлюз, інші робочі станції, а потім сервери;
- команда ping відправляє ICMP-запити та очікує відповіді. Успішне з'єднання підтверджується отриманням пакету-відповіді із зазначенням часу (у мілісекундах), необхідного для відгуку.

Для добре налаштованої локальної мережі "Агрополіс" час відповіді не повинен перевищувати 10 мілісекунд.

Отримання повідомлення "Request timed out" (перевищено час очікування відповіді) може свідчити про такі проблеми:

- мережа не функціонує взагалі (наприклад, вимкнений комутатор або маршрутизатор).
- неправильно вказано IP-адресу одержувача.

Крок 3 – аналіз TCP/IP-з'єднань та портів за допомогою netstat. На цьому етапі необхідно проаналізувати активні TCP/IP-з'єднання та прослуховуючі порти на ключових вузлах, особливо на серверах.

Це дозволить переконатися, що всі необхідні сервіси працюють коректно, а також виявити будь-які несанкціоновані або підозрілі з'єднання, що може вказувати на компрометацію.

3.4 Моделювання мережі

Після завершення етапу проєктування мережі можна переходити до конфігурації обраних мережевих пристроїв, використовуючи термінальний доступ або інтерфейс командного рядка. Для моделювання цієї мережі застосовується програмний комплекс Packet Tracer, який дозволяє імітувати широкий спектр мережевого обладнання, включаючи комп'ютери, сервери, Ethernet-комутатори, маршрутизатори тощо.

Для цього потрібно спочатку із панелі панелі елементів (в лівому нижньому куті) повстановлювати всі мережеві пристрої та поз’єднувати їх кабелями відповідно до логічної схем представленої на рисунку 2.1. При цьому слід враховувати, що однорівневі щодо OSI-моделі пристрої з’єднують кросовим кабелем, а інші – звичайним.

Під’єднання пристроїв по портах здійснюється у відповідності зі схемою фізичного з’єднання по VLAN, представленою у таблиці 3.1. Пристрої для яких передбачено безпровідне з’єднання потрібно слід під’єднати через Wi-Fi-адаптер, а фізично до провідного інтерфейсу комутатора не під’єднувати, хоча порт для них зарезервувати.

Наступним кроком є призначення статичних IP-адрес кінцевим вузлам мережі згідно з розробленою картою IP-адрес. Для конфігурування мережевої адреси кінцевого пристрою необхідно клікнути лівою клавішею миші на відповідному ПК, перейти на вкладку "Desktop" та обрати застосунок "IP Configuration". Далі, відповідно до схеми адресації пристроїв, слід вказати IP-адресу, мережеву маску та адресу шлюзу. В якості IP-адреси DNS-сервера необхідно задати адресу сервера S1 – 8.8.8.8 (див. рис. 3.13).

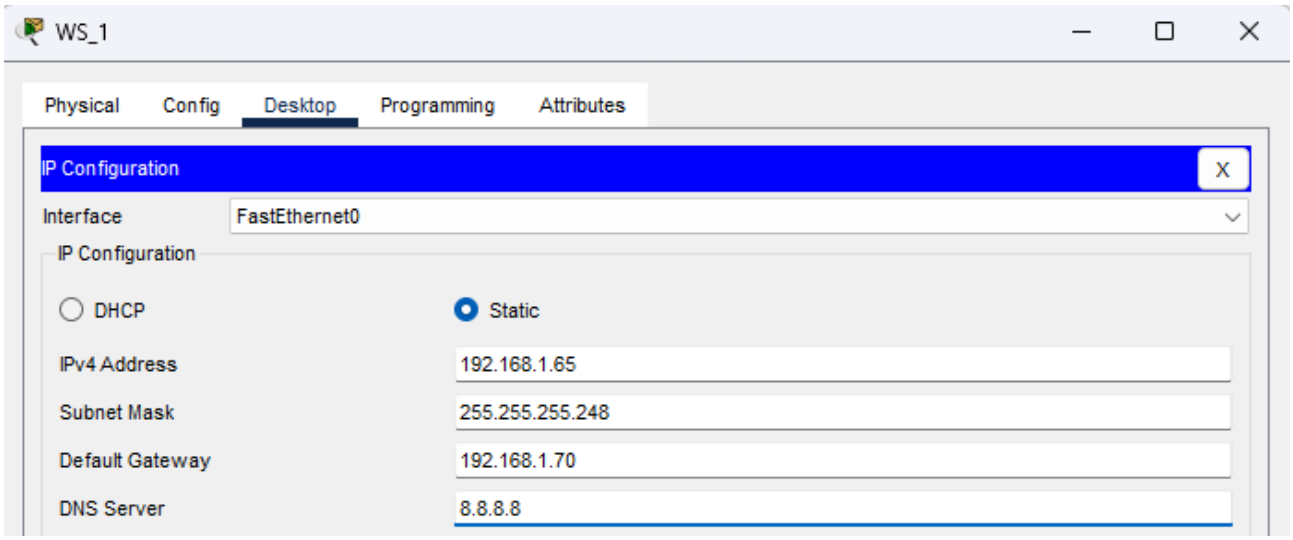


Рисунок 3.13 – Призначення IP-адресації комп'ютерів на прикладі вузла WS_1

Для налаштування безпровідних точок доступу потрібно відкрити вікно налаштування пристрою і у вкладці Config вибрати ліворуч розділ Port 1 і ввести SSID мережі, вказати тип аутентифікації WPA2-PSK та вказати пароль і тим шифрування, як це представлено на рисунку 3.14 для точки доступу AP1.

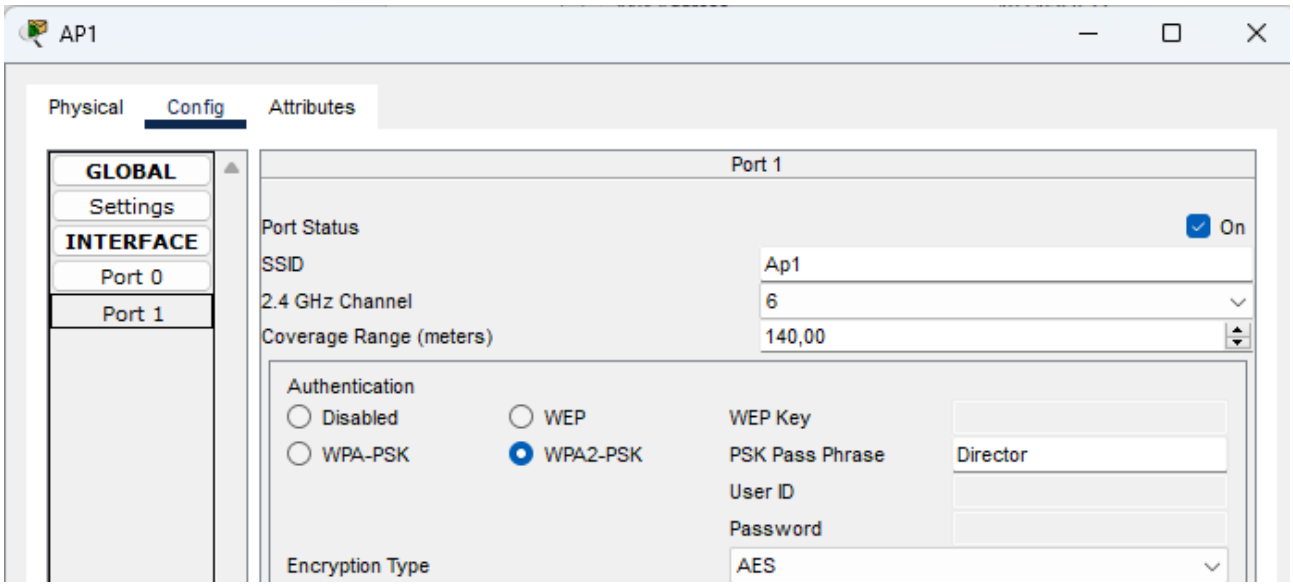


Рисунок 3.14 – Налаштування безпровідної точки доступу

Після цього на кожному безпровідному пристрої слід теж вказати SSID та пароль, що відповідає тій безпровідній точці доступу, до якої він повиненг бути під'єднаний згідно із схемою мережі.

