

**Міністерство освіти і науки України**  
**Відокремлений структурний підрозділ «Тернопільський фаховий коледж**  
**Тернопільського національного технічного університету імені Івана Пулюя»**

---

(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

## **ПОЯСНЮВАЛЬНА ЗАПИСКА**

**до кваліфікаційної роботи**

**бакалавра**

(освітньо-кваліфікаційний рівень)

на тему:

**Розробка проекту комп'ютерної мережі**

**ПП «ВебКатТехнік»**

Виконав: студент VI курсу, групи КІБ-602

Спеціальності:

123 «Комп'ютерна інженерія

(шифр і назва спеціальності)

Дмитро Козак

(підпис)

(ім'я та прізвище)

Керівник

Андрій Юзьків

(підпис)

(ім'я та прізвище)

Рецензент

(підпис)

(ім'я та прізвище)

**Тернопіль – 2023**

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

Відділення телекомунікацій та електронних систем  
Циклова комісія комп'ютерної інженерії  
Освітньо-кваліфікаційний рівень бакалавр  
Спеціальність 123 «Комп'ютерна інженерія»  
(шифр і назва)

**ЗАТВЕРДЖУЮ**

Голова циклової комісії  
комп'ютерної інженерії

Андрій ЮЗЬКІВ

“01” травня 2023 року

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

**Козаку Дмитру Миколайовичу**

(прізвище, ім'я, по батькові студента)

1. Тема роботи: **Розробка проекту комп'ютерної мережі ПП «ВебКатТехнік»**

керівник роботи: Юзків Андрій Васильович

(прізвище, ім'я, по батькові)

затверджені наказом вищого навчального закладу від 1.05.2023р. № 4/9-173

2. Строк подання студентом кваліфікаційної роботи 21.06.2023р.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Перелік термінів і скорочень

Вступ

1 Загальний розділ

## 1.1 Технічне завдання

### 1.1.1 Найменування та область застосування

### 1.1.2 Призначення розробки

### 1.1.3 Вимоги до апаратного та програмного забезпечення

### 1.1.4 Вимоги до документації

### 1.1.5 Техніко-економічні показники

### 1.1.6 Стадії та етапи розробки

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

## 2 Розробка технічного та робочого проекту

### 2.1 Опис та обґрунтування вибору логічного типу мережі

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

### 2.3 Обґрунтування вибору комунікаційного обладнання

### 2.4 Особливості монтажу мережі

### 2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

### 2.6 Обґрунтування вибору засобів захисту мережі

### 2.7 Тестування та налагодження мережі

## 3 Спеціальний розділ

### 3.1 Інструкції з налаштування програмного забезпечення серверів

#### 3.1.1 Інструкція з налаштування файлового сервера

### 3.2 Інструкції з налаштування активного комутаційного обладнання

#### 3.2.1 Інструкція з базового налаштування маршрутизатора

#### 3.2.2 Інструкції з базового налаштування центрального комутатора

#### 3.2.3 Інструкції з налаштування комутаторів робочих груп

### 3.3 Інструкція з використання тестових наборів та тестових програм

### 3.4 Інструкції по налаштуванню засобів захисту мережі

### 3.5 Інструкція з експлуатації та моніторингу в мережі

### 3.6 Моделювання роботи локальної мережі

## 4 Економічний розділ

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

4.3 Розрахунок матеріальних витрат

4.4 Розрахунок витрат на електроенергію

4.5 Визначення транспортних затрат

4.6 Розрахунок суми амортизаційних відрахувань

4.7 Обчислення накладних витрат

4.8 Складання кошторису витрат та визначення собівартості НДР

4.9 Розрахунок ціни НДР

4.10 Визначення економ. ефективності і терміну окупності кап. вкладень

5 Охорона праці, техніка безпеки та екологічні вимоги

5.1 Основні травми і професійні захворювання користувачів комп'ютерних та інформаційних технологій.

5.2 Організація пожежної безпеки в компанії "ВебКатТехнік"

Висновки

Перелік посилань

Висновки: навести результати роботи по кожному розділу зокрема і загальний висновок по кваліфікаційній роботі

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

План приміщень

Логічна топологія

Фізична топологія

Таблиця IP-адрес

Таблиця техніко-економічних показників

Модель мережі

6. Консультанти розділів кваліфікаційної роботи бакалавра

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА викладач		
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	02.05	
2	Збір і узагальнення інформації по роботі	15.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	29.05	
5	Написання спеціального розділу	2.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	12.06	
9	Оформлення проекту	16.06	
10	Проходження нормоконтролю	19.06	
11	Попередній захист роботи	21.06	
12	Захист роботи		

7. Дата видачі завдання 2.05.2023р.

Студент

Керівник кваліфікаційної роботи

\_\_\_\_\_ (підпис) \_\_\_\_\_ Дмитро Козак  
(ім'я та прізвище)

\_\_\_\_\_ (підпис) \_\_\_\_\_ Андрій Юзків  
(ім'я та прізвище)

## АНОТАЦІЯ

Козак Д.М. Розробка проекту комп'ютерної мережі ПП «ВебКатТехнік»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2023. 77с.

Кваліфікаційна робота передбачає розробка проекту комп'ютерної мережі згідно стандартів та вимог замовника. Особливу увагу при розробці було приділено питанням безпеки. Завдання захисту локальної мережі, що проектується, від несанкціонованого доступу вирішено шляхом використання багатофункціонального маршрутизатора на базі ОС Linux (Router OS). Комп'ютерна мережа ПП «ВебКатТехнік» побудована на базі фізичної топології «Розширена зірка». В якості базової технології побудови мереж вибрано стандарт Gigabit Ethernet. При проектуванні комп'ютерної мережі враховано питання безпеки даних.

Ключові слова: комп'ютерна мережа, сервер, маршрутизатор.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						6
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

## ANNOTATION

Kozak D.M. Development of the PP computer network project «WebKatTechnik»: qualifying work for obtaining a bachelor's degree, specialty 123 Computer engineering. Ternopil: SSS "TPC TNTU", 2023. 77p.

The qualification work involves the development of a computer network project according to the standards and requirements of the customer. Special attention was paid to security issues during development. The task of protecting the projected local network from unauthorized access is solved by using a multifunctional router based on the Linux OS (Router OS). The computer network of PP «WebKatTechnik» is built on the basis of the physical topology "Extended Star". The Gigabit Ethernet standard was chosen as the basic technology for building networks. When designing a computer network, the issue of data security is taken into account.

Keywords: computer network, server, router.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		7

## ЗМІСТ

Перелік термінів і скорочень

Вступ

1 Загальний розділ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

1.1.2 Призначення розробки

1.1.3 Вимоги до апаратного та програмного забезпечення

1.1.4 Вимоги до документації

1.1.5 Техніко-економічні показники

1.1.6 Стадії та етапи розробки

1.2 Постановка задачі на розробку проекту. Характеристика компанії, для якого створюється проект мережі

2 Розробка технічного та робочого проекту

2.1 Опис та обґрунтування вибору логічного типу мережі

2.2 Розробка схеми фізичного розташування кабелів та вузлів:

2.3 Обґрунтування вибору комунікаційного обладнання

2.4 Особливості монтажу мережі

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

2.6 Обґрунтування вибору засобів захисту мережі

2.7 Тестування та налагодження мережі

3 Спеціальний розділ

3.1 Інструкції з налаштування програмного забезпечення серверів

3.1.1 Інструкція з налаштування файлового сервера

3.2 Інструкції з налаштування активного комутаційного обладнання

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>			
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>				
<i>Розробив</i>		<i>Козак Д.М.</i>			<i>Розробка проекту комп'ютерної мережі ТОВ "ВебКатТехнік"</i>	<i>Літ.</i>	<i>Арк.</i>	<i>Аркушів</i>
<i>Перевірів</i>		<i>Юзьків А.В</i>					<i>8</i>	
<i>Н. Контр.</i>		<i>Приймак В.А.</i>				<i>ВСП ТФК ТНТУ ім.І.Пулюя гр. КІБ-602 м.Тернопіль</i>		
<i>Затв.</i>								



- 3.2.1 Інструкція з базового налаштування маршрутизатора
- 3.2.2 Інструкції з базового налаштування центрального комутатора
- 3.2.3 Інструкції з налаштування комутаторів робочих груп
- 3.3 Інструкція з використання тестових наборів та тестових програм
- 3.4 Інструкції по налаштуванню засобів захисту мережі
- 3.5 Інструкція з експлуатації та моніторингу в мережі
- 3.6 Моделювання роботи локальної мережі
- 4 Економічний розділ
- 4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР
- 4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи
- 4.3 Розрахунок матеріальних витрат
- 4.4 Розрахунок витрат на електроенергію
- 4.5 Визначення транспортних затрат
- 4.6 Розрахунок суми амортизаційних відрахувань
- 4.7 Обчислення накладних витрат
- 4.8 Складання кошторису витрат та визначення собівартості НДР
- 4.9 Розрахунок ціни НДР
- 4.10 Визначення економ. ефективності і терміну окупності кап. вкладень
- 5 Охорона праці, техніка безпеки та екологічні вимоги
- 5.1 Основні травми і професійні захворювання користувачів комп'ютерних та інформаційних технологій.
- 5.2 Організація пожежної безпеки в компанії "ВебКатТехнік"
- Висновки
- Перелік посилань

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	<i>Арк</i>
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		9

## ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

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

802.3ae - 10 GbE;

DNS (Domain Name System) - сервер доменних імен;

EIA (Electronic Industries Association) - асоціація електронної промисловості;

IEEE 802.3 - 10BASE-T Ethernet;

IEEE 802.3ab - 1000BASE-T Gigabit Ethernet;

IEEE 802.3u - 100BASE-TX Fast Ethernet;

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;

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

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;

ОС - операційна система;

ПК - персональний комп'ютер.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		10

## ВСТУП

За допомогою локальних мереж можна здійснити ефективне управління великою кількістю комп'ютерів, забезпечити централізоване керування, надійну інформаційну безпеку та антивірусний захист. Використання персональних комп'ютерів як частини комп'ютерної мережі є невід'ємною складовою будь-якого підприємства або організації. Таке підключення дозволяє забезпечити спільну роботу, що має велике значення в сучасному світі. Прикладами операційних систем, які сприяють колективній роботі над спільними проектами, є Linux, Unix і інші.

Мережі підприємств і організацій використовують можливості колективної роботи співробітників, які користуються як локальними, так і Інтернет-послугами у своїй роботі. Використання різних типів мереж, включаючи провідні та безпроводові, сприяє підвищенню продуктивності праці, обробки інформації і використання мережевих ресурсів з боку всіх комп'ютерів та пристроїв в мережі. Це дозволяє співробітникам ефективно спілкуватися, спільно працювати над проектами, обмінюватися даними і ресурсами, а також отримувати доступ до централізованих служб інформаційної підтримки. Всі ці фактори сприяють покращенню робочого процесу та досягненню кращих результатів у виробничій діяльності.

