

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

## ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра

на тему: Розробка проєкту комп'ютерної мережі ТОВ «АгроСерв»

Виконав: студент VI курсу, групи КІБ-602

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва, спеціальності)

Павло КАПІТАН

(ім'я та прізвище)

Керівник

ВАСИЛЬ ЯЦИШИН

(ім'я та прізвище)

Рецензент

(ім'я та прізвище)

Тернопіль – 2024

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

Відділення телекомунікацій та електронних систем  
Циклова комісія комп'ютерної інженерії  
Освітній ступінь бакалавр  
Освітньо-професійна програма: Комп'ютерна інженерія  
Спеціальність: 123 Комп'ютерна інженерія  
Галузь знань: 12 Інформаційні технології

**ЗАТВЕРДЖУЮ**

Голова циклової комісії  
комп'ютерної інженерії

\_\_\_\_\_ Андрій ЮЗЬКІВ

“08” травня 2024 року

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

\_\_\_\_\_ Капітану Павлу Васильовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проєкту комп'ютерної мережі ТОВ  
“АгроСерв”

керівник роботи Яцишин Василь Володимирович  
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 07.05.2024 р №4/9-224.

2. Строк подання студентом роботи: 21 червня 2024 року.

3. Вихідні дані до роботи: плани приміщення, завдання на проектування, дані на мережеве обладнання і сервер.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділю. Охорона праці техніки безпеки та екологічні вимоги.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

- схема структурна головної сторінки сайту;
- схема структурна компонент фронтенду сайту;
- схема структурна взаємодії ;
- блок схема ;
- 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	25.06	

7. Дата видачі завдання: 08 травня 2024 року

Студент

\_\_\_\_\_ ( підпис )

Керівник роботи

\_\_\_\_\_ ( підпис )

Павло КАПТАН  
(ім'я та прізвище)

Василь ЯЦИШИН  
(ім'я та прізвище)



## ЗМІСТ

Перелік термінів і скорочень

Вступ

1	Загальний розділ .....	6
1.1	Технічне завдання.....	6
1.1.1	Найменування та область застосування.....	6
1.1.2	Призначення розробки.....	6
1.1.3	Вимоги до апаратного та програмного забезпечення.....	7
1.1.4	Вимоги до документації.....	8
1.1.5	Техніко-економічні показники .....	8
1.1.6	Стадії та етапи розробки.....	9
1.1.7	Порядок контролю та прийому .....	9
1.2	Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі.....	10
2	Розробка технічного та робочого проекту.....	12
2.1	Опис та обґрунтування вибору логічного типу мережі.....	12
2.2	Розробка схеми фізичного розташування кабелів та вузлів.....	14
2.3	Обґрунтування вибору комунікаційного обладнання.....	14
2.4	Особливості монтажу мережі.....	24
2.5	Обґрунтування вибору програмного забезпечення.....	25
2.6	Обґрунтування вибору засобів захисту мережі.....	26
2.7	Тестування та налагодження мережі.....	26
3	Спеціальний розділ.....	28
3.1	Інструкції з налаштування програмного забезпечення серверів.....	28
3.1.1	Інструкції з налаштування проксі-сервера.....	28
3.1.2	Інструкції з налаштування локального сховища даних.....	32

					<i>2024.КРБ.123.602.9.00.00 ПЗ</i>			
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>Літ.</i>	<i>Арк.</i>	<i>Аркушів</i>
<i>Розробив</i>		<i>Л.КАПІТАН</i>			<i>Розробка проекту комп'ютерної мережі ТОВ «АгроСерв»</i>		3	69
<i>Перевірів</i>		<i>В.ЯЦІШИН</i>						
<i>Н. Контр.</i>					<i>Пояснювальна записка</i>	<b>ВСП ТФК ТНТУ</b>		
<i>Затв.</i>						<b>КІБ-602</b>		



## АНОТАЦІЯ

Капітан П.В. Розробка проєкту комп'ютерної мережі ТОВ «АгроСерв»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2024. 69с.

Кваліфікаційна робота в галузі розробки проєкту комп'ютерної мережі. Після огляду та аналізу сучасних стандартів побудови мереж вибрано логічну та фізичну топологію мережі, активне та пасивне мережеве обладнання, сервери та програмне забезпечення.

Розроблено адресацію вузлів, поділ на vlan, вибрано пасивне та активне обладнання. Огрунтовано вибір ОС, засобів тестування та захисту мережі. Описано процедури інсталяції на налаштування мережевого обладнання та серверів. Також здійснено моделювання роботи мережі.

Ключові слова: локальна комп'ютерна мережа, віртуальна мережа, сервер, комутатор.

## ANNOTATION

Kapitan Pavlo. Computer Network Project Development of «AgroServ» company: qualification work for obtaining a bachelor's degree, specialty 123 Computer Engineering. Ternopil: Separate Structural Subdivision "Ternopil Professional College of Ivan Puluj National Technical University", 2024. 69p.

Qualification work in the field of computer network design. After reviewing and analyzing modern networking standards, the logical and physical network topology, active and passive network equipment, servers, and software are selected.

The addressing of nodes, division into vlan, and selection of passive and active equipment are developed. The choice of OS, network testing and security tools is justified. Installation procedures for configuring network equipment and servers are described. Network operation is also modeled.

Keywords: Local Area Network, Virtual Network, Server, Switch. \

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		3

## ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

NAT (Network Address Translation) – мережева трансляція адрес;

802.3ad (Link Aggregation) – технологія об'єднання каналів зв'язку;

802.3ae - 10 GbE;

DHCP (Dynamic Host Configuration Protocol) - протокол динамічного конфігурування стеку протоколів TCP/IP робочих станцій.

DNS (Domain Name System) - сервер доменних імен.

DNS (Domain Name System) - сервер доменних імен;

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

IEEE 802.3ab - 1000BASE-T Gigabit Ethernet;

OSI (Open System Interface) – модель з'єднання відкритих систем;

Server Message Block (SMB) — протокол прикладного рівня (в моделі OSI), зазвичай використовується для надання розділеного доступу до файлів, принтерів, послідовних портів передачі даних, та іншої взаємодії між вузлами в комп'ютерній мережі.

SNMP (Simple Network Management Protocol) – протокол керування мережею.

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

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара;

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара.

ЛМ – локальна мережа.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		4



## ВСТУП

Основна задача комп'ютера – обробка даних, їх обмін через комп'ютерну мережу. Для обміну даними між персональним комп'ютерами можна використовувати різні засоби, найбільш ефективним є локальна провідна або безпроводна мережа. Саме такий вид комунікації дозволить підвищити продуктивність праці, організувати виробничий процес.

Основною метою кваліфікаційної роботи є розробка комп'ютерної мережі для ТОВ «АгроСерв». Мережа будуватиметься з використанням стандартів IEEE 802.3ab Gigabit Ethernet, IEEE 802.1Q, Static Routing, IEEE 802.3p, IEEE 802.11ac На основі аналізу технічного завдання та аналітичного огляду існуючих рішень, необхідно вибрати логічну та фізичну топологію для мережі, активне та пасивне обладнання, розробити інструкції з інсталяції та налаштування шлюза доступу до мережі Інтернет, активного мережевого обладнання.

Проект розроблюваної мережі буде базуватися на використанні надійного, швидкого мережевого обладнання, яке відповідатиме рівню мережі, що проектується.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		5

# 1 ЗАГАЛЬНИЙ РОЗДІЛ

## 1.1 Технічне завдання

### 1.1.1 Найменування та область застосування

Тема: Розробка проекту локальної комп'ютерної мережі для ТОВ «АгроСерв». Проект локальної мережі передбачає розробку ЛОМ стандарту Gigabit Ethernet, її інсталяцію в умовах даного підприємства, налаштування мережевих служб.

Даний проект буде характеризуватися достатньою масштабованістю, наявністю необхідних комунікаційних засобів притаманних сучасному підприємству. Проект може бути використаний й для підприємства з кількістю ПК до 100.

### 1.1.2 Призначення розробки

Розробка призначена для :

1. Забезпечення доступу до мережі Інтернет всім ПК.
2. Використання мережевих ресурсів (як локальних так і глобальних).
3. Захист локальної мережі від несанкціонованого доступу.
4. Об'єднати всі робочі станції в локальну мережу.
5. Збереження вкладених інвестицій при розширенні або модернізації мережі.

Модернізація передбачає використання більш швидкісного обладнання для ядра мережі та оптимізація пропускної здатності мережі шляхом використання технологій керування пропускною здатністю окремих потоків мережевого трафіку.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		6

### 1.1.3 Вимоги до апаратного та програмного забезпечення

Для побудови локальної мережі ТОВ «АгроСерв» необхідно відповідне апаратне та програмне забезпечення. В даному підрозділі кваліфікаційної роботи сформуємо основні вимоги до апаратного забезпечення ЛМ.

Комутатор робочих груп вибирається з підтримкою наступних стандартів:

1. Базові функції 2-го рівня моделі OSI властиві комутаторам.
2. IEEE 802.3 10Base-T.
3. IEEE 802.3u 100Base-TX Fast Ethernet.
4. IEEE 802.3ab 1000Base-T Gigabit Ethernet.
5. Автоузгодження NWay.

Головний комутатор вибирається з підтримкою наступних стандартів:

1. Базові функції 3-го рівня моделі OSI властиві комутаторам.
2. IEEE 802.3 10Base-T.
3. IEEE 802.3u 100Base-TX Fast Ethernet.
4. IEEE 802.3ab 1000Base-T Gigabit Ethernet.
5. Автоузгодження NWay.

Апаратна частина для сервера доступу до мережі Інтернет вибирається з розрахунком на подальше збільшення кількості користувачів, яких він буде обслуговувати. Для файлового сервера одним з основних критеріїв буде швидкодія дискової підсистеми та наявність надійного і відмовостійкого апаратного RAID-масиву.

До програмного забезпечення локальної мережі відносять:

1. ОС сервера доступу до мережі Інтернет. Міжмережевий екран на базі ОС Linux CentOS повинен володіти функціями фільтрації трафіку на 3 та 4 рівнях моделі OSI. Підтримувати функції NAT та інших мережевих сервісів.
2. ОС файлового сервера, яка вибирається з підтримкою наступних протоколів: FTP, SAMBA/CIFS.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		7

3. ОС робочих станцій. Програмне забезпечення робочих станцій повинне підтримувати стек TCP/IP при роботі в локальній та глобальній мережах.

#### **1.1.4 Вимоги до документації**

Документування комп'ютерної мережі є важливим етапом адже сама документація буде потрібна в процесі її експлуатації. Під час проектування локальної мережі повинна бути створена наступна документація: фізична топологія локальної мережі, логічна топологія локальної мережі, схема IP-адресації.

Для збору додаткових даних про вузли мережі буде використано спеціалізоване мережеве програмне забезпечення.

#### **1.1.5 Техніко-економічні показники**

Наведемо основні техніко-економічні показники проекту локальної мережі ТОВ «АгроСерв».