Налаштувавши кінцеві вузли переходимо до налаштування активного мережевого обладнання. Розпочнемо цей процес із налаштування комутаторів окремих сегментів мережі.

Налаштування цих комутаторів полягає у налаштуванні їх імен, інтерфейсів для під'єднання до VLAN та встановленні параметрів захисту із використанням паролів аутентифікації/. Процес налагодження активного мережевого обладнання детально розглянуто в розділі 3.1.

На кожному комутаторі вибрати вікно налаштувань та перейти в закладку CLI для роботи із командним рядком Cisco IOS та ввести всі команди налаштування VLAN, представлені в розділі 3.1.

Так само потрібно налаштувати інтерфейси на маршрутизаторі. Для цього слід клікнути на ньому і вибрати закладку CLI та ввести команди налаштування описані в розділі 3.1

Крім цього потрібно налаштувати маршрут за замовчуванням, який буде направляти всі пакети даних із адресами, які не належать до локальної мережі на інтерфейс пристрою ISP провайдера до кого під'єднано дану локальну мережу.

Остаточний проект мережі представлено у додатку В.

Для тестування спроектованої мережі виконано перевірку з'єднання між пристроями, що належать до різних VLAN за допомогою команди ping. Перевірка виконувалась із робочої станції WS_1, що належить до підмережі VLAN 1 Крім цього, проведено перевірку маршрутів проходження пакетів командою tracert.

3.5 Тестування роботи побудованої моделі мережі

Для моделювання роботи мережі потрібно в програмі Cisco Packet Tracert перейти в режим емуляції роботи мережі, вибравши в правому нижньому куті вікна кнопку Simulation, а тоді Play.

Щоб перевірити роботу мережі центрального офісу слід пропінгувати зв'язок між комп'ютерами, що належать іншим шести підмережам. Для цього

слід клікнути на довільному комп'ютері (в жданому випадку PC61 із підмережі Net 4) і вибрати у вікні, що відкриється закладку Desktop, а тоді Command Prompt. Тоді почергово вводити команду ping із адресами комп'ютерів різних підмереж, починаючи із сервера – 192.168.1.89 (див. рис. 3.15).

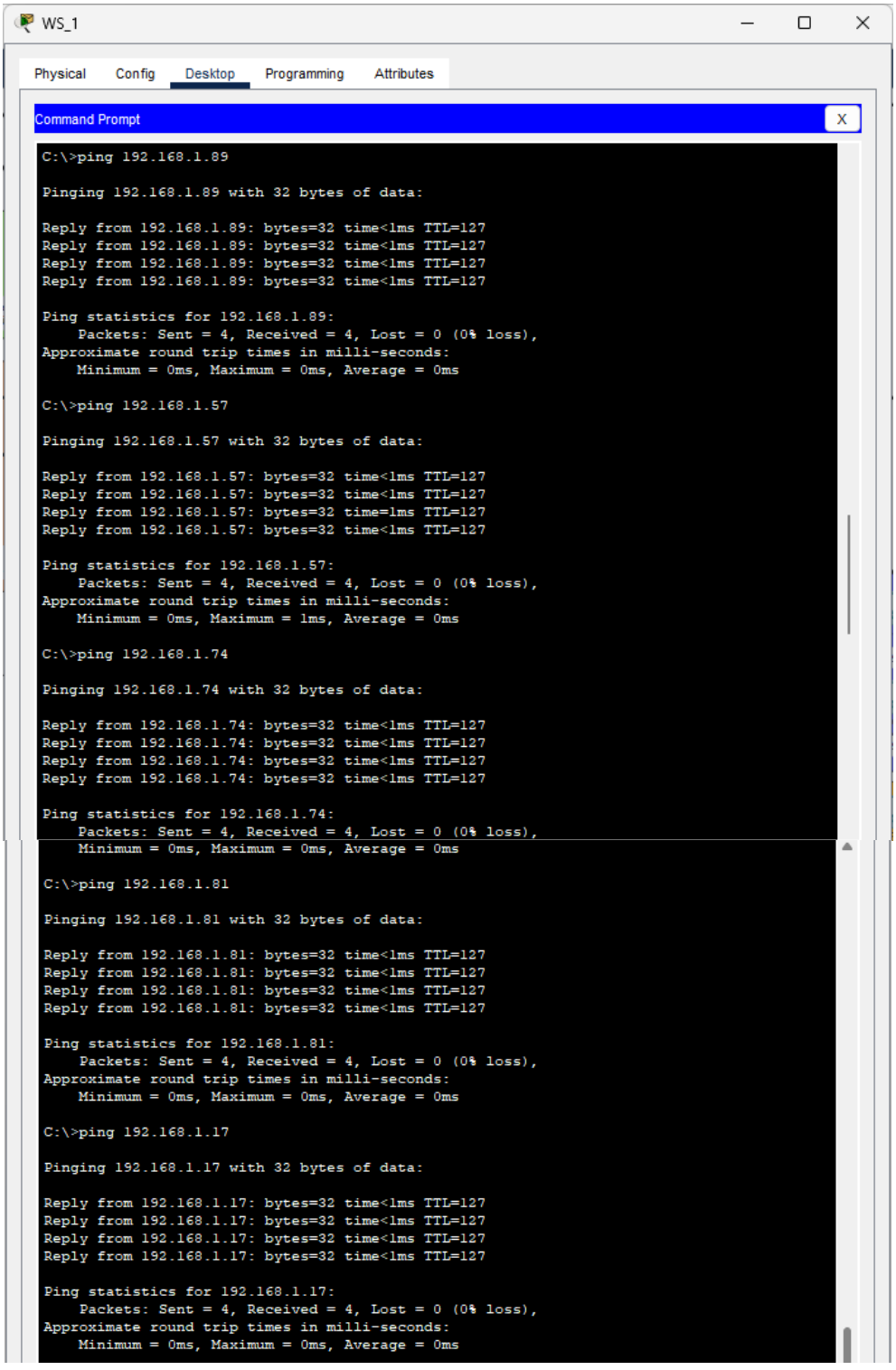


Рисунок 3.15 – Тестування з'єднання командою ping

Для перевірки повного маршруту проходження даних по мережі та визначення затримок на різних ділянках також можна скористатись командою tracert (див. рис. 3.16).