Поряд з використанням локальних мереж актуальним питанням є захист мереж від вірусів та несанкціонованого доступу. Розробка проекту локальної мережі повинна враховувати всі сучасні аспекти мереж. Їх нехтування призведе до нестабільної роботи мережі в цілому або окремих її частин. Отож задача є доволі актуальною

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		11

# 1 ЗАГАЛЬНИЙ РОЗДІЛ

## 1.1 Технічне завдання

### 1.1.1 Найменування та область застосування

Тема дипломного проекту полягає у розробці комп'ютерної мережі для ПП " ВебКатТехнік ". Основним завданням розробки полягає у об'єднанні робочих станцій, забезпеченням доступу до мережевих ресурсів і можливості спільної роботи. Ця розробка має мати практичне застосування.

До ознак локальної мережі належать:

- Можливість використання мережевого обладнання різних виробників, забезпечує можливість вибору оптимального обладнання для конкретних потреб мережі.
- Сегментованість локальної мережі з можливістю передачі трафіку між сегментами та налаштуваннями правил фільтрації.
- Можливість включення вузлів в мережу без суттєвої модернізації структури, дає змогу швидко та зручно розширювати мережу і додавати нові пристрої.
- Можливість спільного використання ресурсів мережі.
- Спільне використання мережі інтернет і централізований захист локальної мережі дають змогу забезпечити доступ до зовнішніх ресурсів і забезпечити безпеку мережі.

### 1.1.2 Призначення розробки

Розробка має містити:

- Мережа має надавати гнучкі можливості використання мережевих ресурсів та обміну даними.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						12
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

- Всі ПК мають бути об'єднані в єдину інформаційну структуру.
- Мережа має забезпечувати спільний доступ до ресурсів мережі локальної обчислювальної мережі (ЛОМ) та мережі Інтернет.
- Всі користувачі мають мати доступ до мережі Інтернет.
- Файловий сервер має бути сконфігурований для збереження даних та забезпечення надійного зберігання даних.
- Фільтрація трафіку Інтернету та трафіку який передається між сегментами локальної мережі, має бути налаштоване.
- Швидкість передачі у мережі має задовольняти потреби мультимедійних додатків і враховувати можливість додавання нових вузлів.
- Потрібно захистити мережу від несанкціонованого допуску з інтернету.

### **1.1.3 Вимоги до апаратного та програмного забезпечення**

Комп'ютерну мережу можемо умовно поділити на апаратну і програмну складові. До апаратної складової належать: кабелі, роз'єми, мережеві плати, комутатори, сервери та інше обладнання. Програмна складова включає операційні системи серверів та комутаційного обладнання.

Сервер доступу до мережі інтернет і файловий сервер мусять забезпечувати необхідну швидкодію, яка розрахована на можливе зростання кількості робочих станцій у майбутньому. При виборі апаратної платформи для серверів важливо враховувати наявність RAID-контролера. Це дозволить налаштувати систему з відмовостійкістю. Так як файловий сервер відіграє одну із ключових ролей у комп'ютерній мережі ПП " ВебКатТехнік ", необхідно також забезпечити безперебійне живлення для вузлів мережі.

Центральний комутатор має мати підтримку швидкості передачі в мережі на рівні 1000 Мбіт/с. Важливо також, щоб комутатор мав підтримку функції STP (Spanning Tree Protocol), яка дозволяє створювати резервні шляхи в мережі

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	<i>Арк</i>
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		13

зادля уникнення петель. Крім того, комутатор має мати можливість роботи на рівні 3 моделі OSI, що дозволяє керувати потоками даних в мережі.

Серверне програмне забезпечення має мати підтримку технології NAT, і також можливість фільту трафіку на різних рівнях, зокрема на каналному, мережевому і транспортному рівнях. Програмне забезпечення робочих станцій мусить підтримувати роботу у мережі за допомогою протоколу TCP/IP.

При виборі мережевого обладнання враховується наявність запасу системних ресурсів, що дозволить використовувати його для майбутнього розширення і забезпечить обробку зростаючого навантаження, включаючи як корисний, і "паразитний" трафік. Рекомендована величина повинна становити не менше 50% від загальних ресурсів. Також слід враховувати можливість резервування інформації, оскільки використання дисків для збереження даних не забезпечує повну надійність.

#### 1.1.4 Вимоги до документації

Документація має значення в експлуатації мережі:

- Документація відіграє велику роль як інструмент для виявлення і вирішення несправностей у мережі.
- Інструмент масштабування локальної мережі, та виявлення вузьких місць.
- Документація допомагає в підготовці персоналу, надаючи інформацію та інструкції для роботи в конкретних ділянках мережі.
- Вона стає дуже корисним ресурсом для постачальників і консультантів, допомагаючи краще розуміти мережеву інфраструктуру і здійснювати роботу ефективніше та швидше. Таким чином, наявність документації мотивує оптимізацію роботи, полегшує навчання співробітників і поліпшує співпрацю з постачальниками і консультантами.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						14
Зм.	Арк	№ докум.	Підпис	Дата		

### 1.1.5 Техніко-економічні показники

- Топологія мережі - Розширена зірка.
- Стандарт мережі - Gigabit Ethernet.
- Кількість робочих станцій - 36.
- Технологія доступу до мережі - NAT
- Тип маршрутизації між підмережами - статична.
- Тип сервера - файловий.
- Фільтрація трафіку на канальному, транспортному, мережевому, прикладному рівнях моделі OSI.
- Трудомісткість проектування і інсталяції мереж - до 100 люд/год.
- Матеріальні витрати на мережу – до 150 000 грн.
- Собівартість мережі не більше – до 300 000 грн.
- Повна вартість мережі не більше - до 350 000 грн.

### 1.1.6 Стадії та етапи розробки

Проектування мережі для ПП " ВебКатТехнік " можна поділити на наступні етапи:

- Складання завдання, враховуючи вимоги замовника мережі.
- Оформлення завдання.
- Розробка логічної топології мережі.
- Розробка фізичної топології мережі.
- Складання списку обладнання для проекту
- Налаштування мережевого обладнання (комутатора третього рівня)
- Налаштування роутера.
- Налаштування файлового сервера.
- Тестування роботи обладнання, та перевірка його роботи.
- Тестування мережі, і визначення максимальних для стабільної роботи показників.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						15
Зм.	Арк	№ докум.	Підпис	Дата		

- Тестування конфігурацій мережевого обладнання та сервера.
- Налаштування програмного забезпечення для клієнтів.

## **1.2 Постановка задачі на розробку проекту.**

### **Характеристика підприємства, для якого створюється проект мережі**

ПП " ВебКатТехнік " спеціалізується на розробці, та наповненні, підтримці і хостингу веб-сайтів та Інтернет-магазинів для різних організацій, підприємств, фінансових установ та громадських організацій. Мета полягає у забезпеченні об'єднання робочих мість усіх відділів у єдину інформаційну мережу. Ми плануємо ввести у експлуатацію служби локальної мережі, що дозволять нам забезпечити з'єднання між робочими станціями різних відділів. Крім того, ми плануємо надати доступ до служб глобальної мережі інтернет, щоб працівники мали змогу використовувати усі переваги інтернет-ресурсів у роботі. Для забезпечення кращої організації і управління мережею, було використано план для розділення локальної мережі на менші логічні групи, які відповідатимуть структурі ПП " ВебКатТехнік ".

Після аналізу структури ПП " ВебКатТехнік " і враховуючи вимоги щодо захисту інформації, було прийнято рішення про створення наступних категорій користувачів:

- Відділ програмування
- Менеджери і маркетологи.
- Відділ дизайну.
- Відділ SEO і підтримки, Відділ наповнення, керівники проектів -

Бухгалтерія.

- Заступник.
- Директор.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	<i>Арк</i>
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		16



## 2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

### 2.1 Опис та обґрунтування вибору логічного типу мережі

Також було описано плани як використати комутатор для фільтрації трафіку у локальній мережі. Щоб досягнути плану було розроблено стандартні і також розширені списки допуску, які будуть установлені в операційній системі комутатора. У таблиці 2.1 було описано дані про розбиття мережі у підрозділи.

Таблиця 2.1 – Логічна адресація в ЛОМ

№ п/п	Діапазон позначення вузлів	Робоча група/Ксть вузлів		Прямі	Назва кабінету та його номер	Номер VLAN	Адреса підмережі/ Маска
1	2	3		4	5	6	7
1	WS_1WS_6	-	6	1	Відділ ремонту та обслуговування	101	10.10.1.0/24
2	WS_7WS_10, SW_1	-	5	1	Менеджери та маркетологи	102	10.10.2.0/24
3	WS_11WS_14	-	4	1	Економічний відділ	103	10.10.3.0/24
4	WS_15WS_18	-	4	1	Бухгалтерія	104	10.10.4.0/24
5	WS_19WS_24, SW_2	-	6	1	Магазин, склад	105	10.10.5.0/24
6	WS_25	-	1	1	Директор	106	10.10.6.0/24
7	WS_26	-	1	1	Приймальня	107	10.10.7.0/24
8	WS_27	-	1	1	Заступник	108	10.10.8.0/24
9	WS_28 WS_32	-	5	1	Відділ розробки	109	10.10.9.0/24
10	WS_33 WS_36	-	4	1	Відділ впровадження	110	10.10.10.0/24
11	R_1, S_1, SW_3	-	3	1	-	111	10.10.11.0/24

У Таблиці 2.2 описано дані типи портів, які можна використовувати на комутаторах для налаштування VLAN на вузлах мережі.

Таблиця 2.2 – Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мереж. пристр.	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS_6	-	-	SW 1	1-6	Access	101
2	WS_7-WS 10	-	-	SW 1	7-10	Access	102
3	WS_11-WS_14	-	-	SW_1	11-14	Access	103
4	WS_15-WS_18	-	-	SW 2	1-4	Access	104
5	WS_19-WS_24	-	-	SW 2	5-10	Access	105
6	WS_25	-	-	SW 3	1	Access	106
7	WS_26	-	-	SW 3	2	Access	107
8	WS_27	-	-	SW 3	3	Access	108
9	WS_28-WS_32	-	-	SW 3	4-8	Access	109
10	WS_33-WS_36	-	-	SW 3	9-12	Access	110
11	R_1, S_1, SW_3	-	-	SW 3	13-15	Access	111
12	SW_1	15	Trunk	SW 3	21	Trunk	-
13	SW_2	15	Trunk	SW 3	22	Trunk	-

Нижче наведено переваги, які отримуємо при об'єднанні персональних комп'ютерів у мережу:

1. Поділ ресурсів дозволяє ефективно використовувати їх, наприклад, керувати пристроями, такими як принтери, зовнішні накопичувачі, модеми та інші, з усіх підключених робочих станцій.
2. Поділ ресурсів процесора дозволяє використовувати обчислювальні потужності задля обробки даних іншими системами.
3. Поділ даних дає доступ та управління базами даних з різних робочих місць, що потребують цієї інформації.

4. Багатокористувацький режим дозволяє кільком користувачам одночасно отримувати доступ до додатків.

5. Поділ програмних засобів дозволяє одночасне використання централізованих програмних, забезпечуючи доступ до них для декількох користувачів одночасно.