Техніко-економічні показники:

- Технологія побудови локальної мережі - 1000Base-TX;
- Фізична топологія – Гібридна;
- Логічна організація - поділ ширококомовного домену на підмережі, що відповідають логічній структурі організації.
- Модель взаємодії між вузлами - Клієнт-сервер;
- Файловий сервер – Vsftpd;
- ОС сервера - Linux CentOS 8;
- Протокол обміну даними з файловим сервером – FTP;
- Доступ до мережі Інтернет засобами проксі-сервера – Squid;
- Ціна - до 350 тис. грн.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		8

– Собівартість – до 250 тис. грн.

### 1.1.6 Стадії та етапи розробки

Етапи проектування локальної мережі ТОВ «АгроСерв»:

1. Планування етапів розробки мережі враховуючи побажання замовника в особі ТОВ «АгроСерв».
2. Розробка логічної топології мережі.
3. Розробка фізичної топології мережі.
4. Вибір активного комутаційного обладнання.
5. Монтаж мережі.
6. Підключення комутаційного обладнання.
7. Конфігурування шлюза.
8. Конфігурування локального сховища даних на базі альтернативного програмного забезпечення.
9. Конфігурування комутаторів.
10. Конфігурування безпроводного маршрутизатора.
11. Тестування мережі.
12. Розробка технічної документації.

### 1.1.7 Порядок контролю та прийому

Локальна комп'ютерна мережа має відповідні технічні показники від яких залежить її робота:

1. Реальна швидкість мережі.
2. Швидкість передачі великих та малих за розміром пакетів між вузлами мережі.
3. Кількість втрачених під час передачі чи прийому пакетів.

									Арк.
									9
Зм.	Арк.	№ докум.	Підпис	Дата	2024.КРБ.123.602.9.00.00 ПЗ				

4. Статистика роботи протоколів каналного, мережевого та транспортного рівнів.

Контроль вище наведених показників буде проводитись уповноваженими на це особами, представниками ТОВ «АгроСерв» з використанням відповідних апаратних (кабельний тестер сертифікований для стандарту Gigabit Ethernet на мідній витій парі) та спеціалізованих програмних засобів.

## **1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі**

Товариство «АгроСерв» займається здачею в оренду сільсько-господарської техніки та транспортними перевезеннями як на території України так і за кордоном. До його складу входять такі підрозділи:

- логісти;
- заступники;
- відділ роботи з клієнтами;
- бухгалтерія;
- відділ контролю за перевезеннями;
- відділ міжнародних зв'язків;
- відділ кадрів;
- відділ експлуатації транспортних засобів;
- відділ маркетингу;
- відділ ТБ та ОП;
- ІТ-відділ;
- відділ розрахунків;
- прийомна;
- директор;
- зал засідань.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		10

Замовник висунув перед початком проектування такі загальні вимоги: необхідна швидкість передачі в проєктованій мережі 1 Гбіт/с., для бездротового сегмента мережі – 1 Гбіт/с. При проектуванні мережі необхідно враховувати можливість підключення нових користувачів, тому в запланованій мережі та мережевому обладнанні необхідно закласти запас на певну пропускну здатність.

При налаштуванні серверного програмного забезпечення необхідно враховувати фактори безпеки та наявність розширених функції, які дуже важливі з огляду на поточний стан речей в галузі. Для локальних проєктів краще використовувати безкоштовне програмне забезпечення, що дозволить заощадити багато грошей на весь проєкт.

									Арк.
									11
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	2024.КРБ.123.602.9.00.00 ПЗ				

## 2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

### 2.1 Опис та обґрунтування вибору логічного типу мережі

Основне призначення будь-якої комп'ютерної мережі, в тому числі локальної - надання інформаційних та обчислювальних ресурсів підключеним до неї хостам а відповідно й користувачам. З цієї точки зору локальну комп'ютерну мережу можна розглядати як сукупність серверів, мережевого обладнання, робочих станцій та засобів фізичного зв'язку між ними. Сервер - це переважно досить потужний комп'ютер, підключений до мережі, і забезпечує її користувачів певними послугами чи сервісами. Ці послуги часто називають спільними мережевими ресурсами, особливо якщо йдеться про дискову систему чи оперативну пам'ять сервера. Крім цього сервери можуть здійснювати збереження даних, управління потоками даних і базами даних, віддалену обробку і друк даних та інші функції. Отже сервер можна розглядати як джерело ресурсів мережі [1].

Робоча станція - це ПК, підключений до мережі, через який користувач отримує доступ до її ресурсів. Робоча станція може функціонувати як у мережевому (спільному), так і в локальному режимі. На ній встановлюється власна ОС або використовується мережева ОС з віддаленим завантаженням. Також вона забезпечує рядового користувача певним інструментальним набором засобів для розв'язання прикладних задач. Робочі станції призначені для інтерактивної взаємодії користувачів [1].

Найчастіше в локальній комп'ютерній мережі використовують файловий сервер. Він керує ресурсами мережі, забезпечуючи доступ до них з інших комп'ютерів мережі - робочих станцій. Основним ресурсом, що надається користувачам у спільне користування, є дискова пам'ять файлового сервера. Розділяються й інші ресурси файлового сервера, наприклад підключений до нього принтер. Тому як робочі станції можна

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		12



використовувати відносно дешеві комп'ютери, що не мають власного під'єднання до принтера й іноді навіть жорсткого диска [2].

Файл-сервер - це переважно комп'ютер з великою ємністю дискової та оперативної пам'яті, або мережеве сховище даних (NAS), який виконаний як окремий пристрій. Незалежно від цього високі вимоги ставлять до швидкісних характеристик та надійності (надлишковості) дискової системи.

В одноранговій комп'ютерній мережі немає єдиного центру керування взаємодією робочих станцій. Переваги однорангової комп'ютерної мережі – досить низька вартість і прийнятний рівень надійності. Недоліками її є [1]:

- Пряма залежність ефективності роботи від кількості станцій;
- Складність нормального керування мережею;
- Проблеми з забезпеченням хорошого захисту даних;
- Труднощі з оновлення і пере інсталяцію програмного забезпечення станцій.

В комп'ютерних мережах з виділеним сервером один із комп'ютерів виконує функції керування мережею, збереження даних, призначених для використання всіма робочими станціями, керування взаємодією між робочими станціями і деякі сервісні функції. Таким чином взаємодія робочих станцій здійснюється через сервер.

Переваги комп'ютерної мережі з виділеним сервером:

- Надійна система захисту інформації;
- Висока швидкодія;
- Відсутність жорстких обмежень на кількість робочих станцій;
- Простота керування та адміністрування порівняно з одноранговими мережами.

- Недоліками такої мережі є:
- Висока вартість через виділення одного комп'ютера під сервер;
- Залежність швидкодії та надійності від сервера;
- Менша гнучкість порівняно з одноранговою мережею.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		13

Крім побудови локальної мережі з використанням технології Gigabit Ethernet, буде використано технологію VLAN згідно стандарту IEEE 802.1Q. Дані про отримані підмережі наведено в таблиці “Логічна адресація в ЛОМ” додатку Б.

В таблиці “Таблиця конфігурування VLAN” додатку Б наведено дані про порти комутаторів для конфігурування VLAN. Ці дані будуть використані у розділі 3 дипломного проекту.

## **2.2 Розробка схеми фізичного розташування кабелів та вузлів**

Локальна мережа ТОВ «АгроСерв» побудована на базі стандарту Gigabit Ethernet з швидкістю передачі 1Гбіт/с, та стандарту IEEE 802.11ac 1Гбіт/с.

Мережа побудована з використанням гібридної (змішаної) фізичної топології, оскільки провідна частина відповідає розширеній зірці, а безпроводна – комірчастій топології. Вибір даної топології обумовлений стандартом провідної частини Gigabit Ethernet. Технологія побудови локальної мережі Gigabit Ethernet (1000Base-T) передбачає використання фізичної топології Зірка та Розширена зірка.

Для проекту мережі буде використано фізичну топологію Гібридна (поєднання фізичної топології Комірчаста та Розширена зірка), оскільки саме вона задовольняє всім вимогам перед даним проектом мережі.

Ядром побудованої локальної мережі буде комутатор 3-го рівня.

## **2.3 Обґрунтування вибору комунікаційного обладнання**

В даному розділі кваліфікаційної роботи буде вибрано відповідне обладнання для проекту локальної мережі.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		14

В таблиці 2.1 наведено порівняльний аналіз технічних параметрів комутаторів рівня 2, які будуть використовуватись для відділів.

Таблиця 2.1 – Порівняльний аналіз технічних показників комутаторів

Виробник/ характеристика	D-Link DGS-1210-20	Cisco SLM2016T-EU	TP-Link TL- SG3216
Швидкість комутації, Гбіт/с	40	36	32
Пропускна здатність, млн. пакетів/с	29,8	26,78	23,8
К-сть портів 10/100/1000	16+4	16+2	16+2
Підтримка VLAN	+	+	+
Об'єм буфера пам'яті	1МБ	1МБ	512КБ
Підтримка функції Port Mirroring	+	+	+
Підтримка технології віртуальних мережі стандарту IEEE 802.1q	+	+	+
Підтримка технології Spanning Tree	+	+	+
Підтримка ведення статистики (кількість переданих та прийнятих пакетів та їх тип)	+	+	+

Для локальної мережі буде використано комутатор 2-го рівня D-Link DGS-1210 на 16 портів [16].

Стандарти та функції портів:

						2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата			15

- IEEE 802.3 10BASE-T Ethernet (мідний кабель на основі витोї пари);
- IEEE 802.3u 100BASE-TX Fast Ethernet (мідний кабель на основі витої пари);
- IEEE 802.3ab 1000BASE-T Gigabit Ethernet (мідний кабель на основі витої пари);
- Автоузгодження ANSI / IEEE 802.3;
- Управління потоком IEEE 802.3x.

Кількість портів:

- 12 портів 10/100/1000 Мбіт/с, 4 комбо-порта 10/100/1000BASE-T/SFP.

Мережеві кабелі:

- UTP категорії. 5, 5e (макс. 100 м);
- EIA/TIA-568 100 Ом STP (макс. 100 м).

Повний/напівдуплекс:

- Повний/напівдуплекс для швидкості 10/100Мбіт/с;
- Повний дуплекс для швидкості Gigabit.

Розширені можливості інтерфейсу:

- Автовизначення MDI/MDI-X для всіх портів на основі витої пари.

Пропускна здатність комутатора:

- 32 Гбіт/с.

Метод комутації:

- Store-and-forward.

Таблиця MAC-адрес:

- 8 Кб записів на пристрій.

Вивчення MAC-адрес:

- До 256 статичних записів MAC-адрес;
- Включення/відключення автовивчення MAC-адрес.

Максимальна швидкість просування пакетів розміром 64 байта:

- 23.8 Mpps.

											Арк.
											16
Зм.	Арк.	№ докум.	Підпис	Дата	2024.КРБ.123.602.9.00.00 ПЗ						

Буфер RAM:

- 512 Кб на пристрій.

На рисунку 2.1 зображено вибраний нами комутатор фірми D-Link.



Рисунок 2.1 - D-Link DGS-1210-20

Робочі станції підключаються безпосередньо до комутатора робочої групи, який в свою чергу підключається до центрального комутатора.

Для робочих груп будуть використовуватись 8-ми портові та 16-ти портові комутатори. Зведена інформація порівняльного аналізу 8-ми портових комутаторів наведена в таблиці 2.2.