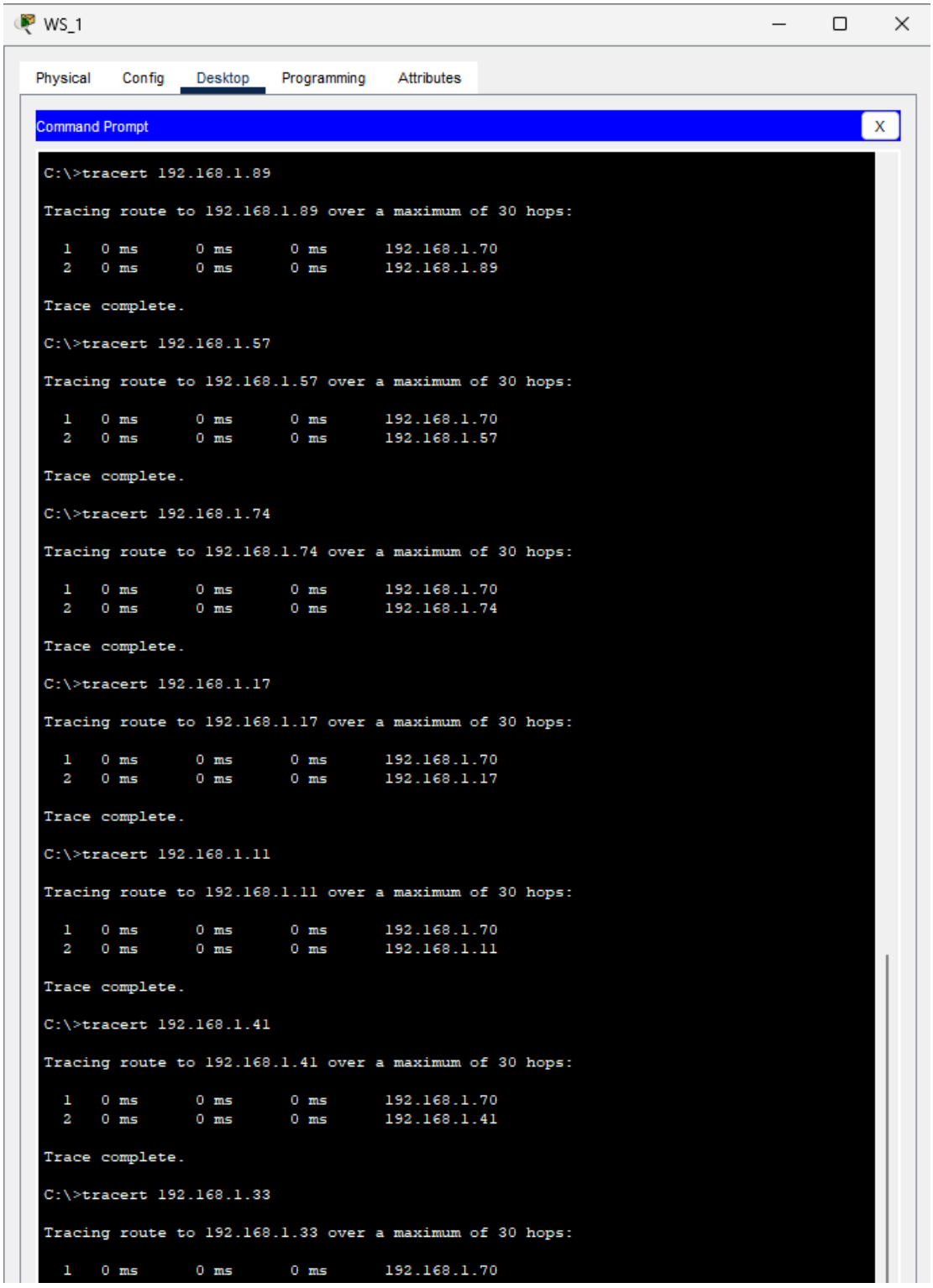


Рисунок 3.16 – Тестування мережі командою Tracert

Всі виконані команди тестування мережі ТОВ “Агрополіс” були успішними, тому можна зробити висновок, що мережа офісу підприємства із створеною статичною маршрутизацію побудована успішно.

Також для перевірки маршрутизації можна скористатись командою show ip route. Для цього слід на одному із маршрутизаторів ввести в привілейованому режимі команду "show ip route". Результат виконання цієї команди представлено на рисунку 3.17. Як видно із рисунку 3.17 в таблицях маршрутизації присутні дані підмереж.

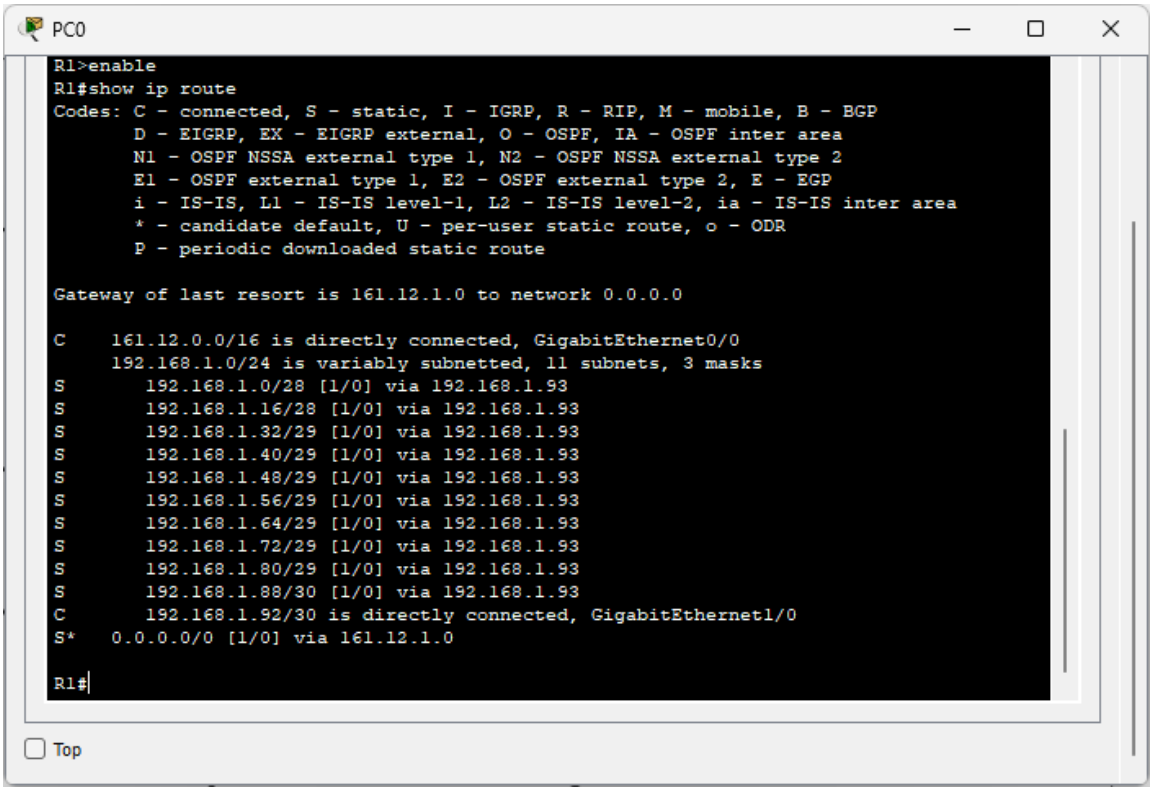


Рисунок 3.17 – Перегляд таблиць маршрутизації

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 ТОВ «Агрополіс». Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури ТОВ «Агрополіс» 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 обмежується.