У мережі має всі послуги мають взаємодію між клієнтами і серверами. Сервер - це комп'ютер, який взаємодіє з клієнтами відповідаючи на їх запити. Ця взаємодія відбувається запуском програм яка знаходиться сервері задля надання послуг. Сервер обробляє запити клієнтів та надсилає їм відповіді. Все надання послуг в мережі можна розділити на клієнтський і серверний. Серверне надання відповідає за надання мережевих послуг, а клієнтське надання забезпечує передачу запитів на сервера та отримання відповідей від нього.

На теперішній день, мережі класифікуються на:

1. Локальні мережі (LAN - Local Area Network) - це мережі, які покривають невелику територію з відстанню між комп'ютерами до 10 км.

2. Регіональні мережі - це мережі, які функціонують в межах міст, районів чи областей.

3. Глобальні мережі, WAN (Wide Area Network), є мережами, які функціонують в межах країни чи декількох країн. У таких мережах комп'ютери можуть бути розташовані на дуже великій відстані.

Локальна обчислювальна мережа (ЛОМ) - це система, у якій декілька комп'ютера підключені до спільного каналу передачі даних. Мінімальною конфігурацією такої мережі є два комп'ютери, які з'єднані між собою кабелем. З'єднання кабелем дає можливість використовувати ресурси обох комп'ютерів.

Архітектура мережі виєвляє фізичне розташування мережевих пристроїв, такі як: адаптери і кабелі, а також методи передачі даних через канали зв'язку. У мережевій архітектурі існують два основних типи мереж: рівноправні та серверно-клієнтські. У рівноправній мережі всі комп'ютери мають однакове значення: немає ієрархії між комп'ютерами і відсутній виділений сервер. Кожен

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		19

комп'ютер у цій мережі може виконувати роль і клієнта, і сервера. Користувачі самостійно вирішують, які дані на комп'ютері зробити загальнодоступними в мережі. Однак, якщо к-сть підключених людей перевищує 10, то рівноправна мережа може стати недостатньо продуктивною. Тому більшість застосовують виділені сервери. Виділений сервер функціонує виключно як сервер. Виділені сервери оптимізовані для бистої і ефективної обробки мережєвих запитів та надання послуг користувачам. Розроблена базова модель взаємодії відкритих систем OSI. Ця модель є міжнародним стандартом.

Існують гібридні типи мережі, які мають в собі переваги пірингових (однорангових) мереж та серверних мереж. Усі локальні обчислювальні мережі (ЛОМ) працюють відповідно до стандарту Open Systems Interconnection (OSI). На рисунку 2.1 зображена OSI модель.

## The Seven Layers of OSI

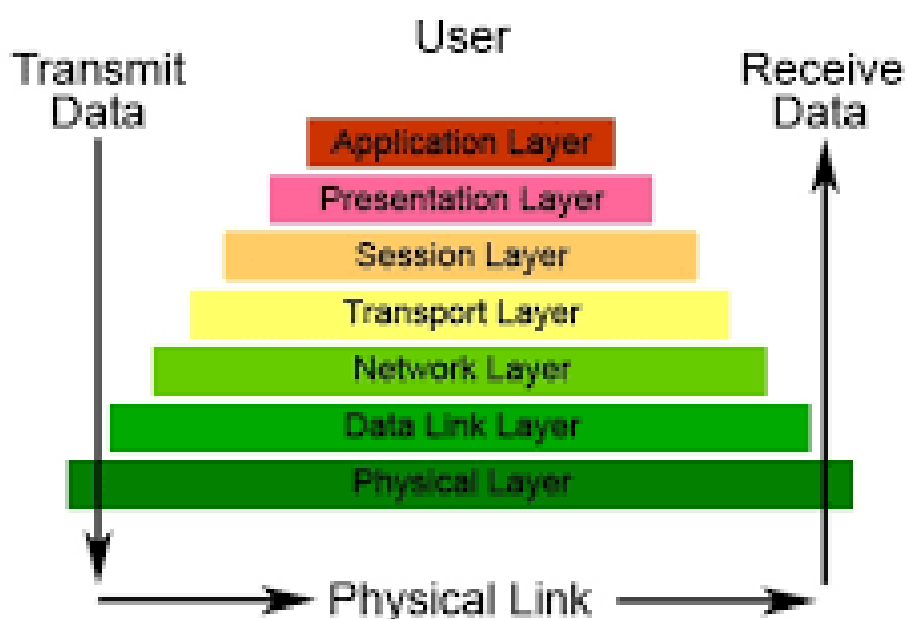


Рисунок 2.1 – Модель OSI

Аналогічно до того, як люди застосовують мову для взаємодії, з комп'ютерами, що є об'єднані в мережу, застосовують стандарти для

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		20

забезпечення взаємодії. Отже данні стандарти визначають спосіб подання даних в лініях зв'язку, через які передається інформація. Міжнародна організація по стандартизації (ISO) була заснована у 1984 році і грає важливу роль у встановленні єдиного стандарту.

Фізичний рівень мережі включає в себе встановлення фізичного з'єднання з каналом передачі даних, управління з'єднанням, визначення швидкості передачі та встановлення топології мережі. На даному рівні здійснюються ось такі дії, як підключення до фізичного каналу, від'єднання від нього, та керування передачею даних та встановлення параметрів швидкості передачі. Також на фізичному рівні визначається структура мережі, яка може мати різні топології, такі як зірка, шина чи кільце.

На каналному рівні мережі відбувається додавання додаткових символів та контрольних даних до переданих масивів інформації. У локальній обчислювальній мережі (ЛОМ) передана інформація розбивається на пакети. Кожен пакет має адреси джерела та призначення, і також засоби для виявлення помилок. Це забезпечує надійну передачу даних та дозволяє виявити та виправити помилки, що виникли при передачі.

Мережевий рівень знаходить шляхи передачі інформації між мережами та комп'ютерами, створює обробку помилок та керування потоками даних. Головне завдання даного рівня полягає у маршрутизації даних, тобто передачі даних. Для цього застосовується спеціальні пристрої, які називаються маршрутизаторами. Маршрутизатори визначають, у яку мережу призначене кожне повідомлення.

Для ідентифікації вузла у мережі використовується адреса вузла. Задля того щоб визначити шлях передачі даних між мережами, на маршрутизаторах будуються таблиці маршрутів, які мають інформацію про послідовність маршрутів для передачі даних. Кожен запис у таблиці маршрутів має адресу кінцевої мережі та адресу наступного маршрутизатора та вартість передачі даних по даному маршруту.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		21

Для побудови таблиць маршрутів практично завжди застосовуються метод векторів чи статичний. При виборі оптимального маршруту застосовують динамічні чи статичні методи.

На мережевому рівні існує можливість використання одного з двох методів передачі пакетів:

1. На мережевому рівні використовується метод віртуальних з'єднань, який встановлює маршрут для повідомлення від відправника до отримувача за допомогою запиту на з'єднання. При позитивній відповіді отримувача на з'єднання, маршрут закріплюється для подальшого трафіку повідомлення. Кожному віртуальному каналу присвоюється свій номер, який використовується лише для інших пакетів того ж повідомлення. Пакети, які передаються через один віртуальний канал, мають скорочений заголовок та порядковим номером пакета, що відноситься до цього повідомлення.

2. На мережевому рівні може застосовуватись метод дейтаграм, коли кожен пакет чи частина повідомлення доставляється до адресата по різних маршрутах. Кожен пакет містить повний заголовок з адресою одержувача. Управління передачею пакетів по мережі здійснюється за допомогою датаграмної служби.

Транспортний рівень у мережі забезпечує взаємозв'язок між нижніми рівнями та верхніми, які виконують функції програмного забезпечення. Даний рівень відповідає за розподіл даних у мережі та уточнення адреси призначення. Він також здатен мультиплексувати передані повідомлення чи з'єднання. Мультиплексування повідомлень дозволяє передавати повідомлення одночасно по кільком лініях.

На даному сеансовому рівні відбувається управління сеансами зв'язку між двома користувачами. Даний рівень визначає початок та закінчення сеансу зв'язку. Він також визначає параметри сеансу зв'язку, такі як час та тривалість, і встановлює точки синхронізації для контролю та відновленню передачі даних.

На рівні ознайомлювання здійснюється керування та передавання даних у відповідній формі для користувачів програм. Даний рівень включає генерацію

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						22
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

та інтерпретацію взаємодії, кодування та декодування даних, включаючи компресію та декомпресію. На робочих станціях можуть використовуватися різні ОС, та кожна має свою власну файловою системою. Завданням даного рівня є перетворення даних у формат, що використовується в інформаційній системі, під час передачі інформації. При отриманні даних, рівень представлення виконується наоборот. Тому це дозволяє організувати обмін даними між ПК, на яких застосовується різні операційні системи.

Компресія або ж упаковка даних, дозволяє скоротити час передачі інформації. Кодування даної переданої інформації забезпечує захист від несанкціонованого доступу.

Прикладний рівень виконує управління мережевими програмами, обробку файлів, обчислювальні операції, пошук інформації, логічні перетворення та передачу поштових повідомлень. Мета цього рівня - надати зручний інтерфейс для користувача. Обмін даними на рівнях різних відбувається різними одиницями, такими як біти, кадри та пакети, сеансові повідомлення та користувальницькі повідомлення. Модель мережі полягає у розподілі ролей, включаючи транспортне середовище, щоб розбити передачі даних на окремі, зрозумілі завдання. Протоколи визначають угоди для зв'язку між рівнями.

Модель OSI визначає обмін між даними на різних рівнях з використанням різних одиниць інформації, таких як біти, кадри, пакети, та сеансові повідомлення і користувальницькі повідомлення. Кожен рівень виконує свою роль у передачі даних, та обробку транспортного середовища. Данна модель розводить загальну задачу передачі даних на окремі, зрозумілі завдання. Угоди, які потрібні для зв'язку між рівнями, називають протоколами. Ураховуючи ці принципи, можна утворити рівневу модель з адміністративними функціями, які виконуються на користувальницькому рівні.

У базовій моделі передачі даних, рівні працюють у двох напрямках: від даних ( рівень 7 до рівня 1 ) та від приймача даних ( рівень 1 до рівня 7 ).

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		23

Користувальницькі дані передаються у низ до нижче розташованих рівнів, поки не досягнуть останнього рівня.

Для передачі інформації по лініях дані перетворюються в послідовність бітів, які передаються послідовно. Це виконується шляхом двійкового кодування, де застосовується два стани "0" та "1". Алфавітно-цифрові символи, які потрібно передати, показуються в бітовій формі за допомогою відповідних бітових комбінацій. Дані бітові комбінації упорядковані у кодовій таблиці, де у кожного символу відповідає певна послідовність бітів. Кількість бітів, використаних у кодуванні, визначає кількість можливих символів, які з них можуть бути передані: наприклад, 4-бітовий код може представити максимум 16 символів, 5-бітовий - 32 символи, 6-бітовий - 64 символи, 7-бітовий - 128 символів і 8-бітовий код - 256 символів

У разі передачі інформації між різними обчислювальними системами застосовуються різні коди. У міжнародному рівні використовується 7-бітове кодування, що дозволяє передати заголовні та малі літери англійського алфавіту, а також спеціальні символи. Але, для передачі національних та спеціальних символів, які не можливо представити за допомогою 7-бітового коду, у цьому разі застосовується спеціальні методи шифрування чи перекодування інформації. Для представлення національних символів використовується 8-бітове кодування.