Таблиця 2.2 – Порівняльна характеристика 8-ти портових комутаторів

Технічні характеристики/ модель комутатора	D-Link DGS-1100-08	TP-LINK TL-SG2208	Cisco SG200-08
1	2	3	4
Швидкість комутаційної шини, Гб/с	16	16	13,6
Швидкість пересилки пакетів 64 байт, млн./с	11,9	11,9	11,9
К-сть портів 10/100/1000	8	8	8
Підтримка технології віртуальних мережі	+	+	+

стандарту IEEE 802.1q			
-----------------------	--	--	--

Продовження таблиці 2.2

1	2	3	4
Підтримка технології Spanning Tree	+	+	+
Підтримка ведення статистики	+	+	+

Для локальної мережі буде використано комутатор D-Link DGS-1100 [17], який зображено на рисунку 2.2.



Рисунок 2.2 – Комутатор D-Link DGS-1100

В таблиці 2.3 наведено порівняння технічних даних серверів.

Таблиця 2.3 – Порівняння апаратних конфігурацій серверів

Модель / Параметри	Dell PowerEdge T30	HPE ProLiant ML10 Gen9	ARTLINE Business T35 v04
1	2	3	4
Процесор	Intel Xeon Quad-Core E3-1225 v5		
Чіпсет	Intel C236		

Пам'ять	DDR4 16 ГБ 2133 ГГц
ЖМД	2 ТБ SATA-III 7200rpm Enterprise x 2 шт, SSD 1ТБ

Продовження таблиці 2.3

1	2	3	4
Мережева плата	Intel PRO/1000 PT Dual Port Server Adapter		
Дисковий контроллер	HP P420i (RAID-0, RAID-1, RAID-10, RAID-5)		

Для серверів буде вибрано апаратну платформу на базі HPE ProLiant ML10 Gen9 [18], яка зображена на рисунку 2.3.



Рисунок 2.3 - HPE ProLiant ML10 Gen9

Для того, що об'єднати всі вузли локальної мережі буде використано центральний комутатор з функцією маршрутизації трафіку між її вузлами. В таблиці 2.4 приведено порівняння комутаторів з функцією маршрутизації різних фірм виробників.

Таблиця 2.4 – Технічні характеристики комутаторів

Характеристика, назва	Allied Telesyn AT- x600-24Ts	Zyxel XGS- 4526	Cisco C3850- 24W
1	2	3	4
Підтримувані функції	L2, L3	L2, L3	L2, L3
Комутація кадрів/пакетів, Гбіт/с	96	96	88
Кадрів/пакетів в секунду	71,4	71,5	128
К-сть портів 10/100/1000 BASE- TX	24+4	20+4	24+4
Маршрутизація	Статична, динамічна	Статична, динамічна	Статична, динамічна
Віддалене керування	WEB, SSH	WEB	WEB
Підтримка IEEE 802.1Q	Так	Так	Так

Для мережі вибрано комутатор Allied Telesyn AT-x600-24Ts враховуючи співвідношення ціна/відповідність технічним параметрам. Даний комутатор зображено на рисунку 2.4.





Рисунок 2.4 - Allied Telesyn AT-x600-24Ts

В таблиці 2.5 наведено порівняльний аналіз технічних параметрів безпроводний маршрутизаторів.

Таблиця 2.5 – Порівняльна характеристика безпроводних маршрутизаторів

Виробник	D-Link		
1	2		
Марка	DIR-853 AC1300	Archer C7 AC1750	RV260W
Стандарти	802.11n, 802.11g, 802.11b, 802.3		
Швидкість передачі	802.11b: 11 Мбіт/с; 802.11g: 54 Мбіт/с; 802.11n: 300 Мбіт/с; 802.11ac: 1000 Мбіт/с		
Підтримувані частоти	5Ггц, 2.4Ггц		
Протоколи безпеки	64/128-бітний WEP, WPA/WPA2, WPA-PSK/WPA2-PSK		
Підтримувані протоколи	DHCP, PPPoE, PPTP, L2TP, DNS, DHCP, IGMP, RSTP, NAT, PAT, DMZ		
Кількість портів LAN	1	4	4

Розглянемо технічні параметри безпроводного маршрутизатора TP-LINK Archer C7 AC1750, який зображено на рисунку 2.5.

Апаратні характеристики:

- 4 порти LAN 10/100/1000 Мбіт/с;

- 1 порт WAN 10/100/1000 Мбіт/с;
- 2 порти USB 2.0;
- 3 знімні антени (RP-SMA).

Параметри бездротового модуля:

- Стандарти бездротових мереж: IEEE 802.11ac/n/a 5 ГГц; IEEE 802.11b/g/n 2,4 ГГц;
- Діапазон частот (прийом і передача): 2,4 ГГц та 5 ГГц;
- Швидкість передачі 5 ГГц: До 1300 Мбіт/с; 2,4 ГГц: До 450 Мбіт/с;
- Функції бездротового режиму: Включення/виключення бездротового мовлення, міст WDS, WMM, статистика бездротового;
- Захист бездротової мережі: 64/128-бітній WEP, WPA/WPA2, WPA-PSK/WPA2-PSK.

На рисунку 2.5 наведено зовнішній вигляд безпроводного маршрутизатора TP-LINK Archer C7 AC1750 [15].



Рисунок 2.5 – Маршрутизатор TP-LINK Archer C7 AC1750

Особливості даного безпроводного маршрутизатора:

- Підтримка сучасного стандарту бездротового зв'язку 802.11ac
- Пропускна здатність до 1,75 Гбіт/с: до 1300 Мбіт/с на 5 ГГц і до 450 Мбіт/с на 2,4 ГГц

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		22

- 2 порти USB, що забезпечить спільний доступу до принтерів, файлів і іншого контенту по локальній мережі або віддалено через FTP-сервер
- Можливість створення гостьової мережі

Для стабілізації енергоживлення вузлів мережі а також підтримки електроживленням протягом де-кількох хвилин після пропаданя напруги буде використано ДБЖ KIN-2200AP-RM, який зображено на рисунку 2.6.



Рисунок 2.6 – ББЖ KIN-2200AP-RM

Додатково буде використано таке пасивне мережеве обладнання:

- Мережеві розетки;
- Кабель вита пара;
- Патч-панель;
- Кабельні тримачі;
- Комутаційна шафа.

В таблиці 2.6 наведено перелік всього обладнання, необхідного для впровадження локальної мережі.

Таблиця 2.6 – Список необхідного обладнання

№ п/п	Найменування матеріальних ресурсів	Одиниці виміру	К-сть	Ціна, грн.	Сума, грн.
-------	------------------------------------	----------------	-------	------------	------------

1	2	3	4	5	6
Пасивне мережеве обладнання					
1	Комутаційна шафа 24U	шт	1	16000	16000
2	Патчпанель 24 порти	шт	1	3200	3200
3	Мережева розетка	шт	40	100	4000

Продовження таблиці 2.6

1	2	3	4	5	6
4	Короб	м	140	57	7980
5	Кабель UTP кат. 6	м	610	10	6100
6	Патчкорд	шт	70	10	700
7	ББЖ Powercom KIN-2200AP-RM	шт	1	15000	15000
8	Кабельні тримачі	шт	2	200	400

Активне мережеве обладнання

9	Комутатор D-Link D-Link DGS-1210-16	шт	3	3900	11700
10	Комутатор рівня групи D-Link DGS-1100-08	шт	3	3000	9000
11	Безпроводний маршрутизатор TP-LINK Archer C7 AC1750	шт	1	1400	1400
12	Сервер HPE ProLiant ML10 Gen9	шт	1	33010	33010
13	Allied Telesyn AT-x600-24Ts	шт	1	14300	14300

Отже, загальна сума коштів, які потрібно витратити на придбання обладнання буде становити 122790 грн.

## 2.4 Особливості монтажу мережі

										Арк.
										24
Зм.	Арк.	№ докум.	Підпис	Дата	2024.КРБ.123.602.9.00.00 ПЗ					

Кабельна інфраструктура локальної мережі буде побудована на основі неекранованої виті пари категорії 6 [15]. Перш ніж починати проектування а тим більше монтаж локальної мережі, необхідно чітко розуміти, де і що буде знаходитися, які компоненти СКС використовуємо і як їх інсталиювати.

Наприклад при монтажі комутаційної шафи варто встановити одну або пару патч-панелей. Тоді для підключення обладнання необхідно буде просто завести кабелі до відповідних портів. Центральний комутаційний вузол можна розміщувати в будь-якому зручному і відповідному для цього місці з дотриманням відповідних вимог щодо СКС та вимог інформаційної безпеки (у нашому випадку він буде розміщено в ІТ-відділі).

Необхідно ретельно і з врахуванням вимог вибрати місце, де буде знаходитися комутатор. При цьому відстань від будь-якого з комутаторів до кінцевого пристрою має становити не більше ніж в 90 метрах. Збільшення відстані призведе до затухання сигналу, появу перешкод та інших завад на лінії.

Комутатори робочих груп закріплюють переважно на стіні близько до електричної розетки. При цьому не рекомендується ховати його за шафою або під столом, адже доступ до нього може знадобитися в будь-який час, також це суперечить вимогам пожежної безпеки. Після того як визначилися з його місцем розташування, необхідно проаналізувати шляхи прокладки кабелю від комутатора до кожного хоста. Найбільш стандартний метод монтажу - уздовж стін, а для укладки кабелів буде використано спеціальні коробки. В коридорах та частині приміщень де присутня підвісна або натяжна стеля кабелі зручного монтувати не по стінах а кріпити до стелі. При цьому кабелі не повинні перетинати вентиляційні та інші шахти, проходити близько до електричних ліній чи труб інших комунікацій.

## 2.5 Обґрунтування вибору програмного забезпечення

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		25

Для функціонування серверного апаратного забезпечення необхідним є відповідне програмне забезпечення (операційна система, сервіси, служби та ін). Серверне програмне забезпечення може реалізовувати специфічні функції, які неможливо або досить складно реалізувати засобами клієнтських ОС, наприклад Windows.

Для шлюза доступу до мережі Інтернет використано ОС CentOS 8 [12]. Саме вона характеризується реалізацією найшвидшого стеку протоколів TCP/IP, досить легко конфігурується, є надійною і стабільною..

Для робочих станцій використано ОС Ubuntu Linux 20.04. Дана ОС є безкоштовною, стабільною та «легкою».

## 2.6 Обґрунтування вибору засобів захисту мережі

Захист локальної комп'ютерної мережі є складним, багатоетапним і багатоступінчастий процес. Він включає:

1. Планове періодичне оновлення всіх ОС та прикладного програмного забезпечення робочих станцій та сервера. У нашому випадку ОС робочих станцій є ліцензійними, тому можливість автономного поновлення у них присутня. Серверна ОС Linux CentOS 8 також підтримує можливість віддаленого автоматичного поновлення.

2. Наявність програм-антивірусів на клієнтських ПК.

3. Централізований захист локальної мережі від небажаного трафіку і атак ззовні. Для таких задач використовується файрвол iptables.

4. Використання комутатора з функцією Port Mirroring дозволить «прослуховувати» і аналізувати мережевий трафік.