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Виходячи з рекомендованих тарифних ставок встановимо таку ставку для керівник проекту – 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:

$$З_{дод}=286 + 936 + 487,5 = 1995,5 \text{ грн.}$$

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:

$$В_{о.п.}= 13150 + 1995,5 = 15145,5 \text{ грн.}$$

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.

$$В_{с.з} = 15145{,}5 \cdot 0{,}22 = 3332{,}01 грн.$$

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
		Тарифна 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	1995,5	3332,01	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:

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

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} \sum M_{B_i} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа Hypernet WMNC-6U-FLAT	шт.	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			-	-	257 633

Отже, загальна сума матеріальних витрат на розробку мережі становить 257633 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,

$$Т_В = 257633 \cdot 0,08 = 20610,64 \text{ грн.}$$

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:

$$A = \frac{26500 \cdot 0{,}04}{150} \cdot 10 = 70{,}67 \text{ грн}$$

4.7 Обчислення накладних витрат

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

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

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

де H_B – накладні витрати.

$$H_B = 6863 \cdot 0{,}4 = 2745{,}2 \text{ грн.}$$

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)	15145,5	5,23
Відрахування на соціальні заходи	3332,01	1,15
Матеріальні витрати	257633	86
Витрати на електроенергію	35	0,01
Транспортні витрати	20610,64	7,12
Амортизаційні відрахування	70,67	0,02
Накладні витрати	2745,2	0,95
Собівартість	299572,02	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 $С_В$=299572,02 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:

$$Ц = 299572{,}02 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 467332{,}35 \text{ грн}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

де *П* – прибуток;

C_B – собівартість;

$$П = 467332{,}35 - 299572{,}02 = 167760{,}33$$

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.	299572,02 грн.
2.	Плановий прибуток, грн.	167760,33 грн.
3.	Ціна, грн.	467332,35 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп'ютерної мережі для аграрного підприємства ТОВ «Агрополіс» становить 467332,35 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 ТОВ “Агрополіс”, де міститься найбльше ПК

Рівень освітленості впливає на працездатність та самопочуття. Державні норми це враховують та визначають, яким має бути освітлення приміщень, залежно від їх призначення, а також робочих місць. Відштовхуючись від цих норм, планують освітлення об'єктів, а значить, від них безпосередньо залежить і те, які світильники та скільки лампочок необхідно купити.

Освітлення робочого місця нормується згідно з Державними будівельними нормами України: 12. ДБН В.2.5-28-2018 Інженерне обладнання будинків і споруд [12].

Мінімальна освітленість встановлюється в залежності від розряду виконуваних зорових робіт. Для IV розряду зорових робіт вона складає 300...500 лк.

У приміщення ТОВ «Агрополіс» найбільша кількість комп’ютерів (11 шт) сконцентрована в приміщенні відділу логістткик (див. додаток Б). Розміри приміщення:

- довжина (L) = 7 м;
- ширина (W) = 5 м
- висота стелі (H) = 2,7 м

Обчислимо площу приміщення (S):

$$S=L\times W=7\text{ м}\times 5\text{ м}=35\text{ м}^2. \quad (5.1)$$

Тип приміщення для якого проводитьсяч розрахунок – офісне приміщення з великою кількістю ПК.

Згідно з ДБН В.2.5-28:2018 "Природне і штучне освітлення" для офісних приміщень з постійною роботою за комп'ютерами (ВДТ-робочі місця) нормована освітленість на робочій поверхні становить E = 500 лк (люкс) [11].

Висота робочого столу становить 0,85 м. Необхідно розрахувати висоту від робочої поверхні до світильника (hm), врховуюч, що виотса стелі 2,7 метра:

$$hm = 2{,}7 \text{ м} - 0{,}85 \text{ м} = 1{,}85 \text{ м}. \quad (5.2)$$

Коефіцієнт запасу (MF - Maintenance Factor) – враховує зниження світлового потоку ламп з часом та забруднення світильників. Для офісних приміщень з регулярним прибиранням приймаємо MF=0,8.

Далі необхідно вибрати тип сітильника. Для сучасного офісу оптимальним вибором є LED-панелі, які забезпечують рівномірне розсіяне світло, високу енергоефективність та довговічність. Оберемо типову LED-панель розміром 600x600 мм, преставлену на рисунку 5.1 [11]:

- потужність: 36 Вт;
- світловий потік одного світильника (Ф_lamp): 3600 лм (люменів);
- колірна температура: 4000K-5000K (нейтральний або холодний білий, комфортний для офісної роботи);
- індекс передачі кольору (Ra): >80.
- показник дискомфортної блискучості (UGR - Unified Glare Rating): Для роботи з ПК UGR повинен бути <19. Це критично важливо для запобігання втоми очей та дискомфорту.

Рисунок 5.1 – LED-панель BAFRA LIGHTING 600x600 мм

Розрахунок освітлення буде провелдено методом коефіцієнта використання світлового потоку. Для цого на першому кроці потрібно розрахувуати коефіцієнта приміщення (k_room) за формулою:

$$k_{room} = \frac{L \text{ x } W}{(L + W) \text{x } h_m} = \frac{7 \text{ x } 5}{(7 + 5) \text{x } 1{,}85} = \frac{35}{22{,}2} \approx 1{,}58 \quad (5.3)$$

Далі слід визначити коефіцієнта використання світлового потоку (UF – Utilization Factor), який залежить від коефіцієнтів відбиття поверхонь (стеля/стіни/підлога) та світлорозподілу світильника. Для офісних приміщень з типовими світлими поверхнями (наприклад, стеля 0,7, стіни 0.5, підлога 0.2) та світильників з розсіяним світлом, при kroom≈1.6, приймаємо UF = 0,6.

На третьому кроці слід розрахувати сумарно необхідний світловий потік (Ф_total) за формулою:

$$\Phi_{total} = \frac{E \text{ x } A}{UF \text{ x } MF} = \frac{500\text{лк x } 35\text{ м}^2}{0{,}6 \text{ x } 0{,}8} = \frac{17500}{0{,}48} \approx 36458{,}33\text{лм} \quad (5.4)$$

Далі необхідно визначити необхідну кількість світильників (N) за формулою:

$$N = \frac{\Phi_{total}}{\Phi_{lamp}} = \frac{36458{,}33\text{ лм}}{3600\text{ лм/світильник}} \approx 10{,}13 \quad (5.5)$$

Оскільки кількість світильників не може бути дробовою, округлюємо в більшу сторону. Для забезпечення рівномірного та естетичного розподілу, а також з урахуванням норми в 500 лк, доцільно використати 12 світильників.

Перевірка фактичної освітленості при 12 світильниках:

$$(E\_fact) = \frac{N \text{ x } \Phi_{lamp} \text{ x } UF \text{ x } MF}{A} = \frac{12 \text{ x } 3600\text{ лм x } 0{,}6 \text{ x } 0{,}8}{35\text{ м}^2} = \frac{20736}{35} \approx 592{,}46\text{ лк} \quad (5.6)$$

Фактична освітленість 592,46 лк перевищує нормоване значення 500 лк, що є прийнятним і навіть кращим для комфортної роботи.