У разі передачі файлів дуже важливо, щоб обидва комп'ютери, що взаємодіють, погодилися на загальному протоколі.

Більшість протоколів передачі файлів мають вже вбудовані засоби для виявлення та виправлення помилок. Дані методи можуть відрізнитися для кожного протоколу. У разі передачі файлу він розбивається на менші блоки, відомі як пакети, та кожен пакет містить додатковий контрольний байт. Приймаючий комп'ютер порівнює отриманий пакет. Якщо значення не сходиться, тоді це свідчить про наявність помилки при передачі, і приймаючий комп'ютер запитує повторну передачу пакету даних.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		24



TCP/IP (Transmission Control Protocol/Internet Protocol) є найпопулярнішим та передовим протоколом, який забезпечує мережеву взаємодію пристроїв. Цей протокол є стандартом для Інтернету та широко використовується в більшості великих мереж.

Впровадження комутаторів дозволяє знизити до мінімуму кількість колізій у локальних мережах. Однак, у повністю комутованій мережі часто виникає проблема домену ширококомовної розсилки. У єдиному домені ширококомовної розсилки, всі пристрої розміщені у одній мережі та отримують усі ширококомовні розсилки. У разі використання єдиного домену ширококомовної розповсюдження є прийнятним для невеликих мереж. Але, у великих мережах плоска мережа не є дуже ефективною при збільшенні кількості вузлів. При збільшенні числа вузлів у комутованій мережі також зростає і кількість передаваних та отримуваних розсилок.

У великих плоских мережах, пакети ширококомовних розсилок можуть займати дуже велику частину пропускної здатності, що призводить до затримок в передачі трафіку і виникнення тайм-аутів. Одним із рішень для розв'язання даних проблем є використання віртуальних локальних мереж (VLAN). Мережа VLAN утворює окремий домен ширококомовної розсилки, даний домен обмежує та ізолює.

Ще одним рішенням подолання великих проблем плоских мереж є впровадження ієрархічної мережі з використанням маршрутизаторів. У великих корпоративних мережах використання ієрархічної моделі мережі та відповідної структури адрес дозволяє досягти великих переваг. Дана структура ієрархічної адресації розділяє мережі на менші підмережі. Доволі ефективна схема ієрархічної адресації включає у себе використання адреси класової мережі на центральному рівні, вона поділяється на менші підмережі на різних рівнях розподілу і доступу.

Ще іншим підходом є використання ієрархічної мережі без її адресації. Хоча мережа може продовжувати функціонувати, але її ефективність конструкції мережі значно знижується, а деякі функції протоколу

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						25
Зм.	Арк	№ докум.	Підпис	Дата		

маршрутизації, наприклад, підсумовування маршрутів, можуть працювати некоректно.

Існує ряд причин, які підтримують розділення мережі на підмережі:

1. Безпека.
2. Логічне групування.
3. Фізичне місце розташування.
4. Обмеження ширококомовної розсилки.

У проєкті локальної мережі було застосовано ієрархічний підхід задля поділу мережі на підмережі. Задля маршрутизації між сегментами мережі буде використаний комутатор третього рівня. У моделі OSI зображено класифікацію мережевих пристроїв на рисунку 2.2, де складність пристроїв залежить від їх обробки та передачі даних від верхніх до нижніх рівнів.



Рисунок 2.2 – Комутатор 3-го рівня моделі OSI

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						26
Зм.	Арк	№ докум.	Підпис	Дата		

## 2.2 Розробка схеми фізичного розташування кабелів та вузлів

Отже при проектуванні локальної мережі дуже важливо вибрати топологію, яка вже визначатиме структуру зв'язків між ПК. У випадку мереж Ethernet, які будуються з використанням фізичної топології "Розширена зірка", даний тип топології буде використовуватись при проектування мережі в компанії "ВебКатТехнік".

Переваги топології "Розширена зірка":

- У разі поломки окремих сегментів мережа працювати.
- Дуже просте встановлення та налаштування.
- Легкість адміністрування та моніторингу.
- Можливість логічного сегментування локальної мережі та контролю трафіку.
- Ціна

Недоліком топології "Розширена зірка" є невелика можливість зупинки роботи всієї мережі у разі поломки центрального комутатора. Але, цей недолік на теперішній момент при використанні сучасних комутаторів стає менш важливим. Так як сучасні комутатори мають хорошу надійність та доволі довгий термін гарантії.

Схему організації мережі з фізичною топологією "Розширена зірка" можна побачити на зображенні, яке наведено на рисунку 2.3.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						27
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

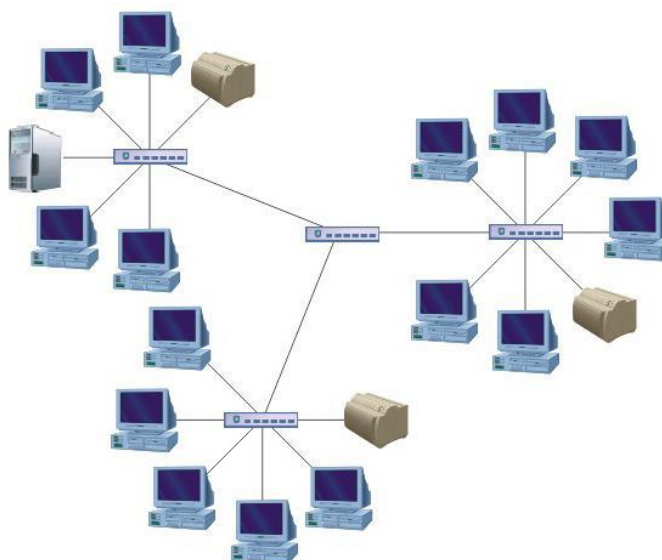


Рисунок 2.3 – Фізична топологія зірка




### 2.3 Обґрунтування вибору комунікаційного обладнання

У таблиці 2.3 показано порівняння технічних характеристик комутаторів, разом з переліком їх технічних характеристик та порівнянням.

Таблиця 2.3 – Порівняльна характеристика комутаторів

Підтримувані функції	HP V1910-24	TP-LINK TL-SG1024DE	Cisco 3750X48
1	2	3	4
К-сть портів 1000Base-TX	24	24	48
Швидкість комут., Гбіт/с	48	48	160
Підтримувані функції	L2+ (статична маршрутизація)	L2+ (статична маршрутизація)	L3+ (статична маршрутизація)
Підтримка базового набору протоколів канального рівня	+	+	+

Продовження таблиці 2.3




1	2	3	4
Підтримка технології IEEE 802.1Q	+	+	+
Моніторинг засобами SNMP	+	+	+
			

У проекті було використано комутатор HP V1910-24G, який має можливість статичної маршрутизації. Комутатор HP V1910-24G є пристроєм рівня L2 та має ось такі технічні характеристики, згідно документації [19]:

1. Об'єм оперативної пам'яті: 128 Мб.
2. Об'єм флеш-пам'яті: 128 Мб.
3. Консольний порт: присутній.
4. Підтримка стандартів: Auto MDI/MDIX, Jumbo Frame, IEEE 802.1p (Priority tags), IEEE 802.1q (VLAN), IEEE 802.1d (Spanning Tree), IEEE 802.1s (Multiple Spanning Tree), статична маршрутизація.
5. Кількість портів комутатора: 24 x Ethernet 10/100/1000 Мбіт/сек.
6. Внутрішня пропускна здатність: 48 Гбіт/сек.
7. Розміри (ШxВxГ): 440 x 44 x 260 мм.
8. Засоби керування: консольний порт, Telnet, SNMP.
9. Додаткова інформація: 4 Gigabit Ethernet SFP-порта.

У таблиці 2.4 було здійснено порівняння технічних характеристик 16-ти портових комутаторів.

Таблиця 2.4 – Комутатори робочих груп (16-ти портів)

	D-link DGS 1216T	TP-LINK TL- SG1016D	NETGEAR GS116GE
К-сть портів	16	16	16
Швидкість Мбіт/с	10/100/1000	10/100/1000	10/100/1000
Пропускна здатність, Гбіт/с	32	32	32
Керування	Web	Web	Web
Підтримка технології VLAN IEEE 802.1Q	+	+	+
			



Для робочих груп локальної мережі використано комутатор D-link DGS1216T [14].

Спільний доступ до мережі Інтернет буде організовано засобами апаратного маршрутизатора, вибір якого з посеред інших моделей наведено в таблиці 2.5.

Таблиця 2.5 – Вибір апаратного маршрутизатора

	Mikrotik RB/1100	Cisco C921-4P
К-сть WAN портів	2	2
К-сть LAN портів	10	4
Швидкість, Мбіт/с	10/100/1000	10/100/1000

Продовження таблиці 2.5

1	2	3
RAM	512MB (up to 1.5GB)	1GB
Керування	Web, CLI, WinBOX	Web, CLI
CPU	PowerPC MPC8544	2.2ГГц
ОС	MikroTik RouterOS v4, Level 6 license	Cisco IOS Software Release 15.8(3)Mb
		

Задля захисту локальної мережі було використано маршрутизатор MikroTik RB/1100 . Розглянемо уважно його технічні характеристики:

У пристрій включені тринадцять 10/100/1000 Mbit/s Gigabit Ethernet портів, та дві світч групи по 5 портів, є також можливість з'єднувальна декількох роутерів. У RB/1100 встановлена RouterOS 6-го покоління.

Характеристики:

1. Пам'ять: SoDIMM DDR слот, без вбудованого модуля, в комплекті поставляється модуль на 512MB, можлива встановка модуля до 1,5GB.
2. Процесор: MPC8544 800/1333MHz.
3. Завантажувач: RouterBOOT, 1Mbit Flash chip.
4. Диск даних на 512MB.
5. Вентеляція
6. Живлення 220V AC.
7. Операційна система: MikroTik RouterOS v3, ліцензія 6-го рівня.
8. Розміри: 45x75x440 мм.

У таблиці 2.6 наведено характеристики серверів різних фірм.

Таблиця 2.6 – Порівняння серверів

	DELL R530 LFF H730	HP ProLiant DL360 Gen9 SFF
Процесор	Intel Xeon E5-2609 v4	Intel Xeon E5-2609 v4
Об'єм ОЗП	16 Гб	16Гб
Тип ОЗП	DDR4-2400 МГц	DDR4-2400 МГц
Формфактор, висота	Rack, 1U	Rack, 1U
Дискова підсистема	2 x 1 ТБ Raid Edition + Intel DC S3500 Series SSD 600GB 2.5"	2 x 1 ТБ Raid Edition + Intel DC S3500 Series SSD 600GB 2.5"
БЖ	500 Вт	500 Вт
Мережева плата стандарту Gigabit Ethernet	інтегрована	інтегрована
Відеоадаптер	інтегрований	

Для підприємства буде використано модель сервера HP ProLiant DL360 Gen9.

Для побудови локальної мережі у ПП "ВебКатТехнік" використовано пасивне мережеве обладнання, яке включає в себе кабель неекранованої витії пари категорії 5е від фірмовиробника Харківкабель, патчпанель з 24 портами, що підтримує категорію 5е, комутаційну шафу об'ємом 24U, кабельні організатори і конектори RJ-45. Для монтажу коробів застосовується шурупи та дюбелі.