## 2.7 Тестування та налагодження мережі

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		26

Тестування є одним з найважливіших етапів проектування комп'ютерної мережі. Передбачити тестування апаратних і програмних компонентів. Спочатку необхідно перевірити, чи відповідає Gigabit SCS локальної мережі стандарту передачі даних 1 Гбіт/с. Тестування SCS включатиме перевірку цілісності всіх сегментів кабелю та їх технічної здатності передавати дані на швидкостях Gigabit Ethernet.

Наступним кроком є підключення мережевого пристрою та перевірка його продуктивності. Центральний комутатор буде виконувати роль маршрутизатора, тому вам також потрібно перевірити наявність усіх підмереж.

Останнім кроком тестування є перевірка роботи сервера доступу до Інтернету та програмного забезпечення файлового сервера.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		27

## 3 СПЕЦІАЛЬНИЙ РОЗДІЛ

### 3.1 Інструкції з налаштування програмного забезпечення серверів

#### 3.1.1 Інструкції з налаштування проксі-сервера

SQUID може бути встановлений з вихідних текстів або у вигляді DEB-пакета. Вихідні коди можна викачати з офіційного сайту за адресою <ftp://ftp.squid.org/>. Для розпакування архіву, потрібно виконати наступні команди:

```
cd /usr/src/  
gunzip squid-4.0.STABLE-src.tar.gz  
tar -xvf squid-4.0.STABLE-src.tar.gz  
cd squid
```

Тепер перейдемо безпосередньо до установки:

```
./configure --prefix=/usr/local/squid  
make all  
make install
```

Squid буде встановлений у каталог, заданий ключем `prefix` - `/usr/local/squid`.

Squid використовує файл конфігурації `squid.conf`. Звичайно він розташовується в каталозі `/etc/squid` (або `/usr/local/squid/etc` - більш ранні версії). Відкриваємо його в будь-якому текстовому редакторі, наприклад `joe /usr/local/squid/etc/squid.conf`.

Вказуємо проксі провайдера:

```
cache_peer проху.ml.net.ua
```

У нашому випадку `проху.ml.net.ua` стає нашим <сусідом> (`neighbour, peer`)

Встановимо обсяг пам'яті, доступний squid, і каталог для кешу:

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		28



```
cache_mem 65536
```

```
cache_dir /usr/local/squid/cache 1024 16 256
```

Вкажемо хости, з яких дозволений доступ до проксі:

```
acl allowed_hosts src 192.168.100.0/255.255.255.0
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

Заборонимо метод CONNECT для всіх портів, крім зазначених в асі SSL\_ports:

```
http_access deny CONNECT !SSL_ports
```

Заборонимо доступ усім, крім тих, кому можна:

```
http_access allow localhost
```

```
http_access allow allowed_hosts
```

```
http_access allow SSL_ports http_access deny all
```

Пропишемо користувачів, яким дозволено користуватися squid (den, admin, developer):

```
ident_lookup on
```

```
acl allowed_users user den admin developer
```

```
http_access allow allowed_users
```

```
http_access deny all
```

Нижче наведений приклад заборони доступу до будь-якого URL, що відповідає шаблону games і дозвіл доступу до нього всім іншим:

```
acl GaMS url_regex games
```

```
http_access deny GaMS
```

```
http_access allow all
```

Тепер, коли здійснено базове налаштування SQUID, його потрібно запустити:

```
/usr/local/squid/bin/squid -z
```

Параметр -z потрібний для створення (обнулення) каталогу, що містить кеш. Звичайно параметр -z потрібний тільки при першому запуску. Параметри проксі-сервера squid наведено в таблиці 3.1.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		29

Таблиця 3.1 – Параметри проксі-сервера squid

Параметр	Опис
1	2
-a	порт для вхідних HTTP-запитів
-d	налагодження (на stderr)
-f	ім'я файлу конфігурації
-h	help
-k reconfigure	посилка сигналу HUP
-k shutdown	завершення роботи проксі
-k kill	завершення без закриття журналів
-u	порт для вхідних ICP запитів
-v	version
-D	не робити DNS-тест при запуску
-N	не ставати демоном (фоновим процесом)
-Y	більш швидке відновлення після збоїв

Розглянемо формат файлу squid.conf. Параметри мережі:

http\_port 3128

Порт для запитів клієнтів:

icp\_port 3130

Якщо сусідів (peer) нема, то потрібно встановити:

icp\_port 0

htcp\_port 4827

Керування кешем:

cache\_swap\_high число - при досягненні цього рівня заповнення кешу (у процентному співвідношенні) починається прискорений процес видалення старих об'єктів.

cache\_swap\_low 90 - процес видалення припиняється при досягненні цього рівня.

maximum\_object\_size 4096 KB - максимальний розмір кешованого об'єкта.

minimum\_object\_size 0 KB - файли меншого розміру не зберігаються.

Протоколювання:

cache\_access\_log /usr/local/squid/logs/access.log - протоколюється кожний запит до SQUID.

cache\_log /usr/local/squid/logs/cache.log - журнал запусків процесів.

cache\_store\_log /usr/local/squid/logs/store.log - журнал запису об'єктів у кеш.

Якщо якийсь журнал не потрібний, потрібно встановити параметр none замість файлу.

Списки ACL:

ACL - визначення списку доступу. Визначається як: acl ім'я тип рядок.

Тип - це тип об'єкта, а рядок - регулярний вираз. Можна використати список acl ім'я тип <ім'я файлу> (по одному параметрі в рядку). Типи параметрів для складання списків доступу наведено в таблиці 3.2.

Таблиця 3.2 – Типи параметрів для списків доступу проксі-сервера

src ip-address/netmask	IP адреса клієнтів
src addr1-addr2/netmask	діапазон адрес
dst ip-address/netmask	URL хостов
time [day-abbrevs] [h1:m1-h2:m2]	Час, де день це одна буква з SMTWHFA
port	список портів
port port1-port2	діапазон портів
proto	протокол - HTTP/FTP

Параметри доступу:

http\_access allow|deny aclname - дозволяти доступ до проксі по http.

icp\_access allow|deny aclname - дозволяти доступ до проксі по ICP.

Параметри адміністрування:

cache\_mgr email - поштова адреса, на який буде посланий лист, якщо squid перестане функціонувати.

cache\_effective\_user nobody - при запуску squid від імені root змінити UID на зазначений.

visible\_hostname ім'я-хоста - це ім'я буде згадуватися в повідомленнях про помилки.

hostname\_aliases ім'я - список синонімів для імені хоста

### 3.1.2 Інструкції з налаштування локального сховища даних

Файлова служба в локальній мережі буде побудована на протоколі FTP, який є одним із найвідоміших.

File Transfer Protocol - протокол передачі файлів, протокол високого рівня, а саме, рівня додатків. Використовується службою FTP для передачі файлів. Перший стандарт - RFC114 (File Transfer Protocol АК Bhushan Apr-10-1971). Остання версія - RFC959 (File Transfer Protocol J. Postel, JK Reynolds Oct-01-1985) [7].

FTP відрізняється від інших протоколів такою особливістю, що він використовує два TCP-з'єднання для передачі файлу. Перше - керуюче з'єднання – призначене для посилки команд серверу й одержання відповідей від нього. Відповідно з'єднання даних – використовується власне для передачі користувацьких файлів. Для каналу керування можна використати протокол Telnet.

Цікаво, що в старих версіях для передачі даних використовувався тільки 20-й порт (активний режим), а в сучасних версіях FTP-серверів відповідний для каналу порт даних може призначатися самим сервером з списку вільних ( $N > 1024$ ) портів (пасивний режим).

									Арк.
									32
Зм.	Арк.	№ докум.	Підпис	Дата					

Протокол FTP визначає запит-відповідь спосіб взаємодії між програмою-клієнтом і програмою-сервером. Робота FTP на призначеному для користувача рівні містить кілька етапів:

- Ідентифікація (логуватись);
- Вибір каталогу;
- Визначення режиму обміну (по блоках, потоковий, ascii або двійковий);
- Виконання команд обміну (get, mget, dir, mdel, mput або put);
- Завершення процедури (quit або close).

Розглянемо різницю роботи пасивного режиму і активного.

Отже активний режим, при цьому дії сервера і клієнта: клієнт ініціює зв'язок і надсилає запит на 21 порт сервера з порту N ( $N > 1024$ ). Сервер посилає відповідь на порт N ( $N > 1024$ ). Далі сервер встановлює зв'язок для передачі даних по порту 20 на порт клієнта N + .

Клієнт ініціює лінк і надсилає запит (повідомляє, що треба працювати в пасивному режимі) на 21 порт сервера з порту N ( $N > 1024$ ). Сервер надає відповідь, у якій повідомляє номер порту для каналу даних P ( $P > 1024$ ) на порт N ( $N > 1024$ ) клієнта. В подальшому клієнт встановлює зв'язок для передачі даних по порту N + 1 на відповідний порт сервера P ( $P > 1024$ ).

Активний FTP вигідний для FTP-сервера, але не дуже ефективний для клієнта. FTP сервер намагається з'єднатися з випадковими високими (за номером) портами на клієнті. В більшості випадків воно буде заблоковано фаєрволом на стороні клієнта.

Пасивний FTP вигідний для клієнта, але не надто ефективний для FTP-сервера. Клієнт буде робити обидва з'єднання до сервера, але низьким номером порту і відповідно пріоритетом.

Даний сервіс налаштовується за допомогою файлу vsftpd.conf - основний конфігураційний файл сервера vsftpd. Приклад файлу, використаного нами:

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		33

listen=YES  
listen\_address=192.168.1.0/24  
pam\_service\_name=vsftpd  
anonymous\_enable=NO  
local\_enable=YES  
write\_enable=YES  
anon\_upload\_enable=NO  
anon\_mkdir\_write\_enable=NO  
anon\_other\_write\_enable=NO  
anon\_root=/var/ftp/anonymous  
dirmessage\_enable=YES  
connect\_from\_port\_20=YES  
chown\_uploads=YES  
chown\_username=ftp  
xferlog\_enable=YES  
xferlog\_file=/var/log/vsftpd.log  
idle\_session\_timeout=600  
data\_connection\_timeout=12000  
nopriv\_user=ftp  
ascii\_upload\_enable=NO  
ascii\_download\_enable=NO  
ftpd\_banner=Hello.  
user\_config\_dir=/etc/vsftpd/vusers  
chroot\_local\_user=YES  
chroot\_list\_enable=YES  
chroot\_list\_file=/etc/vsftpd/chroot\_list  
userlist\_file=/etc/vsftpd/user\_list  
userlist\_enable=YES  
userlist\_deny=NO

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		34

Додатково створимо файл `user_list` з користувачами яким дозволено під'єднуватись до сервера і файл `chroot_list`, в якому, якщо потрібно, вказується перелік користувачів, які будуть ізольовані одні від одного. Створюємо каталог `/etc/vsftpd/vusers`, куди поклав файли, названі так само, як імена користувачів, які мають доступ до FTP, наприклад, `upload`. Іншим користувачам доступ за замовчуванням закритий.

Тепер створюємо каталог `/etc/vsftpd/vusers`, в якому будуть зберігатися файли з конфігураціями для користувачів, що мають право на доступ до каталогів. Наприклад, якщо є користувач `upload`, створюємо у цьому каталозі файл з ім'ям `upload` і прописуємо в нього рядок `local_root = /var/ftp/upload`, відповідно створивши цей каталог і встановивши на нього потрібні права. Дана папка буде основною і відправною для даного користувача, а в ньому можна буде створити потрібну структуру каталогів з відповідними правами доступу.

На останньому етапі стартуємо службу командою `/etc/rc.d/init.d/vsftpd start`. Перевірити зв'язок можна з'єднавшись з сервером з іншого хоста.

## **3.2 Інструкції з налаштування активного комутаційного обладнання**

### **3.2.1 Інструкції з налаштування головного комутатора**

Allied Telesyn AT-x600-24Ts – комутатор рівня 2 і 3, що підтримує статичну та динамічну маршрутизацію, а також VLAN.

Підключення та налаштування:

Фізичне підключення: Підключіть комутатор до джерела живлення та підключіть його порти до відповідних пристроїв (серверів, інших комутаторів, робочих станцій) за допомогою кабелів Ethernet.

Доступ до інтерфейсу управління:

									Арк.
									35
Зм.	Арк.	№ докум.	Підпис	Дата	2024.КРБ.123.602.9.00.00 ПЗ				

IP-адреса за замовчуванням: Зазвичай це 192.168.1.1.

Доступ через веб-браузер: Відкрийте веб-браузер та введіть IP-адресу комутатора.

Логін та пароль: Зазвичай, це admin/admin або admin/password. Змініть пароль за замовчуванням з міркувань безпеки.

Базова конфігурація:

Назва комутатора (hostname): Встановіть унікальну назву для ідентифікації комутатора в мережі.

Часовий пояс: Налаштуйте правильний часовий пояс для синхронізації часу на комутаторі.

IP-адресація: Призначте статичну IP-адресу комутатору або налаштуйте отримання IP-адреси через DHCP, якщо це необхідно.

Маршрутизація:

Статична маршрутизація: Використовуйте команду ip route для додавання статичних маршрутів до інших підмереж або шлюзу за замовчуванням.

Динамічна маршрутизація: Якщо використовується протокол динамічної маршрутизації (наприклад, OSPF), налаштуйте його відповідно.

VLAN (Віртуальні локальні мережі):

Створення VLAN: Створіть необхідні VLAN та призначте їм унікальні ідентифікатори (VLAN ID).

Призначення портів: Призначте порти комутатора до відповідних VLAN.

VLAN Tagging: Увімкніть VLAN Tagging на портах, які підключаються до інших комутаторів або пристроїв, що підтримують VLAN.

Spanning Tree Protocol (STP):

Увімкнення STP: Увімкніть STP для запобігання петлям у мережі.



Налаштування пріоритету: Налаштуйте пріоритет STP на комутаторі, щоб визначити, який комутатор буде кореневим мостом.

Безпека:

SSH: Увімкніть доступ до комутатора через SSH та вимкніть доступ через Telnet з міркувань безпеки.

ACL (Списки контролю доступу): Використовуйте ACL для обмеження доступу до комутатора або певних VLAN.

Port Security: Увімкніть Port Security для обмеження кількості MAC-адрес, які можуть бути вивчені на порту.

Моніторинг та управління:

SNMP: Налаштуйте SNMP для моніторингу комутатора за допомогою системи управління мережею (NMS).

Syslog: Налаштуйте Syslog для відправки повідомлень про події на віддалений сервер журналювання.

Додаткові функції:

QoS (Quality of Service): Налаштуйте QoS для пріоритезації важливого трафіку.

Link Aggregation (802.3ad): Об'єднайте кілька портів в один логічний канал для збільшення пропускної здатності та забезпечення резервування.

Приклад конфігурації (CLI):