Для приміщення 7x5 метрів та 12 світильників оптимальним буде симетричне розміщення у 3 ряди по 4 світильники або 4 ряди по 3 світильники.

Варіант 1 (3 ряди по 4 світильники, вздовж довшої сторони):

По довжині 7 м – 4 світильники. Інтервал між світильниками та від стін: 4+17=57=1,4 м (це якщо рахувати інтервали, але краще: 4 світильника, 3 проміжки між ними, 2 проміжки до стін.

$$x+3x+3x+3x+x=7 \text{ -> } 11x=7 \text{ -> } x=0.875\text{m}. \quad (5.7)$$

Отже, 0.875м від стін, 1.75 м між світильниками.

По ширині 5 м – 3 світильники:

$$y+2y+2y+y=5 \text{ -> } 6y=5 \text{ -> } y=0.85\text{m}. \quad (5.8)$$

Отже, 0.85м від стін, 1.65 м між світильниками. Схема розмішення світильників представлена на рисунку 5.2.

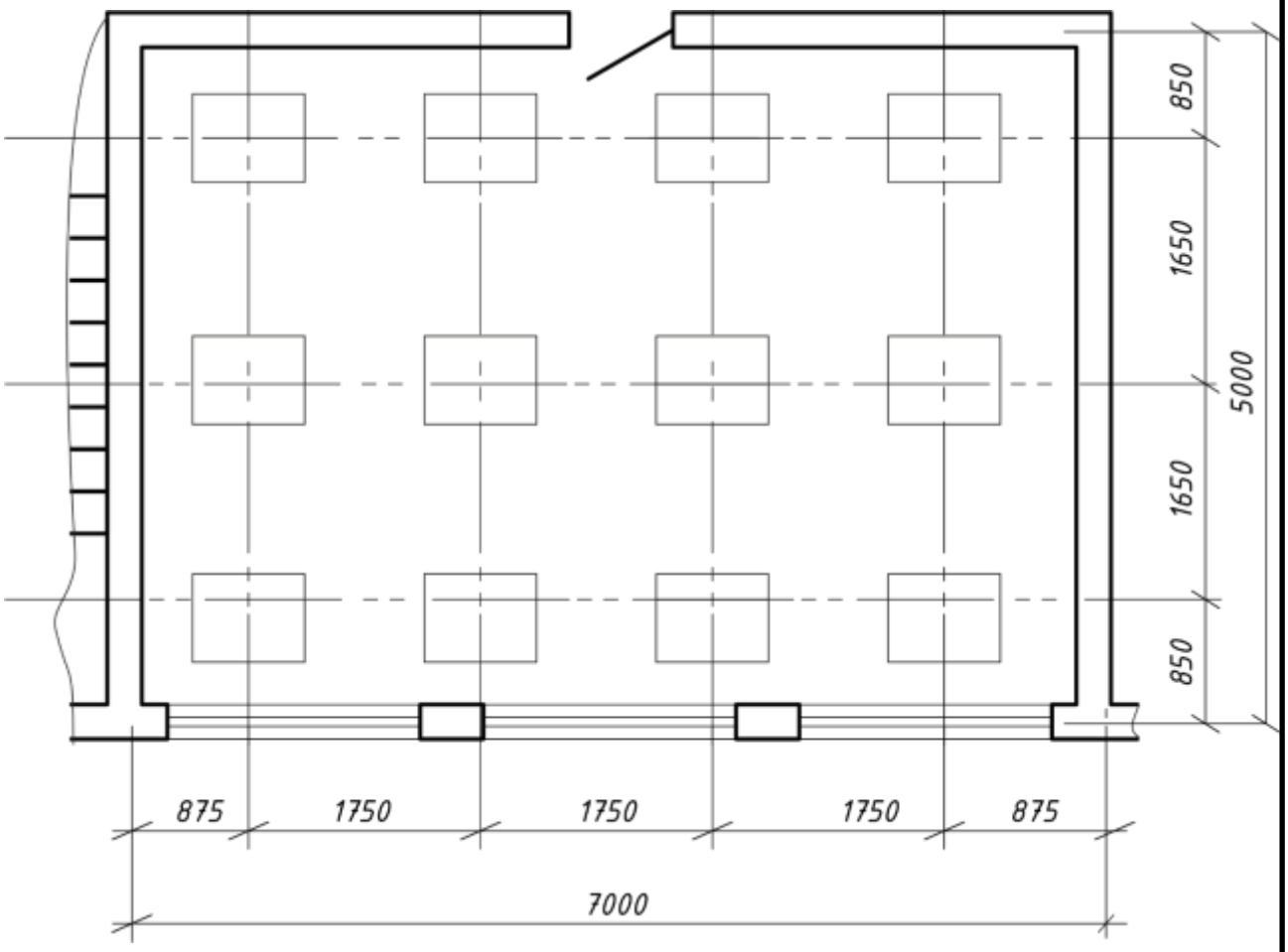


Рисунок 5.2 Схема розташування світильників

Таке розміщення забезпечить рівномірне освітлення.

Додаткові вимоги при виборі світильників:

– обов'язково обирати LED-панелі з низьким показником UGR (<19), спеціально призначені для офісів з ПК, щоб уникнути блискучості та втоми очей;

– світильники повинні бути розміщені таким чином, щоб забезпечити рівномірність освітлення на робочих поверхнях не менше 0,7;

– розміщення світильників відносно робочих місць слід планувати так, щоб світло не створювало прямих або відбитих від екранів ПК відблисків;

– можна розглянути інтеграцію з системою керування освітленням (наприклад, з датчиками присутності або освітленості) для додаткової енергоефективності.

Таким чином, для приміщення ТОВ «Агрополіс» розміром 7х5 метрів з 11 ПК рекомендується встановлення 12 LED-панелей (36 Вт, 3600 лм, UGR<19), що забезпечить нормовану освітленість понад 500 лк та комфортні умови для роботи.

5.2 Особливості заходів електробезпеки в ТОВ “Агрополіс”

Виділяють три системи засобів і заходів забезпечення електробезпеки [5]:

– система технічних засобів і заходів;
– система електрозахисних засобів;
– система організаційно-технічних заходів і засобів.

Технічні засоби і заходи з електробезпеки реалізуються в конструкції електроустановок при їх розробці, виготовленні і монтажі відповідно до чинних нормативів. За своїми функціями технічні засоби і заходи забезпечення електробезпеки поділяються на дві групи [4]:

– технічні заходи і засоби забезпечення електробезпеки при нормальному режимі роботи електроустановок;
– технічні заходи і засоби забезпечення електробезпеки при аварійних режимах роботи електроустановок.

Основні технічні засоби і заходи забезпечення електробезпеки при нормальному режимі роботи електроустановок включають [2]:

– ізоляцію струмовідних частин;
– недоступність струмовідних частин;
– блоківки безпеки;
– засоби орієнтації в електроустановках;
– виконання електроустановок, ізольованих від землі;
– захисне розділення електричних мереж;

– компенсацію ємнісних струмів замикання на землю;

– вирівнювання потенціалів.