У таблиці 2.7 наведено повний перелік обладнання, для побудови локальної мережі.



Таблиця 2.7 – Мережеве обладнання

№ п/п	Назва елемента	Фірма виробник/Модель	Од. вим.	К-сть	Ціна, грн.	Сума, грн.
1	2	3	4	5	6	7
1	Кабель	Харківкабель/UTP	м	610	12	7320
2	Шуруп	-	шт	200	1.1	220
3	Дюбель	-	шт	200	1.2	240
4	Кабельний тримач	-	шт	4	200	800
5	Короб	-	м	90	70	6300
6	Роз'єми	RJ-45	шт	150	1.3	195
7	Керований комутатор	HP/V1910-24G	шт	1	11200	11200
8	Керований комутатор	D-link DGS-1216T	шт	2	3200	6400
9	Сервер	HP ProLiant DL360 Gen9 SFF	шт	1	29800	29800
10	Маршрутизатор	Mikrotik RB/1100	шт	1	8700	8700
11	Комутаційна шафа	24U	шт	1	8000	8000
12	Патчпанель	UTP 5e, 24 портів	шт	1	2000	2000
13	Патчпанель	UTP 5e, 16 портів	шт	2	1800	3600
Разом, грн.						84775

## 2.4 Особливості монтажу мережі

Основою структурованої кабельної системи являється екранована вита пара категорії 5e.

1. Мінімальний радіус вигину для чотирьохпарного кабелю повинен бути не менше 8-діаметрів при прокладці та не менше 4-діаметрів при експлуатації. Порушення даних вимог може призвести до пошкодження кабелю і погіршення його електричних характеристик. Якщо кабель має

										Арк
										33
Зм.	Арк	№ докум.	Підпис	Дата	<b>2023.КРБ.123.602.08.00.00 ПЗ</b>					

пошкодження через неправильний радіус вигину, рекомендується замінити його.

2. Максимальна довжина горизонтального кабелю обмежена значенням 90 метрів. У робочих зонах, а також для з'єднувальних кабелів і перемичок в телекомунікаційних шафах, можна використовувати кабель довжиною до 10 метрів.

3. Необхідно вирішити проблему надмірного навантаження на кабель, яке може виникнути через розтягнення чи неправильне прокладання кабелю. Для цього рекомендується усунути любе навантаження на кабель, забезпечивши достатню відстань між центрами опор у межах 110-150 см. Також потрібно обов'язково уникати скручування кабелю під час монтажу, оскільки це може призвести до деформації чи розриву кабелю.

4. Для чотирьохпарного горизонтального кабелю максимально допустиме розтягуюче зусилля становить 50 Н. Дуже важливо уникати розтягуючого навантаження під час монтажу, так як це може спричинити деформацію кабелю та погіршенню його електричних характеристик. Якщо кабель пошкоджений через сильне розтягуюче навантаження, його потрібно замінити.

Крім вищезазначених правил, рекомендується дотримуватись додаткових порад виробника щодо монтажу, які базуються на стандартах ISO/IEC 11801 та TIA/EIA-568:

1. Використання хамутів на липучці дозволяє доволі надійно закріпити кабель без пошкодження його.

2. Дотримуйтесь відстані не менше 20 см між кабелем і потенційними джерелами електромагнітних перешкод.

3. Уникайте попадання кабелю під вантажні візки чи навантажувачі, може спричинити поломку кабелю.

4. Утримуйтесь від використання звичайних скоб оскільки вони можуть тиснути на кабель та спричиняти деформацію пар проводів.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		34

Для побудови кабельної системи використовуватиметься екранована вита пара категорії 5е. Кабель буде прокладатися в коробках.

## **2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі**

Для файлового сервера використовується операційна система CentOS 8.1 x64 [15]. Дана система забезпечує функції аутентифікації користувачів мережі, надання доступу до файлів та її централізоване зберігання. Обрана операційна система повністю відповідає вимогам, які ставляться до серверної ОС.

Операційна система маршрутизатора забезпечує реалізацію наступних мережевих функцій:

- NAT;
- Динамічне керування потоками трафіку;
- Statefull Firewall.

Робочі станції застосовують операційні системи Windows 10 Professional і CentOS 8.1 x64.

## **2.6 Обґрунтування вибору засобів захисту мережі**

Маршрутизатор MikroTik з операційною системою RouterOS має вбудований брандмауер і механізми NAT, так вони забезпечують потужні можливості фільтрації пакетів, високоякісну реалізацію SNAT і DNAT, а також можливість класифікації пакетів згідно [21]:

- Діапазонах портів;
- По вмісту пакетів;
- Опціях протоколів (ICMP типам, TCP прапорам і MSS);
- Інтерфейсах;
- IP-адресах (можливість задання мереж);
- IP-протоколах;

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						35
Зм.	Арк	№ докум.	Підпис	Дата		

- МАС-адресі джерела;
- За розміром пакетів.

За техніко-економічними оцінками, використання даної вбудовано операційної системи маршрутизатора задля забезпечення захисту локальної мережі є раціональним рішенням.

## 2.7 Тестування та налагодження мережі

Налагоджувальні роботи будуть включати:

1. Підключення мережевого обладнання.
2. Налаштування IP-адрес вузлів локальної мережі.
3. Конфігурування комутатора.
4. Конфігурування сервера.
5. Конфігурування маршрутизатора.

Тестування локальної мережі буде передбачати такі етапи:

1. Перевірка кабельних сегментів на наявність дефектів використовуючи кабельний тестер.
2. Звірка стеків TCP/IP вузлів мережі згідно таблиці IP-адресації.
3. Перевірка доступності вузлів.
4. Перевірка конфігурації комутатора (створених підмереж).
5. Перевірка конфігурації файлового сервера (створених робочих груп та облікових записів користувачів).
6. Тестування пропускної здатності Інтернет-з'єднання.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		36

### 3. СПЕЦІАЛЬНИЙ РОЗДІЛ

#### 3.1 Інструкції з налаштування програмного забезпечення серверів

##### 3.1.1 Інструкція з налаштування файлового сервера

FTP (File Transfer Protocol) є доволі старим і вже стандартизованим для людей мережевим протоколом на простому рівні, призначеним для передачі файлів між людиною та сервером у мережі.

Основні можливості FTP включають в себе просту реєстрацію клієнтів, здійснюється за допомогою імені користувача та придуманого пароля.

Для забезпечення безпеки передачі даних, можна використовувати FTPS, який базується на протоколі SSL/TLS, чи SFTP, який є більш розширеним протоколом. Структуру протоколу FTP можна побачити на рисунку 3.1.

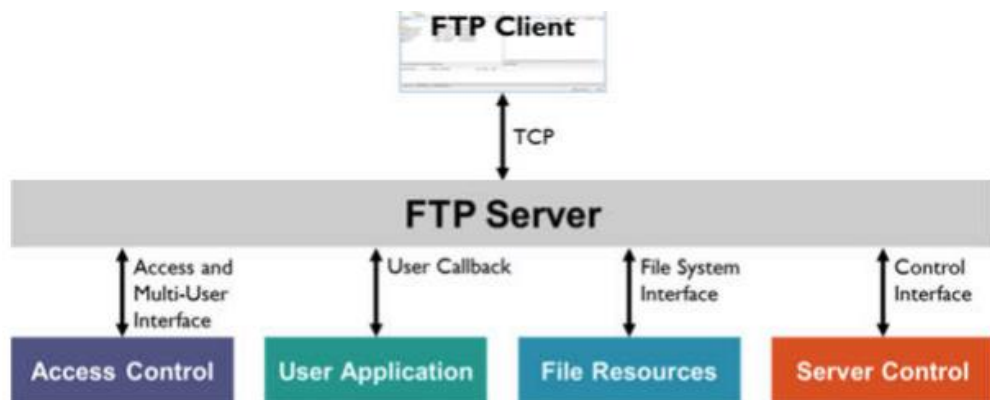


Рисунок 3.1 – Структура протоколу FTP

Перед тим як появиться у користувача графічний інтерфейс в операційних системах, FTP клієнт були розроблені з використанням командного рядка. Ці клієнти залишаються доволі актуальними й по сьогоднішній день, Та є складовою частиною сучасних ОС, таких як Windows,

UNIX та Linux. Після створення FTP було створено дуже багато різних версій FTP клієнтів, а підтримка протоколу була вбудована в різноманітні утиліти.

Vsftpd (Very Secure FTP Daemon) являється FTP сервером, призначеним для використання в Unix системах, включаючи Linux, з повною підтримкою IPv6 і SSL.

Далі прості вказівки по встановленню та налаштуванню vsftpd.

Встановлення на CentOS (Fedora, RHEL):

1. Перевіряємо чи ftp-сервер не є встановленим:

```
# rpm -q vsftpd# yum install vsftpd3.
```

2. Якщо він не встановлений, то встановлюємо:

```
# yum install vsftpd
```

3. Додаємо в автозагрузку:

```
# chkconfig vsftpd on
```

4. Запускаємо:

```
# service vsftpd start.
```

5. Знімаємо блокування фаєрволом:

```
system-config-firewall-tui
```

Заходимо в Customize і відкриваємо порт FTP.

Налаштування:

1. По стандарту, сервер має включену можливість анонімного доступу без паролю. Для використання даної функції достатньо ввести ім'я користувача "anonymous".

2. Якщо доступ анонімних користувачів є дозволений, тоді можна вимкнути запит пароля для анонімного підключення за допомогою опції:

```
no_anon_password=YES.
```

3. Доступ до локальних користувачів можна вмикати та вимикати опцією:

```
local_enable=YES/NO.
```

4. Задля того щоб локальні користувачі не могли заходити далі своїх домашніх каталогів, вмикаємо це обмеження:

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		38

chroot\_local\_user=YES.

5. Обмежуємо максимальну кількість підключень:  
max\_clients=xx, де xx являється кількістю.

6. Включаємо та виключаємо дозвіл на команди задля створення нових файлів:

write\_enable=YES/NO.

7. Включаємо та виключаємо дозвіл на команди створення нових каталогів анонімними користувачами:

anon\_mkdir\_write\_enable=YES/NO

8. Включаємо та виключаємо дозвіл на команди створення нових файлів анонімними користувачами:

anon\_other\_write\_enable=YES/NO.

9. Дозволяємо та забороняємо анонімам завантажувати нові файли:

anon\_upload\_enable=YES/NO.

Створюємо окремого користувача, для підключень:

1. Створюємо користувача:

```
# useradd ftpuser
```

2. Задаємо якийсь пароль:

```
# passwd ftpuser
```

При використанні систем, що підтримують SELinux, потрібно урахувати, що параметри можуть мати інші значення, незважаючи на те, що вони вказані в конфігураційному файлі.

Подивитись чи активовано SELinux:

```
# sestatus
```

У результаті виведення enforcing - означає примусовий режим, а permissive - режим попередження.