```
configure terminal // Вхід в режим налаштування
hostname Switch-Core // Ім'я комутатора
ip domain-name agroserv.com // Доменне ім'я
interface vlan 1 // Налаштування VLAN 1
  name Default // Ім'я VLAN
```

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		37

```

ip address 10.15.0.1 255.255.0.0 // IP-адреса та маска
exit
interface GigabitEthernet 1/0/1 // Налаштування порту 1
  switchport mode access // Режим порту: access
  switchport access vlan 11 // Призначення VLAN 11
exit
// (аналогічно налаштувати інші порти)
ip default-gateway 10.15.0.254 // Шлюз за замовчуванням
spanning-tree mode rstp // Увімкнення RSTP
snmp-server community public RO // Налаштування SNMP (тільки читання)
logging host 10.15.19.2 // IP-адреса Syslog сервера
// (налаштування QoS, Link Aggregation та інших функцій)
end // Вихід з режиму налаштування
copy running-config startup-config // Збереження конфігурації

```

Allied Telesyn AT-x600-24Ts підтримує функцію агрегування каналів (Link Aggregation), що дозволяє об'єднати кілька фізичних портів в один логічний.

Переваги агрегування каналів:

Збільшення пропускної здатності: Сумарна пропускна здатність агрегованого каналу дорівнює сумі пропускних здатностей окремих портів.

Резервування: Якщо один з портів в агрегованому каналі виходить з ладу, трафік автоматично перемикається на інші порти, забезпечуючи безперервність роботи.

Балансування навантаження: Трафік розподіляється між портами агрегованого каналу, що дозволяє уникнути перевантаження окремих портів.

Налаштування агрегування каналів (Link Aggregation) на Allied Telesyn AT-x600-24Ts:

Створення групи агрегування (LAG):

```

configure terminal
lag <LAG_ID>

```

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		38

Замініть <LAG\_ID> на унікальний ідентифікатор групи агрегування.

Додавання портів до LAG:

```
lag <LAG_ID> member GigabitEthernet <PORT_LIST>
```

Замініть <LAG\_ID> на ідентифікатор LAG, а <PORT\_LIST> на список портів, які потрібно додати до групи (наприклад, 1/0/1 1/0/2).

Налаштування LAG:

```
interface lag <LAG_ID>
```

IP-адреса: Якщо необхідно, призначте IP-адресу агрегованому каналу.

VLAN: Призначте агрегований канал до відповідного VLAN.

LACP: Якщо використовується протокол LACP для динамічного формування агрегованих каналів, увімкніть його на комутаторі та на підключеному пристрої.

Перевірка:

```
show lag
```

Ця команда покаже інформацію про налаштовані групи агрегування та їх стан.

### 3.2.2 Інструкції з налаштування комутаторів робочих груп

Налаштування комутаторів робочих груп D-Link DGS-1100-08 (або D-Link DGS-1210-16):

Підключення:

Підключіть комутатор до джерела живлення.

Підключіть порти комутатора до робочих станцій та до центрального комутатора (uplink).

Доступ до інтерфейсу управління:

IP-адреса за замовчуванням: 192.168.0.1 (або 10.90.90.90).

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		39

Доступ через веб-браузер: Відкрийте веб-браузер та введіть IP-адресу комутатора.

Логін та пароль: admin/admin (або admin/password). Змініть пароль за замовчуванням.

Налаштування VLAN:

Створення VLAN: Створіть необхідні VLAN (наприклад, VLAN10 для відділу маркетингу).

Призначення портів:

Access порти: Призначте порти, підключені до робочих станцій, до відповідних VLAN.

Trunk порт: Порт, підключений до центрального комутатора, повинен бути налаштований як Trunk, дозволяючи передачу трафіку декількох VLAN.

QoS (Quality of Service):

Пріоритезація трафіку: Налаштуйте QoS для пріоритезації важливого трафіку (наприклад, голосового або відео).

Обмеження пропускної здатності: Обмежте пропускну здатність для певних типів трафіку або користувачів.

Безпека:

Port Security: Увімкніть Port Security для обмеження кількості MAC-адрес на портах.

DHCP Snooping: Увімкніть DHCP Snooping для запобігання несанкціонованим DHCP-серверам.

Моніторинг та управління:

SNMP: Налаштуйте SNMP для моніторингу комутатора.

Syslog: Налаштуйте Syslog для відправки повідомлень про події.

Port Mirroring: Використовуйте Port Mirroring для моніторингу трафіку.

Налаштування (CLI):

configure terminal

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		40