Із метою підвищення рівня безпеки, залежно від призначення, умов експлуатації і конструкції, в електроустановках застосовується одночасно більшість з перерахованих технічних засобів і заходів.

Ізоляція струмовідних частин. Забезпечує технічну працездатність електроустановок, зменшує вірогідність потраплянь людини під напругу, замикань на землю і на корпус електроустановок, зменшує струм через людину при доторканні до неізольованих струмовідних частин в електроустановках, що живляться від ізольованої від землі мережі за умови відсутності фаз із пошкодженою ізоляцією. ДСТУ EN 50110-1:2019 "Експлуатація електричних установок. Частина 1. Загальні вимоги" розрізняє ізоляцію [11]:

– робочу – забезпечує нормальну роботу електроустановок і захист від ураження електричним струмом;

– додаткову – забезпечує захист від ураження електричним струмом на випадок пошкодження робочої ізоляції;

– подвійну – складається з робочої і додаткової;

– підсилену – поліпшена робоча ізоляція.

Аграрне підприємтсво ТОВ “Агрополіс” здійснює вирощення та обробку сільськогосподарської продукції, що пов'язано з різноманітністю виробничих процесів, використанням потужного обладнання, роботою на відкритому повітрі та специфічними умовами сільськогосподарського середовища (вологість, пил).

При викорристанні сільськогосподарська техніка та обладнання є наступні особливості електробезпеки:

– використання електродвигунів високої потужності в комбайнах, тракторах, насосах, вентиляційних системах тощо вимагає особливої уваги до стану ізоляції, заземлення та захисних пристроїв;

– електробезпека при використанні пересувних агрегатів (зварювальні апарати, електроінструмент) потребує ретельного контролю за станом кабелів, штепсельних з'єднань та наявності захисного відключення (ПЗВ);

– ремонт та обслуговування електрообладнання повинні проводитися тільки кваліфікованим персоналом після відключення від електромережі та вжиття заходів проти випадкового ввімкнення;

– ефективна система захисного заземлення та занулення є критично важливою для запобігання ураженню електричним струмом при пошкодженні ізоляції.

Заходи та засоби електробезпеки на території агропідприємства ТОВ “Агрополіс” :

– на відкритому повітрі електропроводка піддається впливу атмосферних опадів, температурних коливань та механічних пошкоджень, що потребує посиленого контролю за її станом;

– у зерносховищах та інших виробничих зонах підвищена вологість та запиленість можуть негативно впливати на ізоляцію електрообладнання та збільшувати ризик ураження струмом;

– використання хімічних речовин (добрив, засобів захисту рослин) може призводити до корозії металевих частин електроустановок та пошкодження ізоляції;

– наявність високих споруд та великих відкритих площ робить агрофірми вразливими до ударів блискавки, тому необхідно передбачати ефективну систему блискавкозахисту;

– при використанні електрообладнання в полях необхідно враховувати можливість пошкодження кабелів сільськогосподарською технікою та вплив погодних умов.

Заходи та засоби електробезпеки в офісних приміщекннях агропідприємтсва ТОВ “Агрополіс”:

– використовуються розеток із заземлюючими контактами;

– контроль кількості одночасно підключених пристроїв до однієї розетки або подовжувача, щоб запобігати перевантаженню електричної мережі;

– використовуються лише сертифіковані подовжувачі відповідної потужності. Регулярно перевіряти їх на пошкодження;

– будь-який ремонт або заміна розеток та вимикачів повинна здійснюватися кваліфікованим електриком при відключеному живленні;

– регулярно проводиться обслуговування електрообладнання (очищення від пилу, перевірка контактів);

– використання електроприладів відповідно до інструкцій виробника.

Організаційні заходи:

– призначено відповідальних за електрогосподарство та електробезпеку на окремих ділянках;

– весь персонал, який працює з електрообладнанням або в зонах підвищеної електронебезпеки, проходить відповідне навчання та інструктажі;

– до самостійної роботи з електрообладнанням допускаються особи, які мають відповідну кваліфікаційну групу з електробезпеки;

– електроустановки та електрообладнання підлягають регулярним плановим перевіркам та випробуванням відповідно до встановлених норм;

– персонал забезпечений необхідними засобами індивідуального захисту (діелектричні рукавиці, взуття, килимки тощо);

– на території агропідприємтсва розміщені плакати з електробезпеки та попереджувальні знаки;

– в офісних приміщеннях знаходяться інструкції з надання першої допомоги при ураженні електричним струмом;

– періодичне навчання працівників основним прийомам надання першої допомоги.

Електробезпека на підприємстві ТОВ “Агрополіс” є комплексним питанням, що охоплює як технічні, так і організаційні заходи, спрямовані на запобігання ураженню електричним струмом в умовах різноманітних сільськогосподарських робіт та виробничих процесів. Врахування специфіки кожного виду робіт та кожної зони є ключовим для забезпечення безпеки працівників та збереження майна.

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проект локальної мережі аграрного підприємства ТОВ «Агрополіс». 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 2015 р.) – 500 с.

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

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

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

11. ДСТУ EN 50110-1:2014. Експлуатація електроустановок. Частина 1: Загальні вимоги. URL: https://standards.ua/50110-1. (Дата звернення: 14.05.2025)

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: 14.05.2025)

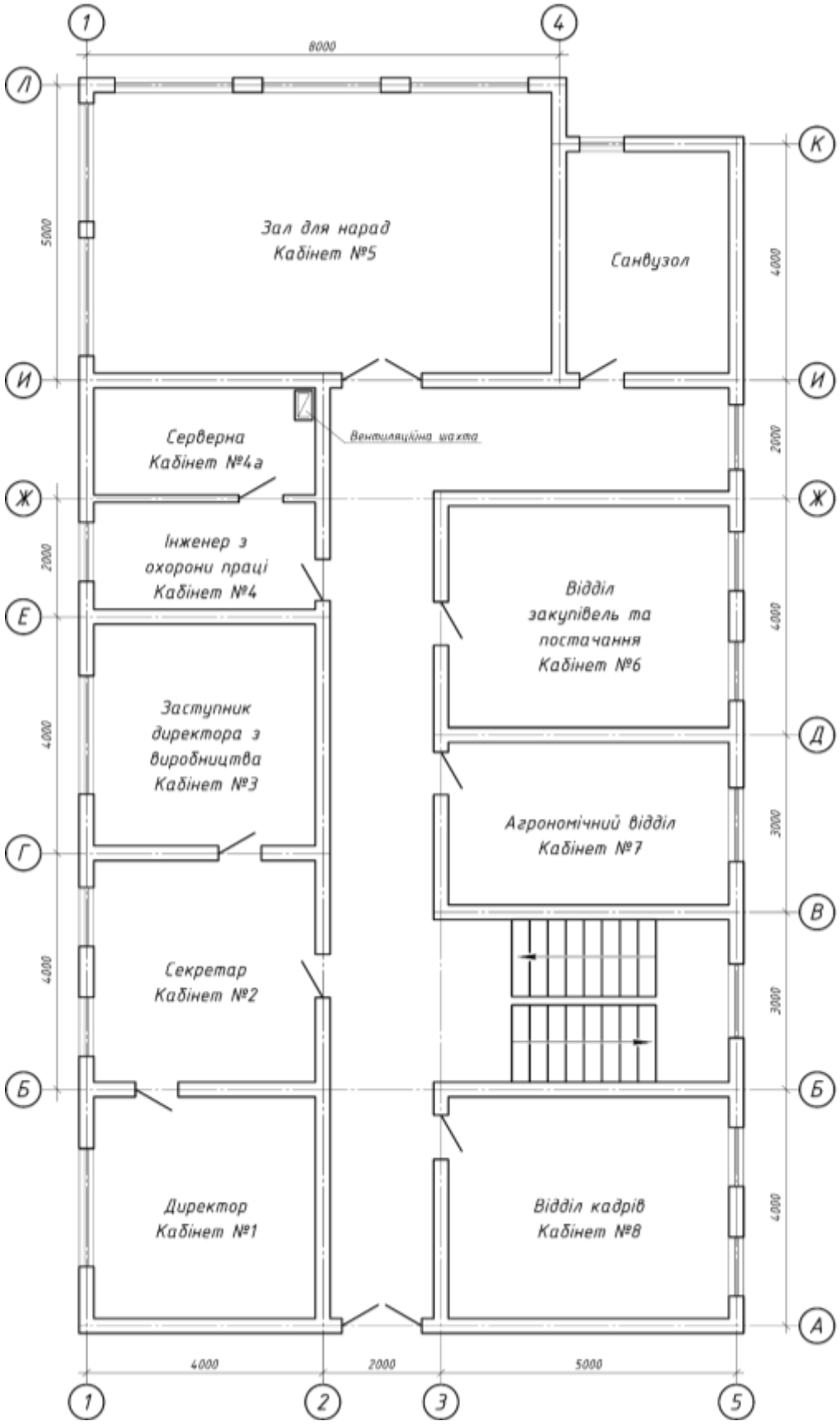
13. App.Diagrams сайт для створення схем URL: https://app.diagrams.net. (Дата звернення: 14.05.2025)