Подивитись список примусових SELinux параметрів:

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		39

# getsebool -a | grep ftp allow\_ftp\_anon\_write -> off - запис дозволений анонімним користувачам. allow\_ftp\_full\_access -> off – має повний доступ.

allow\_ftp\_use\_cifs -> off - дозволить розшарювати мережеві windows папки.

allow\_ftp\_use\_nfs -> off - дозволити розшарити NFS.

ftp\_home\_dir -> off - дозволити користувачам доступ до каталогів.

ftpd\_connect\_db -> off httpd\_enable\_ftp\_server -> off  
sftpd\_anon\_write -> off sftpd\_enable\_homedirs -> off  
sftpd\_full\_access -> off sftpd\_write\_ssh\_home -> off tftp\_anon\_write -> off

Змінити параметр SELinux: # setsebool -P ftp\_home\_dir on чи

# setsebool -P ftp\_home\_dir 1

(-P , зберегти налаштування після перезавантаження).

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

### **3.2.1 Інструкція з базового налаштування маршрутизатора**

Задля налаштування маршрутизатора потрібно установити з'єднання з ним за допомогою якоїсь утиліти наприклад WinBox. Після успішного з'єднання з маршрутизатором потрібно перейти до простих налаштувань параметрів з'єднання з провайдером. Дані дії можна зробити в меню IP, у підпункті Address, де потрібно налаштувати таблицю IP адрес. Це дозволить установити параметри зв'язку з провайдером для правильної маршрутизації усіх даних.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						40
Зм.	Арк	№ докум.	Підпис	Дата		



У пункті меню IP вибираємо підпункт Firewall, потім переходимо на закладку NAT. Тут ми уже можемо задати правила для спільного доступу до Інтернету. Одним із налаштувань є маскування адреси сегменту мережі з використанням технології NAT. Наприклад, якщо ми бажаємо замаскувати адресу 2-го сегменту мережі (10.10.2.0/24), то ми вказуємо дану адресу в налаштуваннях NAT. Це дозволить забезпечити доступ до інтернету для комп'ютерів у даному сегменті.

У наступному кроці переходимо у закладку Firewall та задаємо фільтрації для усієї мережі.

Правила фільтрації дозволяють проходження всіх пакетів, що належать до мережі 10.10.0.0/16 та є відповіддю на ініційовані з'єднання з користувачами локальної мережі. Пакети, які відповідають на ініційовані з'єднання, отримують статус Established чи Related від файрволу. Отже для цих пакетів застосовується дія підтвердження, яка дозволяє їм пройти через файрвол.

Черги для обмеження та пріорітизацію трафіку:

- Застосування різних обмежень по часу;
- Розподіл доступного трафіку порівну між користувачами чи в залежності від завантаження каналу;
- Налаштування вибухового режиму, проходу трафіку для прискорення веб-серфінгу;
- Обмеження пірінгового трафіку;
- Пріоретизація певних потоків пакетів над іншими.

Організація черг в MikroTik RouterOS має базу на використанні Hierarchical Token Bucket (НТВ, Буфер токенів). НТВ дає змогу створити ієрархічну структуру черг та встановити залежності між ними. У RouterOS ці ієрархічні структури можуть бути розміщені в 4 різних місцях:

- global-in: об'єднує у собі усі вхідні інтерфейси.
- global-total: об'єднує у собі усі вхідні та вихідні інтерфейси разом використовується лише тоді коли встановлене єдине обмеження.
- global-out: об'єднує в собі всі вихідні інтерфейси в цілому.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						41
Зм.	Арк	№ докум.	Підпис	Дата		

Існує лише два способи налаштування черг у RouterOS:

- Меню/queue simple - призначене для полегшення конфігурування у випадках простих повсякденних завдань.

- Меню/queue tree - для виконання розширених завдань.

Обмеження швидкості передачі використовується лише для контролю потоку трафіку, який надсилається чи отримується через мережевий інтерфейс. Ця функція дозволяє визначити максимальну швидкість для передачі даних і вплинути на трафік в залежності від його швидкості.

При умові якщо швидкість трафіку менше чи дорівнює заданому значенню, тоді він буде надісланий лише через мережевий інтерфейс. Однак, якщо швидкість трафіку перевищує задане значення, він може бути відкинутий чи тимчасово затриманий.

Обмеження швидкості передачі даних є інструментом для керування мережевим трафіком, забезпечення рівномірного розподілу пропускної здатності та запобігання перевантаженню мережі.

Обмеження швидкості передачі даних може бути виконано двома способами:

- Відкидаються всі пакети, що перевищують ліміт;
- Затримка перевищили ліміт швидкості передачі пакетів в черзі і відправка їх пізніше.

Для кожної черги ми маємо можливість поставити лише два обмеження швидкості передачі:

- CIR (Committed Information Rate) та гарантована смуга пропускання (limit-at в RouterOS) гарантує, що незалежно від любых обставин, включаючи самий гірший сценарій, коли вся доступна пропускна здатність використовується, потік трафіку буде мати стабільну передачу з своєю швидкістю.

- MIR (Maximum Information Rate) чи максимальна смуга пропускання (max-limit в RouterOS) визначає найбільшу швидкість передачі даних у потоці при ідеальних умовах.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						42
Зм.	Арк	№ докум.	Підпис	Дата		

Види черг чи алгоритми побудови черг описуює, який пакет буде відправлений наступним. RouterOS підтримує кілька алгоритмів побудови черг:

- BFIFO, PFIFO, MQ PFIFO ;
- RED;
- SFQ;
- PCQ.

PFIFO, BFIFO та MQ PFIFO - це алгоритми який керує чергою. Основна відмінність між PFIFO і BFIFO полягає у тому, що перший вимірюється в пакетах, а другий у байтах.

Кожен пакет, який не має можливості бути поміщений у чергу, буде відкинутий. Збільшення розміру черги може привести до збільшення затримок, але тим самим поліпшує використання пропускної здатності каналу. Для налаштування розміру застосовується параметри `pfifo-limit` і `bfifo-limit`. `mq-pfifo` є розширеною версією `pfifo` черги, яка підтримує декілька черг передачі. Даний тип черги корисний у системах SMP з Ethernet-інтерфейсами, які підтримують декілька черг.

RED (Random Early Detection) - це механізм який керує чергою, який спрямований на попередження мережевого перевантаження шляхом контролю середнього розміру черги. Середній розмір черги порівнюється з двома порогами: мінімальним і максимальним. Якщо середній розмір черги менше мінімального порогу, пакети не відкидаються. Коли середній розмір черги перевищує максимальний поріг, всі пакети відкидаються. Але, якщо значення середнього розміру черги знаходиться між мінімальним та максимальними порогами, пакети можуть відкидатися випадковим чином з ймовірністю  $P_d$ . Ця ймовірність залежить від середнього розміру черги за формулою:  $P_d = P_{max} * (avg\ q - min\ th) / (max\ th - minth)$ , де  $P_{max}$  - коефіцієнт, що регулює величину ймовірності відкидання пакетів (здебільшого  $P_{max} = 1$ ). Збільшення середнього розміру черги призводить до збільшення ймовірності відкидання вхідних пакетів.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						43
Зм.	Арк	№ докум.	Підпис	Дата		

SFQ (Stochastic Fairness Queuing) зазвичай за допомогою алгоритмів хешування і циклічного перебору. Потік трафіку може бути точно ідентифікований за чотирма характеристиками (src-address, dst-address, src-port та dst-port), тому дані параметри застосовуються алгоритмом SFQ задля класифікації пакетів в один з 1024 можливих підпотоків. Здебільшого алгоритм циклічного перебору перегруповує доступні смуги пропускання між усіма підпотоками, виділяючи на кожен цикл задану кількість байтів трафіку за для параметра sfq-allot.

SFQ (Stochastic Fairness Queuing) має слово "Stochastic" в даній назві, оскільки цей вид фактично не виділяє окрему чергу для кожного потоку. SFQ працює за алгоритмом, який розподіляє трафік між обмеженою кількістю черг, застосовуючи алгоритм хешування.

PCQ (Per Connection Queuing) є її спеціальним варіантом SFQ та має свої особливості. Можна вибрати ідентифікатори потоків (за допомогою dst-address, dst-port, src-address, src-port).

За дією параметра rcq-rate, можна встановити обмеження швидкості для усіх підпотоків. Якщо rcq-rate = 0, доступний трафік буде розподілятися рівномірно між усіма підпотоками.

### 3.2.2 Інструкції з базового налаштування центрального комутатора

Описано послідовність усіх команд, які потрібні для конфігурування комутатора 2 рівня фірми HP V1910. Дані дії команд має розбити ширококомовний домен мережі на підмережі та зєднати їх. Також потрібно надати маршрут за замовчуванням, який має указувати на маршрутизатор. На рисунку 3.2 наведено приклад використання віртуальних мереж.

Переходимо у привілейований режим роботи маршрутизатора:  
SW\_3>enable

Очищаємо файл від решти налаштувань: SW\_3#erase startup-config

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						44
Зм.	Арк	№ докум.	Підпис	Дата		

Configuration will be deleted and device rebooted, continue [y/n]? Y

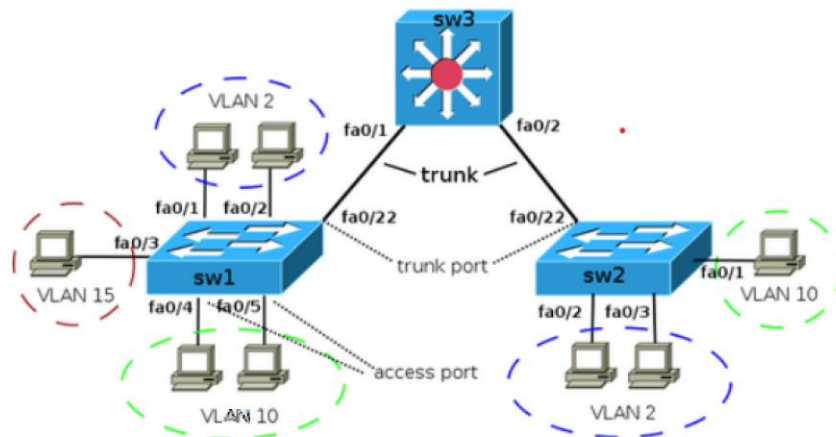


Рисунок 3.2 – Використання технології віртуальних мереж

Переходимо в режим конфігурування:

```
SW_3#conf t
```

```
SW_3 (config)#
```

Створюємо 11 сегментів локальної мережі:

1. Сегмент мережі 10.10.1.0/24
2. Сегмент мережі 10.10.2.0/24
3. Сегмент мережі 10.10.3.0/24
4. Сегмент мережі 10.10.4.0/24
5. Сегмент мережі 10.10.5.0/24
6. Сегмент мережі 10.10.6.0/24
7. Сегмент мережі 10.10.7.0/24
8. Сегмент мережі 10.10.8.0/24
9. Сегмент мережі 10.10.9.0/24
10. Сегмент мережі 10.10.10.0/24
11. Сегмент мережі 10.10.11.0/24

```
SW_3 (config)#vlan 101, SW_3 (config)#vlan 102, SW_3 (config)#vlan 103,  
SW_3 (config)#vlan 104, SW_3 (config)#vlan 105 SW_3, (config)#vlan 106, SW_3
```

(config)#vlan 107, SW\_3 (config)#vlan 108, SW\_3 (config)#vlan 109, SW\_3 (config)#vlan 110, SW\_3 (config)#vlan 111.