```

hostname Switch-Marketing // Ім'я комутатора
vlan 10 // Створення VLAN 10
  name Marketing // Ім'я VLAN
  exit
interface GigabitEthernet 1/0/1 // Налаштування порту 1
  switchport mode access
  switchport access vlan 10
  exit
// (аналогічно налаштувати інші порти)
interface GigabitEthernet 1/0/8 // Налаштування Trunk порту
  switchport mode trunk
  exit
spanning-tree mode rstp
loop-protect all // Захист від петель
// (налаштування QoS, Port Security)
end
copy running-config startup-config

```

Захист від петель реалізується за допомогою функції Loop Protect. IGMP Snooping дозволяє комутатору «прослуховувати» IGMP-трафік між маршрутизатором і кінцевими вузлами. Це дозволяє комутатору дізнатися, які порти зацікавлені в отриманні багатоадресного трафіку, і пересилати його тільки на ці порти, зменшуючи навантаження на інші порти і мережу в цілому. IPv6 – це новий протокол Інтернету, який має замінити IPv4. Він має більший адресний простір, що дозволяє підключити до Інтернету набагато більше пристроїв. Якщо ваша мережа використовує IPv6, переконайтеся, що комутатор підтримує цей протокол.

### 3.2.3 Інструкції з налаштування безпроводного маршрутизатора

						2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата			41

TP-Link Archer C7 AC1750 – це потужний дводіапазонний маршрутизатор, що підтримує сучасний стандарт Wi-Fi 802.11ac. Він забезпечує високу швидкість передачі даних до 1,75 Гбіт/с (1300 Мбіт/с на 5 ГГц і 450 Мбіт/с на 2,4 ГГц).

Підключення та вхід в інтерфейс налаштувань:

Підключіть маршрутизатор до джерела живлення та підключіть його WAN-порт до модему або іншого пристрою, що надає доступ до Інтернету. Підключіть комп'ютер до одного з LAN-портів маршрутизатора за допомогою кабелю Ethernet. Відкрийте веб-браузер та введіть IP-адресу маршрутизатора (зазвичай 192.168.0.1 або 192.168.1.1). Введіть ім'я користувача та пароль (зазвичай admin/admin).

Налаштування Інтернет-з'єднання:

Перейдіть до розділу "WAN" або "Internet" в інтерфейсі налаштувань. Виберіть тип підключення до Інтернету (DHCP, Static IP, PPPoE тощо), який надає ваш провайдер. Введіть необхідні дані, такі як IP-адреса, маска підмережі, шлюз за замовчуванням, ім'я користувача та пароль (якщо потрібно).

Налаштування Wi-Fi:

Перейдіть до розділу "Wireless" або "Wi-Fi". Встановіть ім'я мережі (SSID) для кожного діапазону (2,4 ГГц та 5 ГГц). Виберіть режим безпеки WPA2-PSK та встановіть надійний пароль. Увімкніть функцію WPS (Wi-Fi Protected Setup), якщо потрібно спростити підключення пристроїв.

Налаштування DHCP-сервера:

Перейдіть до розділу "LAN" або "Network". Увімкніть DHCP-сервер та встановіть діапазон IP-адрес, які будуть видаватися пристроям автоматично. Встановіть час оренди IP-адрес.

Налаштування безпеки:

									Арк.
									42
Зм.	Арк.	№ докум.	Підпис	Дата	2024.КРБ.123.602.9.00.00 ПЗ				

Перейдіть до розділу "Security" або "Firewall". Увімкніть брандмауер маршрутизатора. Налаштуйте правила брандмауера для обмеження доступу з Інтернету до локальної мережі. Увімкніть функцію захисту від DoS-атак.

Додаткові налаштування:

Гостьова мережа: Створіть окрему гостьову мережу Wi-Fi з обмеженим доступом до локальної мережі.

Батьківський контроль: Налаштуйте обмеження доступу до певних сайтів або в певний час.

VPN-сервер: Увімкніть VPN-сервер для безпечного віддаленого доступу до локальної мережі.

Переадресація портів: Налаштуйте переадресацію портів, якщо потрібно надати доступ з Інтернету до певних сервісів у локальній мережі.

Так само варто відзначити, що DGS-1210-20 підтримує статичну маршрутизацію, що дозволяє вручну налаштувати маршрути для трафіку між різними підмережами. Це може бути корисним, якщо у вашій мережі є кілька VLAN або підмереж, і вам потрібно контролювати, як трафік передається між ними. Крім того, комутатор підтримує протокол SNMP (Simple Network Management Protocol), який дозволяє віддалено моніторити та керувати комутатором. Це може бути корисним для адміністраторів мережі, оскільки дозволяє їм відстежувати стан комутатора, налаштовувати його параметри та отримувати сповіщення про проблеми. Також DGS-1210-20 має функцію Port Mirroring, яка дозволяє копіювати трафік з одного або декількох портів на інший порт для моніторингу та аналізу. Це може бути корисним для виявлення та усунення несправностей у мережі.

### **3.3 Інструкції з використання тестових наборів та тестових програм**

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		43

Для тестування локальної мережі можна використовувати різноманітні тестові набори та програми. Найпростіший спосіб - використання вбудованих у операційну систему інструментів, таких як ping та traceroute. Ping дозволяє перевірити доступність віддаленого вузла та виміряти час відгуку. Traceroute показує маршрут пакетів до віддаленого вузла та час проходження кожного сегмента маршруту.

Для більш детального тестування можна використовувати спеціалізовані програми, такі як iperf та netperf. Iperf дозволяє виміряти пропускну здатність мережі, а netperf - продуктивність різних мережевих протоколів. Також існують комплексні тестові набори, які включають різноманітні інструменти для тестування різних аспектів роботи мережі.

Наприклад, набір інструментів NetIQ Chariot дозволяє емулювати різні типи трафіку та вимірювати продуктивність мережі в різних умовах.

При виборі тестових наборів та програм необхідно враховувати особливості мережі, яку потрібно протестувати. Наприклад, якщо мережа використовує технологію VLAN, необхідно вибрати інструменти, які підтримують цю технологію. Також важливо враховувати вимоги до точності та деталізації результатів тестування.

Після вибору тестових інструментів необхідно розробити план тестування. План повинен включати опис тестових сценаріїв, метрики, які будуть вимірюватися, та критерії успішності тестування. Тестування необхідно проводити в різних умовах, наприклад, при різному навантаженні на мережу.

Результати тестування необхідно проаналізувати та зробити висновки щодо відповідності мережі вимогам. Якщо виявлені проблеми, необхідно вжити заходів щодо їх усунення. Тестування необхідно проводити регулярно, щоб забезпечити стабільну та надійну роботу мережі.

Для моніторингу та аналізу мережевого трафіку комутатор DGS-1210-20 має функцію Port Mirroring, яка дозволяє копіювати трафік з одного або

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		44



декількох портів на інший порт. Це може бути корисним для виявлення та усунення несправностей мережі, а також для аналізу безпеки. Крім того, комутатор підтримує функцію Loopback Detection, яка допомагає виявляти та запобігати петлям у мережі. Петлі можуть виникати, коли два порти комутатора підключені один до одного, або коли є кілька шляхів між двома пристроями в мережі. Петлі можуть призвести до зниження продуктивності мережі та навіть до її повної відмови. Loopback Detection допомагає запобігти цьому, відключаючи порти, на яких виявлено петлі.

### 3.4 Інструкції з експлуатації та моніторингу в мережі

Експлуатація та моніторинг локальної мережі є важливим аспектом забезпечення її безперебійної та ефективної роботи. Для цього необхідно регулярно проводити моніторинг стану мережевого обладнання, виявляти та усувати несправності, а також оновлювати програмне забезпечення.

Моніторинг мережевого обладнання можна здійснювати за допомогою спеціалізованих програмних засобів, таких як Nagios, Zabbix або Cacti. Ці програми дозволяють відстежувати різні параметри роботи обладнання, такі як завантаження процесора, використання пам'яті, пропускну здатність мережевих інтерфейсів тощо. У разі виявлення проблем, програми можуть надсилати сповіщення адміністратору мережі.

Виявлення та усунення несправностей мережі може бути складним завданням, особливо у великих мережах. Для полегшення цього процесу можна використовувати спеціалізовані інструменти, такі як мережеві аналізатори та тестери. Ці інструменти дозволяють аналізувати мережевий трафік, виявляти помилки та інші проблеми.

Оновлення програмного забезпечення є важливим заходом безпеки, оскільки воно дозволяє усувати вразливості, які можуть бути використані зловмисниками для атак на мережу. Необхідно регулярно

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		45

оновлювати операційні системи, мережеві служби та інше програмне забезпечення, яке використовується в мережі.

Крім того, важливо мати план дій у разі виникнення аварійних ситуацій. Цей план повинен включати процедури відновлення роботи мережі, а також контакти відповідальних осіб.

Для забезпечення безпеки мережі необхідно використовувати різні засоби захисту, такі як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення. Брандмауери дозволяють контролювати трафік, що проходить через мережу, і блокувати небажаний трафік. Системи виявлення вторгнень дозволяють виявляти спроби несанкціонованого доступу до мережі. Антивірусне програмне забезпечення дозволяє виявляти та видаляти шкідливе програмне забезпечення.

Loopback Detection відключає порти, на яких виявлено петлі, і таким чином запобігає виникненню проблем у мережі. Крім того, комутатор підтримує функцію управління потоком (Flow Control), яка дозволяє запобігти перевантаженню мережі шляхом обмеження швидкості передачі даних відправником. Це може бути корисним, якщо приймач не встигає обробляти дані, що надходять зі швидкістю, з якою їх відправляє відправник.

### 3.5 Інструкції по налаштуванню засобів захисту мережі

iptables - це потужний інструмент для налаштування брандмауера в Linux, який дозволяє фільтрувати пакети на основі різних критеріїв, таких як IP-адреси, порти, протоколи тощо. Він є частиною ядра Linux і забезпечує високу продуктивність та гнучкість.

Основні поняття:

Таблиці: iptables має кілька вбудованих таблиць, кожна з яких відповідає за певний тип обробки пакетів. Найчастіше використовуються

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		46

таблиці filter (для фільтрації пакетів), nat (для трансляції мережевих адрес) та mangle (для зміни пакетів).

Ланцюжки: Кожна таблиця містить кілька ланцюжків, які визначають порядок обробки пакетів. Наприклад, таблиця filter має ланцюжки INPUT (для вхідного трафіку), OUTPUT (для вихідного трафіку) та FORWARD (для трафіку, що пересилається).

Правила: Кожен ланцюжок містить набір правил, які визначають, що робити з пакетом. Правило складається з умови (наприклад, IP-адреса джерела) та дії (наприклад, ACCEPT або DROP).

Базові команди:

iptables -L: Показати список правил у таблиці filter.

iptables -F: Видалити всі правила у таблиці filter.

iptables -A INPUT -s <IP\_ADDRESS> -j ACCEPT: Дозволити вхідний трафік з IP-адреси <IP\_ADDRESS>.

iptables -A OUTPUT -d <IP\_ADDRESS> -j ACCEPT: Дозволити вихідний трафік на IP-адресу <IP\_ADDRESS>.

iptables -A FORWARD -s <IP\_ADDRESS> -d <IP\_ADDRESS> -j ACCEPT: Дозволити пересилання трафіку з IP-адреси <IP\_ADDRESS> на IP-адресу <IP\_ADDRESS>.

iptables -P INPUT DROP: Заборонити весь вхідний трафік за замовчуванням.

iptables -P OUTPUT DROP: Заборонити весь вихідний трафік за замовчуванням.

iptables -P FORWARD DROP: Заборонити все пересилання трафіку за замовчуванням.

Налаштування брандмауера:

# Заборонити весь вхідний, вихідний та пересилаємий трафік за замовчуванням

iptables -P INPUT DROP

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		47

```
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# Дозволити весь трафік з локальної мережі
iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.1.0/24 -j ACCEPT
# Дозволити петльовий трафік
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Дозволити встановлені з'єднання
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Дозволити вхідний SSH трафік
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
# Дозволити вихідний DNS трафік
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
# Включити маскування для вихідного трафіку
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Функція Spanning Tree Protocol (STP) дозволяє запобігти утворенню петель у мережі, які можуть виникнути, якщо є кілька шляхів між двома пристроями. Петлі можуть призвести до зниження продуктивності мережі та навіть до її повної відмови. STP вирішує цю проблему, блокуючи деякі порти комутатора, щоб залишити тільки один активний шлях між будь-якими двома пристроями.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		48

## 4 ЕКОНОМІЧНА ЧАСТИНА

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі портфолію власних графічних робіт.

Комп'ютерна мережа і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для розрахунку вартості НДР необхідно виконати наступні етапи:

- описати технологічний процес розробки із зазначенням трудомісткості кожної операції;
- визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;
- визначити суму матеріальних затрат;
- обчислити витрати на електроенергію для науково–виробничих цілей;
- розрахувати транспортні витрати;
- нарахувати суму амортизаційних відрахувань;
- визначити суму накладних витрат;
- скласти кошторис та визначити собівартість НДР;
- розрахувати ціну НДР;
- визначити економічну ефективність та термін окупності продукту.

### 4.1 Визначення економічної ефективності і терміну окупності капітальних вкладень

Для визначення загальної тривалості проведення НДР доцільно дані витрат часу по окремих операціях технологічного процесу звести у таблиця 4.1.

					2024.КРБ.123.602.09.00.00 ПЗ	Арк
Змн	Арк	№. докум.	Підпис	Дата		49

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

№п /п	Назва стадії	Виконавець	Середній час виконання операції, год.
1	Аналіз технічного завдання	Керівник проекту	2 год.
2	Вибір елементної бази	Керівник проекту	2 год.
3	Розробка функціональної мережі	Керівник проекту	8 год.
4	Розробка додатку для Комп'ютерної мережі	Лаборант	10 год.
5	Розробка алгоритму мережі	Лаборант	8 год.
6	Написання текстів програми для мережі	Лаборант	5 год.
7	Розробка інструкції з експлуатації мережі	Лаборант	2 год.
8	Затвердження проекту	Лаборант	1 год.
Разом			38 год.

#### 4.2 Визначення витрат на оплату праці та відрахування на соціальні заходи

Відповідно до Закону України «Про оплату праці» заробітна плата – це «винагорода, обчислена у грошовому виразі, яку власник виплачує працівникові за виконану ним роботу».