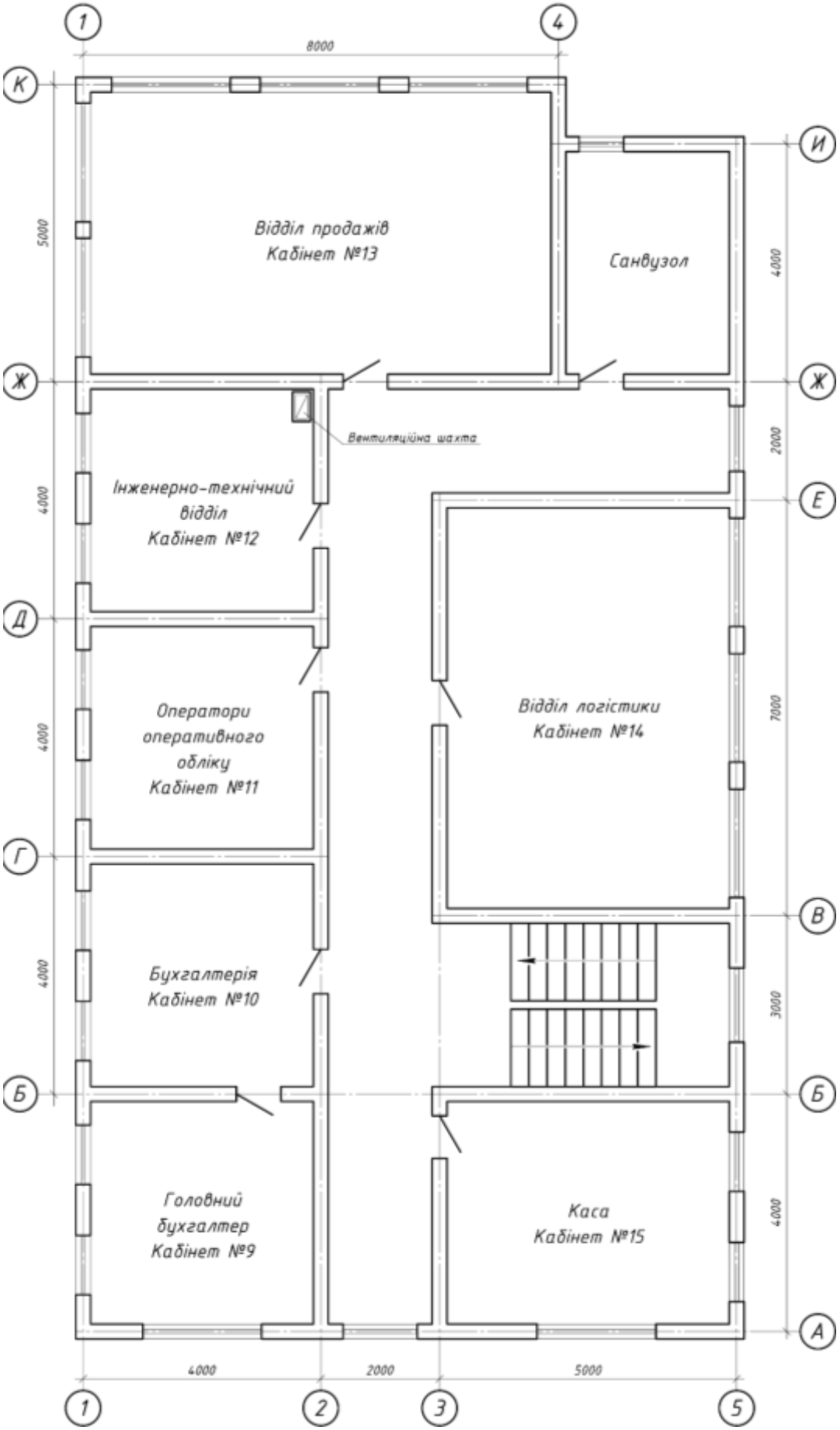
14. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 16.05.2024)

15. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 16.05.2025)