Включаємо маршрутизацію між ними: SW\_3 (config)#ip routing  
Задаємо маршрут за замовчуванням на маршрутизатор Mikrotik з адресою 10.10.11.2/24:

```
SW_3 (config)#ip route 0.0.0.0/0 10.10.11.2
```

Задамо ім'я кожній підмережі та IP адресу, вказуємо також порти комутатора, які входять у vlan:

```
SW_3 (config)#vlan111
```

```
SW_3 (vlan-111)#name subnet11
```

```
SW_3 (vlan-111)#ip address 10.10.11.0/24
```

```
SW_3 (vlan-111)#untaged 1,2
```

Виконаємо настройки які описані вище для усіх інших сегментів:

```
SW_3 (config)#vlan101
```

```
SW_3 (vlan-101)#name subnet1
```

```
SW_3 (vlan-101)#ip address 10.10.1.0/24
```

```
SW_3 (vlan-101)#tagged 3
```

```
SW_3 (config)#vlan102
```

```
SW_3 (vlan-102)#name subnet2
```

```
SW_3 (vlan-102)#ip address 10.10.2.0/24
```

```
SW_3 (vlan-102)#tagged 3
```

```
SW_3 (config)#vlan103
```

```
SW_3 (vlan-103)#name subnet3
```

```
SW_3 (vlan-103)#ip address 10.10.3.0/24
```

```
SW_3 (vlan-103)#tagged 3
```

```
SW_3 (config)#vlan104
```

```
SW_3 (vlan-104)#name subnet4
```

```
SW_3 (vlan-104)#ip address 10.10.4.0/24
```

```
SW_3 (vlan-104)#tagged 4
```

```
SW_3 (config)#vlan105
```

```
SW_3 (vlan-105)#name subnet5
```

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		46

```

SW_3 (vlan-105)#ip address 10.10.5.0/24
SW_3 (vlan-105)#tagged 4
SW_3 (config)#vlan106
SW_3 (vlan-106)#name subnet6
SW_3 (vlan-106)#ip address 10.10.6.0/24
SW_3 (vlan-106)#untagged 5,6,7,8
SW_3 (config)#vlan107
SW_3 (vlan-107)#name subnet7
SW_3 (vlan-107)#ip address 10.10.7.0/24
SW_3 (vlan-107)#untagged 9,10,11,12,13
SW_3 (config)#vlan108
SW_3 (vlan-108)#name subnet8
SW_3 (vlan-108)#ip address 10.10.8.0/24
SW_3 (vlan-108)#untagged 14
SW_3 (config)#vlan109
SW_3 (vlan-109)#name subnet9
SW_3 (vlan-109)#ip address 10.10.9.0/24
SW_3 (vlan-109)#untagged 15
SW_3 (config)#vlan110
SW_3 (vlan-110)#name subnet10
SW_3 (vlan-110)#ip address 10.10.10.0/24
SW_3 (vlan-110)#untagged 16

```

На комутаторах робочих груп SW\_1 та SW\_2 створюємо відповідно мережі vlan101, vlan102, vlan103, vlan104, vlan105, vlan106, vlan107, vlan108, vlan109, vlan 110 та указуємо, які порти до них належать. Також необхідно задати транкові порти.

Після конфігурування мереж перевіряємо їх працездатність командою ping.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		47

### 3.2.3 Інструкції з налаштування комутаторів робочих груп

На комутаторах sw1, sw2 потрібно нам налаштувати мережі згідно таблиці 2.2 «Таблиця конфігурування VLAN». У якості комутаторів використано модель D-link DGS-1216T.

Для налаштування мережі потрібно у пункті меню Configuration вибрати 802.1Q VLAN. У даному розділі потрібно вибрати команду Add VID та вказати номер VLAN, його назву та відмітити порти, які будуть входити у VLAN і до яких будуть підключатися робочі станції у режимі Untagged. У кожній з створених VLAN потрібно відмітити один із портів в режимі Trunk.

Режим Trunk дасть можливість мітити пакети спеціальними помітками, які будуть вказувати приналежність пакету до групи. Даний підхід є простим, оскільки не потрібно нічого фізично перекомутувати, а лише сконфігурувати правильно мережеве обладнання.

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

Технологію тестування мережі можна розділити лише на 2 етапи. Перший етап полягає у фізичному тестуванні з'єднань, а другий етап полягає у простому тестуванні протоколів ОС.

Для фізичного тестування з'єднань провідних сегментів використовується кабельний тестер. Кабельний тестер дозволяє перевірити кабель на повну справність та визначити його технічні характеристики, які є дуже важливими для високих швидкостей, наприклад Gigabit Ethernet

Для програмного тестування зв'язку можна використати різні утиліти ОС. Для тестування параметрів безпроводних сегментів мережі використовується безкоштовно програма NetStumbler. За допомогою даної програми можна зібрати корисні дані про безпроводну мережу та вирішити деякі проблеми, які з її експлуатацією. Перш за все, NetStumbler дозволяє нам визначити радіус дії

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						48
Зм.	Арк	№ докум.	Підпис	Дата		



мережі у реальному часі на діаграмі можна побачити величину. Дана функція програми допоможе точно направити антену для зв'язку на далекі відстані.

### 3.4 Інструкції по налаштуванню засобів захисту мережі

Захист локальної комп'ютерної мережі - це довгий процес, який має такі етапи:

1. Захист сервісів локальної мережі.
2. Захист від несанкціонованого доступу активного комутаційного обладнання.
3. Захист периметру локальної мережі з боку мережі Інтернет.

Захист локальної мережі відбувається з використанням ОС Mikrotik. ОС Mikrotik побудована на базі Linux. Для захисту даної локальної мережі буде використано програмний файрвол типу Statefull. В локальну мережу дозволено лише трафік, який є відповіддю на запити від людей локальної мережі. Більш детально налаштування ОС апаратного маршрутизатора описана в розділі 3.1.2.

Під час налаштування файлового сервера було ураховано вимоги до конфіденційності зберігання даних користувачів. На файловому сервері буде зберігатися уся база даних користувачів. Усі користувачі будуть мати доступ до спільної мережевої папки. Також передбачено зберігання даних на сервері для окремих користувачів, які мають логін та пароль. Більш детально налаштування файлового сервера описано в розділі 3.1.1.

Опишемо більш детальніше налаштування облікових записів користувачів на центральному комутаторі.

Базові настройки по захисту доступу до комутатора передбачають, такі як, настройку паролів для рівня менеджера і оператора.

Синтаксис команди для задання паролів:

пароль <manager|operator|all|port-access> [ім'я користувача<name>][<hash-type><password>]

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						49
Зм.	Арк	№ докум.	Підпис	Дата		

Параметри команди:

1. Manager - вказує, що будуть задаватися параметри для спеціального рівня доступу менеджер.
2. Operator - вказує, що будуть задаватися параметри для спеціального рівня доступу оператор.
3. All - вказує, що будуть задаватися параметри для менеджера та оператора.
4. Port-access - задання пароля оператора для аутентифікації по стандарту 802.1X.
5. User name - задання імені користувача.
6. Hash type - вказує який алгоритм використовується для хешування паролю: текст, sha1.

Налаштування пароля на режим менеджера:

```
sw(config)# password manager
```

```
New password for Manager: *****
```

```
Please retype new password for Manager: *****
```

Розглянемо правила для захисту роутера:

```
/ip firewall filter
```

```
add action=accept chain=input comment="default configuration" connection-  
state=established,related
```

```
add action=accept chain=input src-address-list=allowed_to_router
```

```
add action=accept chain=input protocol=icmp
```

```
add action=drop chain=input
```

```
/ip firewall address-list
```

```
add address=10.10.0.1-10.10.254.254 list=allowed_to_router
```

Блокування підозрілих пакетів на основі IP:

```
/ip firewall address-list
```

```
add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
```

```
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
```

```
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
```

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						50
Зм.	Арк	№ докум.	Підпис	Дата		

```

add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]"
list=not_in_internet

```

Пересилка пакетів через роутер:

```
/ip firewall filter
```

```
add action=fasttrack-connection chain=forward comment=FastTrack
connection state=established,related
```

```
add action=accept chain=forward comment="Established, Related" connection-
state=established,related
```

```
add action=drop chain=forward comment="Drop invalid" connection-
state=invalid log=yes log-prefix=invalid
```

```
add action=drop chain=forward comment="Drop tries to reach not public
addresses
```

```
from LAN" dst-address-list=not_in_internet in-interface=bridge1 log=yes log-
prefix=!public_from_LAN out-interface=!bridge1
```

```
add action=drop chain=forward comment="Drop incoming packets that are not
NAT`ted" connection-nat-state=!dstnat connection-state=new in
interface=ether1
```

```
log=yes log-prefix=!NAT
```

```
add action=jump chain=forward protocol=icmp jump-target=icmp
comment="jump to ICMP filters"
```

```
add action=drop chain=forward comment="Drop incoming from internet
which is not
```

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		51

```
public IP" in-interface=ether1 log=yes log-prefix=!public src-address-  
list=not_in_internet
```

```
add action=drop chain=forward comment="Drop packets from LAN that do  
not have
```

```
LAN IP" in-interface=bridge1 log=yes log-prefix=LAN_!LAN src-  
address=!10.10.0.0/16
```

### 3.5 Інструкції з експлуатації та моніторингу в мережі

Для експлуатації локальної мережі необхідними, є наступні види документів: логічна топологія, фізична топологія, план приміщення, таблиця IP-адрес.

У процесі експлуатації мережі з часом буде потреба в приєднанні нових користувачів. Для кожної робочої групи при розробці мережі було впроваджено резервні точки підключення клієнтів.

Моніторинг процесів в мережі є важливим аспектом у її експлуатації.

Моніторинг мережевих процесів буде передбачати:

1. Моніторинг роботи файлового сервера.
2. Моніторинг роботи маршрутизатора.
3. Моніторинг роботи головного комутатора засобами ОС комутатора.

Для моніторингу центрального комутатора потрібно на ньому сконфігурувати SNMP.

Налаштування виробляємо в такій послідовності. Створюємо комюніті спочатку на read, потім на write

```
#create snmp community name1 view CommunityView read_only
```

```
#create snmp community name2 view CommunityView write_only
```

CommunityView - ім'я має відрізняється від community name1 name2

```
#create snmp community public view CommunityView read_only
```

```
#create snmp host xxxx v2c public
```

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						52
Зм.	Арк	№ докум.	Підпис	Дата		

Вказуємо адресу сервера прийому trap ів. Тут xx.xx.xx.xx IP адреса сервера, public комюніті . У реальній конфігурації комюніті необхідно задати своє. Задля того, щоб повідомлення не відправлялися з інтерфейсів які потрібно виключити з числа контрольованих, на такому інтерфейсі необхідно застосувати конфігурацію:

```
#config snmp link_traps ports 01-24 disable
```

```
#config snmp link_traps ports 25-26 enable
```

Тут вимикається контроль і відправка traps при зміні стану портів 1-24 і включається для портів 25-26

Перевірити параметри відправки snmp traps можна командами:

```
#show snmp traps
```

```
Command: show snmp traps
```

```
SNMP Trap: Enabled
```

```
Authenticate Traps: Enabled
```

```
Link Traps: Enabled
```

Перевірити відправку з портів можна командою:

```
#show snmp traps link_traps
```

```
Command: show snmp traps link_traps
```

```
Link Traps: Enabled
```

```
Port 1: Disabled Port 2: Disabled
```

```
...
```

```
Port 23: Disabled
```

```
Port 24: Disabled
```

```
Port 25: Enabled Port 26: Enabled
```

Доповнивши команду можна подивитися налаштування відправки traps для конкретного порту:

```
#show snmp traps link_traps ports 25-26
```

```
Command: show snmp traps link_traps ports 25-26
```

```
Link Traps: Enabled
```

```
Port 25: Enabled
```

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						53
Зм.	Арк	№ докум.	Підпис	Дата		

Port 26: Enabled

Для обробки та візуалізації трапів буде впроваджено службу моніторингу Zabbix, яка фізично буде працювати на файловому сервері.