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно–ділових якостей працівника, результатів його праці та

господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

$$Z_{осн.} = T_c \cdot K_2, \quad (4.1)$$

де  $T_c$  – тарифна ставка, грн.;

$K_2$  – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 90 грн./год., лаборант – 70 грн./год.

$$Z_{осн.} = 90 \cdot 12 + 70 \cdot 26 = 2900 \text{ грн.}$$

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

$$Z_{дод.} = Z_{осн.} \cdot K_{дод.}, \quad (4.2)$$

де  $K_{дод.}$  – коефіцієнт додаткових виплат працівникам.

$$Z_{дод.} = 2900 \cdot 0,15 = 435 \text{ грн.}$$

Звідси загальні витрати на оплату праці (Во.п.) визначаються за формулою:

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

$$B_{о.п.} = 2900 + 435 = 3335 \text{ грн.}$$

Крім того, слід визначити відрахування на заробітну плату: єдиний соціальний внесок – 22 %.

					2024.КРБ.123.602.09.00.00 ПЗ	Арк
Змн	Арк	№. докум.	Підпис	Дата		51

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{з.п.} = \Phi ОП \cdot 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$B_{с.з.} = 3335 \cdot 0,22 = 733,7 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

No п/п	Категорія прац.	Основна заробітна плата, грн			Додаткова зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрат на оплату праці, грн.
		Тариф. ставка, грн.	К–сть від– пр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	90	12	1080	162	–	–
2	Лаборант	70	26	1820	273	–	–
Разом				2900	435	733,7	4068,7

Отже, загальні витрати на оплату праці становлять 12 206,1 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 і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

					<i>2024.КРБ.123.602.09.00.00 ПЗ</i>	Арк
Змн	Арк	№. докум.	Підпис	Дата		52



$$З_{м.в.} = \sum M_{Ві}, \quad (4.6)$$

$$З_{м.в.} = 5\,066.6 \text{ грн.}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1–ці, грн	Загальна сума витрат, грн.
1	Комунікаційна шафа	шт.	1 шт.	16 000	16 000
2	Патч-панелі	шт.	1 шт.	3 200	3 200
3	Мережеві розетки	шт.	1 шт.	4 000	4 000
4	Кабель UTP кат.	шт.	1 шт.	6 100	6 100
5	Патч-корди	шт.	1 шт.	700	700
6	Кабельні тримачі	шт.	1 шт.	400	400
Разом			1 шт.	30 400	30 400

#### 4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

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

де  $W$  – необхідна потужність, кВт;

$T$  – кількість годин роботи обладнання;

$S$  – вартість кіловат–години електроенергії.

Для розробки проекту веб–сайту портфоліо власних графічних робіт використовується один ПК, потужність якого  $W = 0,5$  кВт і який працює 120 години. Вартість 1 кВт електроенергії становить 4,32 грн.

$$З_e = 0,50 \cdot 36 \cdot 4,32 = 77,76 \text{ грн.}$$

					<i>2024.КРБ.123.602.09.00.00 ПЗ</i>	Арк
Змн	Арк	№. докум.	Підпис	Дата		53

## 4.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є 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.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$Ц = \frac{Б_в \cdot Н_A}{100\%} \quad (4.8)$$

де  $A$  – амортизаційні відрахування за звітний період, грн.;

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

$НА$  – норма амортизації, %.

Для проектування комп'ютерної мережі використовується один комп'ютер (вартість якого становить 20000 грн.), який працює 38 години.

Тоді:

$$A = 20000 \cdot 0,04 \cdot 36 / 150 = 192 \text{ грн.}$$

## 4.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

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

$$H_в = V_{o.n.} \cdot 0,2 \dots 0,6, \quad (4.9)$$

де  $HВ$  – накладні витрати.

$$H_в = 3335 \cdot 0,4 = 1334 \text{ грн.}$$

					2024.КРБ.123.602.09.00.00 ПЗ	Арк
Змн	Арк	№.докум.	Підпис	Дата		54

#### 4.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у табл. 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	3335	9,24
Відрахування на соціальні виплати	733,7	2,03
Матеріальні витрати	30 400	84,25
Витрати на електроенергію	77,76	0,22
Амортизаційні відрахування	202,67	0,56
Накладні витрати	1334	3,70
Собівартість	36 083,13	100

Собівартість ( $C_b$ ) НДР розраховуємо за формулою:

$$C_b = B_{o.n.} + B_{c.z.} + Z_{m.v.} + Z_e + A + H_b, \quad (4.10)$$

$$C_b = 3335 + 733,7 + 30\,400 + 77,76 + 202,67 + 1334 = 5694,50 \text{ грн.}$$

#### 4.8 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_b(1 + P_{рен}) \cdot K + B_{н.і}}{K} \cdot (1 + ПДВ), \quad (4.11)$$

де  $P_{рен}$  – рівень рентабельності;

					<b>2024.КРБ.123.602.09.00.00 ПЗ</b>	Арк
						55
Змн	Арк	№. докум.	Підпис	Дата		

$K$  – кількість замовлень, од.;

$V_{н.і.}$  – вартість носія інформації, грн.;

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

$$Ц = 36\,083,13 * 1,3 * 1,2 = 52\,286,68 \text{ грн.}$$

#### 4.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$\Pi = Ц - C_v \quad (4.13)$$

$$\Pi = 52\,286,68 - 36\,083,13 = 20\,206,55 \text{ грн.}$$

Економічна ефективність ( $E_p$ ) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$E_p = \Pi / C_v, \quad (4.14)$$

де  $\Pi$  – прибуток;

$C_v$  – собівартість.

$$E_p = 20\,206,55 / 36\,083,13 = 0,55$$

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень ( $T_p$ ):

					2024.КРБ.123.602.09.00.00 ПЗ	Арк
Змн	Арк	№. докум.	Підпис	Дата		56

$$T_p = 1 / E_p \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

$$T_p = 1 / 0,55 = 1,81$$

Таблиця 4.5 - Економічні показники НДР

№	Показник	Значення
1.	Собівартість, грн.	36 083,13
2.	Плановий прибуток, грн.	20 206,55
3.	Ціна, грн.	8883,43
4.	Термін окупності, рік	1,81

Враховуючи основні економічні показники, зведені у таблицю 4.5, можна зробити висновок, що при терміні окупності – 1,78 року проводити роботи по модернізації даної мережі є доцільним та економічно вигідним.



## 5 ОХОРОНА ПРАЦІ ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

### 5.1 Розслідування та облік нещасних випадків профзахворювань та аварій на виробництві

Розслідування та облік нещасних випадків, професійних захворювань та аварій на виробництві є важливою складовою системи управління охороною праці на підприємстві. Цей процес має на меті виявити причини та обставини, що призвели до нещасного випадку або захворювання, та вжити заходів щодо запобігання подібним випадкам у майбутньому. Розслідування проводиться комісією, до складу якої входять представники роботодавця, профспілкової організації та інші фахівці.

У разі нещасного випадку на виробництві, роботодавець зобов'язаний негайно повідомити про це відповідні органи та провести розслідування. Розслідування проводиться з метою встановлення обставин та причин нещасного випадку, а також визначення винних осіб. За результатами розслідування складається акт за формою Н-1, який є підставою для призначення страхових виплат потерпілому.

Професійні захворювання також підлягають розслідуванню та обліку. Професійне захворювання - це захворювання, спричинене впливом шкідливих виробничих факторів на здоров'я працівника. Розслідування професійних захворювань проводиться з метою встановлення причинно-наслідкового зв'язку між захворюванням та умовами праці. За результатами розслідування складається акт за формою П-4.

Аварії на виробництві також підлягають розслідуванню та обліку. Аварія на виробництві - це раптова подія, що призвела до травмування або загибелі людей, пошкодження будівель, споруд, обладнання або транспортних засобів, а також до порушення виробничого

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		58

процесу. Розслідування аварій проводиться з метою встановлення причин та обставин аварії, а також визначення винних осіб.

Облік нещасних випадків, професійних захворювань та аварій на виробництві ведеться у спеціальних журналах. Ці журнали є підставою для аналізу стану охорони праці на підприємстві та розробки заходів щодо його покращення.

Для забезпечення високої якості обслуговування (QoS) в мережі можна використовувати механізм пріоритезації трафіку, який дозволяє виділити важливий трафік, такий як голосовий або відео, і надати йому перевагу перед іншим трафіком. Це забезпечує більш високу якість передачі важливого трафіку, навіть якщо мережа перевантажена.

Також для підвищення безпеки мережі можна використовувати технологію віртуальних локальних мереж (VLAN), яка дозволяє розділити фізичну мережу на кілька логічних мереж, що підвищує безпеку та керованість мережі. Наприклад, можна створити окремі VLAN для різних відділів компанії або для різних типів трафіку.

Для забезпечення високої доступності мережі можна використовувати технологію резервування маршрутизаторів. Це означає, що в мережі буде два маршрутизатори, один з яких буде основним, а інший - резервним. У разі відмови основного маршрутизатора, резервний маршрутизатор автоматично візьме на себе його функції, забезпечуючи безперервність роботи мережі.

Для моніторингу та управління мережею можна використовувати протокол SNMP (Simple Network Management Protocol), який дозволяє збирати інформацію про стан мережевого обладнання та відправляти сповіщення про проблеми. Це дозволяє адміністратору мережі швидко виявляти та усувати несправності, забезпечуючи стабільну роботу мережі.

Для захисту мережі від несанкціонованого доступу можна використовувати різні методи аутентифікації, такі як

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		59



паролі, сертифікати, біометричні дані тощо. Також можна використовувати технологію мережевого екранування для захисту мережі від зовнішніх атак.

Для забезпечення оптимальної продуктивності мережі можна використовувати технологію балансування навантаження. Ця технологія дозволяє розподілити навантаження між кількома серверами або іншими мережевими пристроями, що підвищує продуктивність та надійність мережі.

## 5.2 Засоби пожежогасіння для оснащення ТОВ «АгроСерв»

Засоби пожежогасіння поділяються на такі основні види:

- Вогнегасники – переносні або пересувні пристрої для гасіння пожеж у початковій стадії їх виникнення. Вони бувають різних типів залежно від виду вогнегасної речовини:
  - Порошкові: ефективні для гасіння пожеж класів А, В, С та електроустановок під напругою до 1000 В.
  - Вуглекислотні: використовуються для гасіння пожеж класів В, С та електроустановок під напругою до 10 000 В. Не рекомендується використовувати для гасіння пожеж класу А, оскільки вони не забезпечують охолодження матеріалів, що горять, і можливе повторне займання.
  - Пінні: ефективні для гасіння пожеж класу А та деяких пожеж класу В.
- Внутрішні пожежні крани (ВПВ): призначені для гасіння пожеж водою. Вони встановлюються всередині будівель і підключаються до системи водопостачання.
- Пожежні щити: призначені для розміщення первинних засобів пожежогасіння (вогнегасників, лопат, відер, багрів тощо).

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		60

- Автоматичні установки пожежогасіння: призначені для автоматичного виявлення та гасіння пожеж. Вони бувають різних типів залежно від виду вогнегасної речовини (вода, піна, газ, порошок).
- Системи пожежної сигналізації: призначені для виявлення пожежі на ранній стадії та оповіщення людей про небезпеку.