ДОДАТКИ

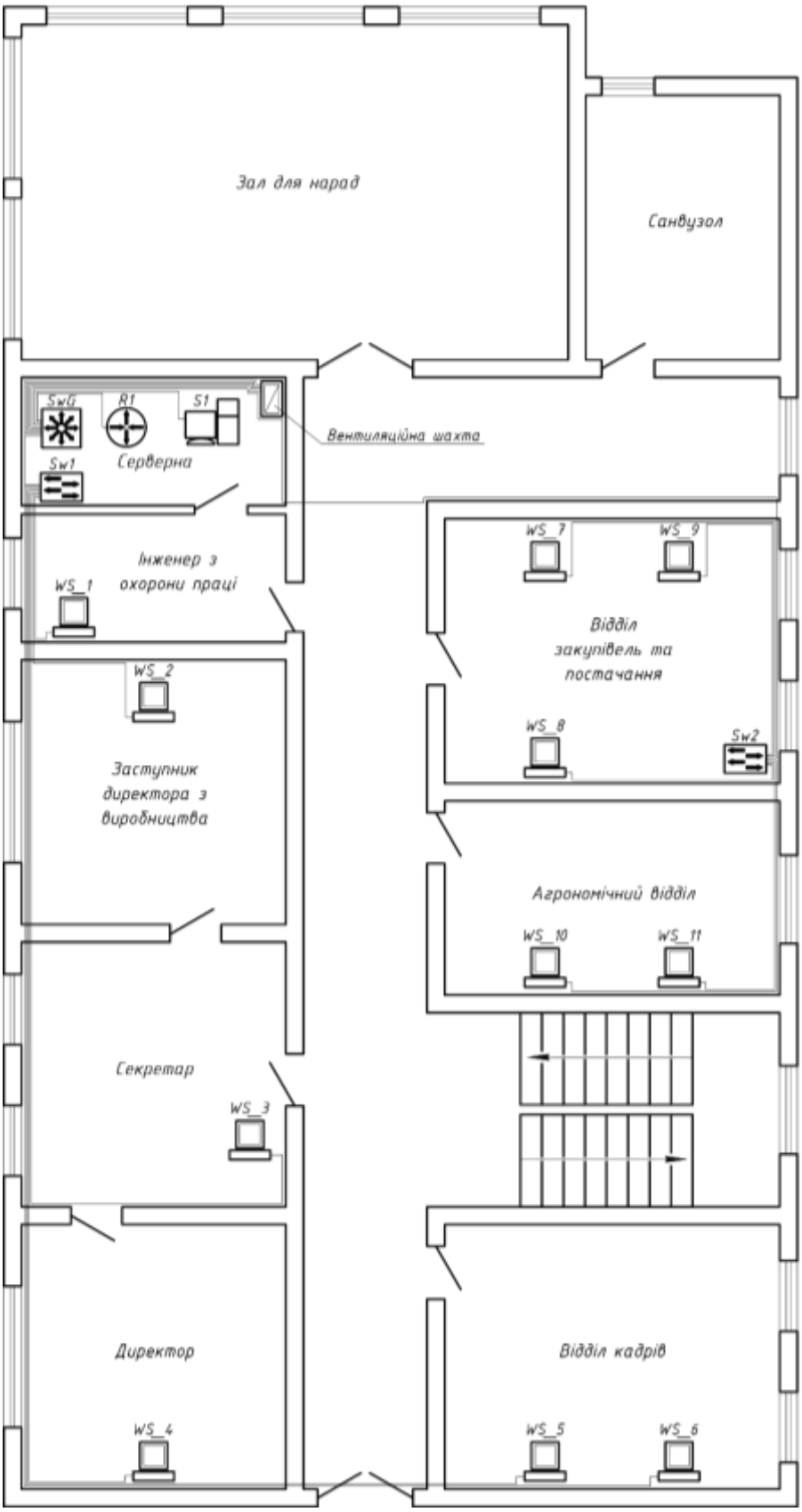
Додаток А. План приміщення будівлі ТОВ «Агрополіс»

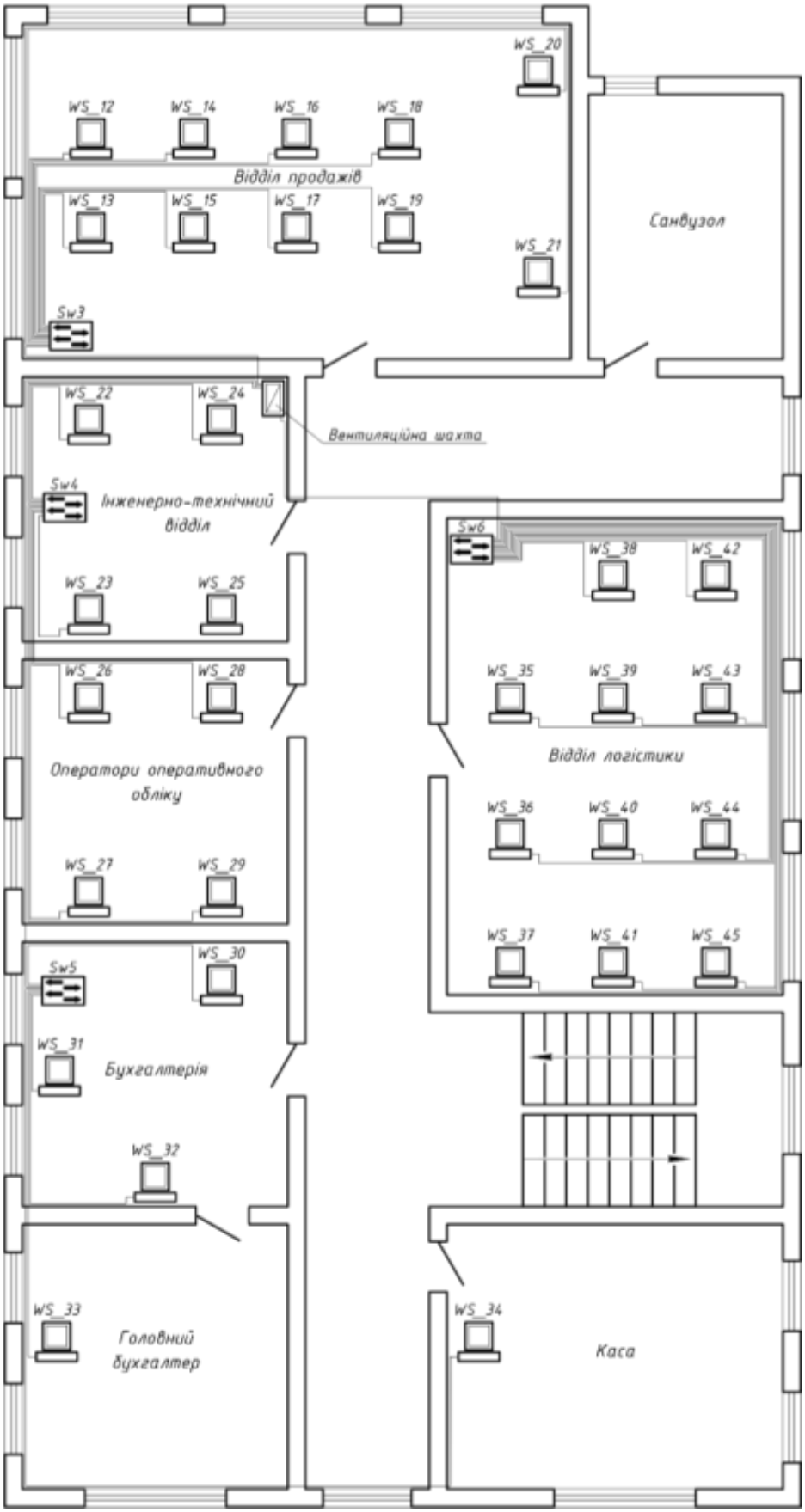




					2025.КРБ.123.602.15.00.00 ПЗ	Арк
Зм.	Арк	№ докум.	Підпис	Дата		108

Додаток Б. План прокладання кабелів СКС мережі ТОВ «Агрополіс»




WS_20
WS_12
WS_14
WS_16
WS_18
Відділ продажів
WS_13
WS_15
WS_17
WS_19
Санвузол
WS_21
Sw3
WS_22
WS_24
Вентиляційна шахта
Sw4
Інженерно-технічний відділ
Sw6
WS_38
WS_42
WS_23
WS_25
WS_35
WS_39
WS_43
WS_26
WS_28
Відділ логістики
Оператори оперативного обліку
WS_36
WS_40
WS_44
WS_27
WS_29
WS_37
WS_41
WS_45
Sw5
WS_30
WS_31
Бухгалтерія
WS_32
WS_33
Головний бухгалтер
WS_34
Каса