Для оснащення ТОВ «АгроСерв» засобами пожежогасіння необхідно враховувати такі фактори:

- Площа та поверховість будівель: від цього залежить кількість та тип вогнегасників, ВПВ та пожежних щитів.
- Категорія пожежної безпеки приміщень: визначається залежно від виду виробництва та матеріалів, що використовуються.
- Наявність електроустановок: визначає необхідність використання вогнегасників, що не проводять електричний струм.

На основі аналізу цих факторів можна розробити план розміщення засобів пожежогасіння на підприємстві.(див.рис.5.1)Наприклад, можна встановити порошкові вогнегасники біля входу в кожне приміщення, вуглекислотні вогнегасники - біля електрощитових, пінні вогнегасники - в гаражах та майстернях. ВПВ та пожежні щити слід розміщувати на кожному поверсі будівлі у легкодоступних місцях.

Крім того, для підвищення рівня пожежної безпеки можна встановити автоматичні установки пожежогасіння та системи пожежної сигналізації. Це дозволить своєчасно виявити пожежу та вжити заходів щодо її гасіння, що мінімізує збитки від пожежі.

Важливо також проводити регулярні інструктажі з пожежної безпеки для співробітників підприємства та забезпечувати їх засобами індивідуального захисту (протигази, респіратори, захисні костюми).

										Арк.
										61
Зм.	Арк.	№ докум.	Підпис	Дата	2024.КРБ.123.602.9.00.00 ПЗ					



## ВИСНОВКИ

Результатом виконання кваліфікаційної роботи є розробка локальної комп'ютерної мережі для ТОВ «АгроСерв». Для проекту локальної мережі вибрано відповідні стандарти та технології, які дозволяють реалізувати поставлені завдання. Також вибрано відповідні логічну та фізичні топології, які відображають рух інформаційних потоків. Засобами технологій static routing, IEEE 802.1q оптимізовано структуру мережі згідно її організаційної структури.

Для проекту локальної мережі розроблено інструкції з налаштування сервера доступу до мережі Інтернет, файлового сервера, центрального комутатора. Всі інструкції враховують вимоги безпеки, що ставляться до сучасних локальних мереж.

В економічному розділі зроблено розрахунок собівартості робіт по розробці, встановленню та налаштуванню мережі для ТОВ «АгроСерв».

В розділі охорона праці описано техніку безпеки при роботі з обчислювальною технікою.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		63

## ПЕРЕЛІК ПОСИЛАНЬ

1. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Навчальний посібник. – Вид. 2-ге., доп. – Львів.: Афіша, 2000. – 176с.
2. Методичні вказівки до виконання дипломного проекту за напрямом підготовки №123 «Комп'ютерна інженерія»
3. Спортук М. Компьютерные сети и сетевые технологии./М. Спортук, Ф.Папас – ООО „ТИД ДС”, 2002. – 736 с.
4. Тхір І.,Калушка В., Юзьків А. Посібник користувача ПК.3-є видання. – Тернопіль: Підручники і посібники. 2006.-1024с.
5. Cent OS Project. [електронний ресурс] – Режим доступу: URL: <https://www.centos.org/docs/>. Дата доступу: 1.06.2022.
6. Базові поняття мережевих технологій. [електронний ресурс] – Режим доступу: URL: <http://um.co.ua/8/8-17/8-1748.html>. Дата доступу: 01.06.2022.
7. Безпека мережі. [електронний ресурс] – Режим доступу: URL: [https://uk.wikipedia.org/wiki/Безпека\\_мережі](https://uk.wikipedia.org/wiki/Безпека_мережі). Дата доступу: 25.05.2022.
8. Коммутатор DGS-1210. [електронний ресурс] – Режим доступу: URL: <http://www.dlink.ru/ru/products/1/3620.html>. Дата доступу: 1.06.2022.
9. Коммутатор DGS-1100-16. [електронний ресурс] – Режим доступу: URL: <http://www.dlink.ru/ru/products/1/1100.html>. Дата доступу: 1.05.2022.
10. Сервер HPE ML10. [електронний ресурс] – Режим доступу: URL: [http://rozetka.com.ua/ua/hp\\_e\\_ml-10\\_s\\_wsf/p4744250/](http://rozetka.com.ua/ua/hp_e_ml-10_s_wsf/p4744250/). Дата доступу: 1.06.2022.

					2024.КРБ.123.602.9.00.00 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		64

## ДОДАТКИ

Додаток А - Таблиця IP-адрес

Таблиця А1

№ п/п	Діапазон позначення вузлів	Назва відділу	Номер VLAN	Адреса вузла/ Маска	Шлюз
1	2	3	4	5	6
1	WS_1	Логісти	11	10.15.11.1/24	10.15.11.254
2	WS_2			10.15.11.2/24	
3	WS_3			10.15.11.3/24	
4	WS_4			10.15.11.4/24	
5	SW_1		1	192.168.1.1/24	-
6	WS_5	Відділ розрахунків	12	10.15.12.1/24	10.15.12.254
7	WS_6			10.15.12.2/24	
8	WS_7			10.15.12.3/24	
9	WS_8			10.15.12.4/24	
10	WS_9	Відділ роботи з клієнтами	13	10.15.13./24	10.15.13.254
11	WS_10			10.15.13./24	
12	WS_11			10.15.13./24	
13	WS_12			10.15.13./24	
14	SW_2		1	192.168.1.2/24	-
15	WS_13	Відділ контролю за перевезеннями	14	10.15.14.1/24	10.15.14.254
16	WS_14			10.15.14.2/24	
17	WS_15			10.15.14.3/24	
18	WS_16			10.15.14.4/24	
19	WS_17	Бухгалтерія	15	10.15.15./24	10.15.15.254
20	WS_18			10.15.15./24	
21	WS_19			10.15.15./24	
22	WS_20			10.15.15./24	
23	SW_3		-	192.168.1.3/24	-
24	WS_21	Заступники	16	10.15.16.1/24	10.15.16.254
25	WS_22			10.15.16.2/24	

Продовження таблиці А1

1	2	3	4	5	6
26	SW_4		1	192.168.1.4/24	
27	WS_23	Приймозна	17	10.15.17.1/24	10.15.17.254
28	WS_24	Директор	18	10.15.18.1/24	10.15.18.254
29	WS_25	ІТ-відділ	19	10.15.19.1/24	10.15.19.254
30	S_1			10.15.19.2/24	
31	S_2			10.15.19.3/24	
			-	динамічно	динамічно
32	SW_5		1	192.168.1.5/24	-
33	AP_1	Зал засідань	20	10.15.20.1/24	10.15.20.254
34	WS_26	Відділ евакуації та інженер з ТБ	21	10.15.21.1/24	10.15.21.254
35	WS_27			10.15.21.2/24	
36	WS_28	Відділ маркетингу	22	10.15.22.1/24	10.15.22.254
37	WS_29			10.15.22.2/24	
38	WS_30			10.15.22.3/24	
39	WS_31			10.15.22.4/24	
40	SW_6		1	192.168.1.6/24	-
41	WS_32	Відділ експлуатації транспортних засобів	23	10.15.23.1/24	10.15.23.254
42	WS_33			10.15.23.2/24	
43	WS_34			10.15.23.3/24	
44	WS_35			10.15.23.4/24	
45	WS_36	Відділ кадрів	24	10.15.24.1/24	10.15.24.254
46	WS_37			10.15.24.2/24	
47	SW_7		-	192.168.1.7/24	-
48	WS_38	Відділ міжнародних зв'язків	25	10.15.25.1/24	10.15.25.254
49	WS_39			10.15.25.2/24	

Додаток Б - Логічна адресація в ЛОМ. Таблиця конфігурування VLAN

Таблиця Б1 - Логічна адресація в ЛОМ

№ п/п	Діапазон позначення вузлів	Робоча група/К-сть вузлів		Приміщення	Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
		3	4		5	6		
1	WS_1-WS_4, SW_1	-	5	1	Логісти	-	11	10.15.11.0/24
2	WS_5-WS_8	-	4	1	Відділ розрахунків	-	12	10.15.12.0/24
3	WS_9-WS_12, SW_2	-	5	1	Відділ роботи з клієнтами	-	13	10.15.13.0/24
4	WS_13-WS_16	-	6	1	Відділ контролю за перевезеннями	-	14	10.15.14.0/24
5	WS_17-WS_20, SW_3	-	5	1	Бухгалтерія	-	15	10.15.15.0/24
6	WS_21-WS_22, SW_4	-	3	1	Заступники	-	16	10.15.16.0/24
7	WS_23	-	1	1	Приймозна	-	17	10.15.17.0/24
8	WS_24	-	1	1	Директор	-	18	10.15.18.0/24
9	WS_25, S_1, S_2, SW_5	-	3	1	ІТ-відділ	-	19	10.15.19.0/24
10	AP_1	-	1	1	Зал засідань	-	20	10.15.20.0/24
11	WS_26-WS_27	-	2	1	Відділ евакуації транспортних засобів	-	21	10.15.21.0/24
12	WS_28-WS_31, SW_6	-	5	1	Відділ маркетингу	-	22	10.15.22.0/24
13	WS_32-WS_35, SW_6	-	4	1	Відділ експлуатації транспортних засобів	-	23	10.15.23.0/24



Продовження таблиці Б1

1	2	3	4	5	6	7	8	9
14	WS_36- WS_37, SW_7	-	1	1	Відділ кадрів	-	24	10.15.24.0/24
15	WS_38- WS_39	-	1	1	Відділ міжнародних зв'язків	-	25	10.15.25.0/24

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мер. пристар.	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS_4	-	Access	SW_1	2-5	Trunk	11
2	WS_5-WS_8	-	Access	SW_1	6-9	Trunk	12
3	WS_9-WS_12	-	Access	SW_2	2-5	Trunk	13
4	WS_13-WS_16	-	Access	SW_2	6-9	Trunk	14
5	WS_17-WS_20	-	Access	SW_3	1-5	Trunk	15
6	WS_21-WS_22	-	Access	SW_4	2-5	Trunk	16
7	WS_23	-	Access	SW_4	6	Trunk	17
8	WS_24	-	Access	SW_4	7	Trunk	18
9	WS_25, S_1, S_2	-	Access	SW_5	1-3	Trunk	19
10	AP_1	-	Access	SW_5	4	Trunk	20
11	WS_26-WS_27	-	Access	SW_5	5-6	Trunk	21
12	WS_28-WS_31	-	Access	SW_6	2-5	Trunk	22
13	WS_32-WS_35	-	Access	SW_6	6-9	Trunk	23
14	WS_36-WS_37	-	Access	SW_7	2-3	Trunk	24
15	WS_38-WS_39	-	Access	SW_7	4-5	Trunk	25
17	SW_1	1	Trunk	SW_5	7	Trunk	-
18	SW_2	1	Trunk	SW_5	8	Trunk	-
19	SW_3	1	Trunk	SW_5	9	Trunk	-
20	SW_4	1	Trunk	SW_5	10	Trunk	-

Продовження таблиці Б2

1	2	3	4	5	6	7	8
21	SW_6	1	Trunk	SW_5	11	Trunk	-
22	SW_7	1	Trunk	SW_5	12	Trunk	-