Zabbix - вільна система моніторингу і відстеження статусів різноманітних сервісів комп'ютерної мережі, серверів і мережевого устаткування [16].

Для зберігання даних використовується MySQL, PostgreSQL, SQLite чи Oracle.

Zabbix підтримує кілька видів моніторингу:

- Simple checks - може перевіряти доступність і реакцію стандартних сервісів, таких як SMTP чи HTTP;
- External check - виконання зовнішніх програм. ZABBIX а також підтримує моніторинг через SNMP;
- ZABBIX agent - може бути встановлений на UNIX-подібних чи Windows хостах для отримання даних про навантаження процесора.

Zabbix сервер - це ядро його забезпечення Zabbix. Сервер може віддалено перевіряти мережеві сервіси, та є сховищем, у якому зберігаються усі конфігураційні, статистичні та оперативні дані, та він являється тим суб'єктом в програмному забезпеченні Zabbix, який сповістить адміністраторів у разі виникнення проблем з будь яким контрольованим обладнанням.

Zabbix-проксі - збирає дані про продуктивність і доступність. Усі зібрані дані заносяться у буфер на локальному рівні та передаються на Zabbix сервера, до якого належить проксі сервер. Zabbix проксі є ідеальним рішенням для централізованого віддаленого моніторингу місць, мереж, які не мають локальних адміністраторів. Він може бути також використаний для розподілу навантаження одного Zabbix сервера.

Zabbix агент - контроль локальних ресурсів та додатків. На мережевих системах, ці системи повинні працювати з запущеним Zabbix агентом.

Веб інтерфейс - інтерфейс є частиною Zabbix сервера, і як правило запущений на тому ж фізичному сервері, що і Zabbix сервер.

Огляд можливостей:

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						54
Зм.	Арк	№ докум.	Підпис	Дата		

1. Розподілений моніторинг аж до 1000 вузлів. Конфігурація молодших вузлів повністю контролюється старшими вузлами.
2. Сценарії на основі моніторингу.
3. Централізований моніторинг файлів статистики.
4. Веб-інтерфейс для адміністрування і настройки.
5. Звітність і тенденції.
6. Підтримка високопродуктивних агентів практично для усіх платформ.
7. Комплексна реакція на події.
8. Підтримка SNMP v1, 2, 3.
9. Підтримка IPMI
10. Гнучка система шаблонів і груп.
11. Можливість створювати карти мереж.
12. Розширення за рахунок виконання зовнішніх скриптів.
13. Підтримка виконання запитів в різні бази даних.
14. Комплексна реакція на події.
15. SLA моніторинг.

### 3.6 Моделювання роботи локальної мережі

Виконуємо моделювання процесу роботи локальної мережі ПП «ВебКатТехнік» в програмі Cisco Packet Tracer. Метою даного моделювання має бути перевірка з'єднання між центральним комутатором SW\_3 та маршрутизатором R\_1. На рисунку 3.3 наведено логічну топологію ПП «ВебКатТехнік».

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		55

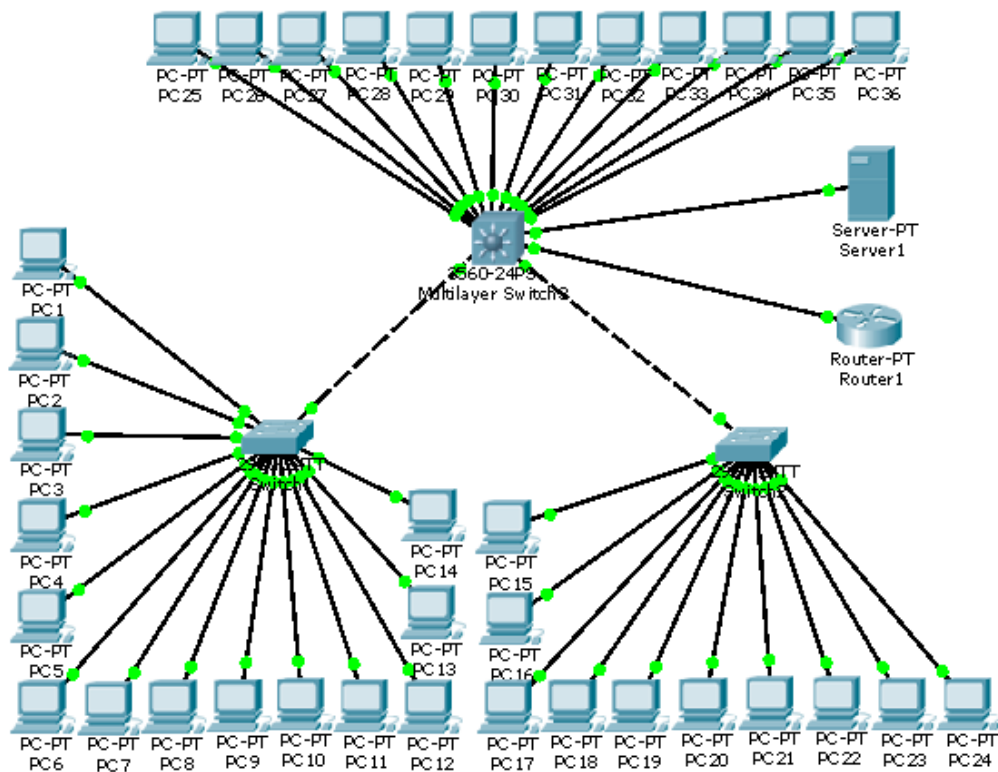


Рисунок 3.3 - Змодельована логічна топологія локальної мережі

Для початку потрібно сконфігурувати дані вузли локальної мережі.

Задля конфігурування маршрутизатора R\_1 потрібно виконати:

```
Continue with configuration dialog? [yes/no]: no
```

```
Press RETURN to get started!
```

```
Router>
```

```
Router>enable
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#hostname R1
```

```
R1(config)#interface fastethernet 0/0
```

```
R1(config-if)#ip address 10.10.11.2 255.255.255.0
```

```
R1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```



%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,  
changed state to up

R1(config-if)#

%SYS-5-CONFIG\_I: Configured from console by console

Застосовуючи дані таблиці IP-адрес вузлів локальної мережі створюємо головний комутатор. Задля перевірки зв'язку з головним комутатором і маршрутизатором, застосовуємо команду ping з маршрутизатора на IP-адресу комутатора:

R1#ping 10.10.12.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/23/32 ms

Даними діями можна зробити висновок щодо правильності сконфігурованого мережевого обладнання.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						57
Зм.	Арк	№ докум.	Підпис	Дата		

## 4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для офісної будівлі ПП «ВебКатТехнік» і прийняття рішення про її подальше впровадження в роботу.

### 4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР дані витрат часу по окремих операціях технологічного процесу зводяться у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва стадії	Виконавець	Середній час виконання операції, год.
1	Постановка задачі та збір інформації про об'єкт	Керівник проекту	10
2	Розробка проекту	Інженер	10
3	Монтаж мережі	Технік	30
4	Налагодження мережі	Інженер	20
5	Підготовка документації.	Інженер	8
Разом			78

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для офісної будівлі ПП «ВебКатТехнік» складає 78 годин.

#### 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 керівником підприємства найманому працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів його роботи, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою:

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

де  $T_c$  – тарифна ставка, грн.;

$K_z$  – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 74 грн./год., інженер – 60 грн./год., технік – 57 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту -  $Z_{осн1} = 10 \cdot 74 = 740$  грн.
2. Інженер -  $Z_{осн2} = 48 \cdot 60 = 2880$  грн.
3. Технік -  $Z_{осн3} = 20 \cdot 57 = 1140$  грн.

Сумарна основна заробітна плата становить:

$$Z_{осн} = 740 + 1140 + 2880 = 4760,00 \text{ грн.}$$

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

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

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						59
Зм.	Арк	№ докум.	Підпис	Дата		

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту -  $Z_{\text{доп1}} = 740,00 \cdot 0,15 = 111$  грн.
2. Інженер -  $Z_{\text{доп2}} = 2880,00 \cdot 0,15 = 432,00$  грн.
3. Технік -  $Z_{\text{доп3}} = 1140,00 \cdot 0,15 = 171,00$  грн.

Загальна додаткова заробітна плата становить:

$$Z_{\text{доп}} = 111,00 + 432,00 + 171,00 = 714,00 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

$$V_{\text{о.п.}} = Z_{\text{осн.}} + Z_{\text{доп.}}, \quad (4.3)$$

$$V_{\text{о.п.}} = 4760,00 + 714,00 = 5474,00 \text{ грн}$$

Необхідно визначити відрахування на соціальні заходи:

1. Фонд страхування на випадок безробіття – 1,6 %;
2. Фонд по тимчасовій втраті працездатності – 1,4 %;
3. Пенсійний фонд – 33,2 %;
4. Внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$V_{\text{с.з.}} = \text{ФОП} \cdot 0,376, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$V_{\text{с.з.}} = 5474,00 \cdot 0,376 = 2058,22 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						60
Зм.	Арк	№ докум.	Підпис	Дата		

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія прац.	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	74	10	740,00	111,00	-	-
2	Інженер	60	48	2880,00	432,00	-	-
3	Технік	57	20	1140,00	171,00	-	-
Разом				4760,00	714,00	2058,22	7532,22

Отже, загальні витрати на оплату праці становлять 7532,22грн.

### 4.3 Розрахунок матеріальних витрат

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

$$M_{Vi} = q_i \cdot p_i \quad (4.5)$$

де  $q_i$  – кількість витраченого матеріалу  $i$ -го виду;

$p_i$  – ціна матеріалу  $i$ -го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$Z_{м.в.} = \sum M_{Vi} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						61
Зм.	Арк	№ докум.	Підпис	Дата		

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Назва елемента	Фірма виробник/Модель	Од. вим.	К-сть	Ціна, грн.	Сума, грн.
1	2	3	4	5	6	7
1	Кабель	Харківкабель/UTP	м	610	12	7320
2	Шуруп	-	шт	200	1.1	220
3	Дюбель	-	шт	200	1.2	240
4	Кабельний тримач	-	шт	4	200	800
5	Короб	-	м	90	70	6300
6	Роз'єми	RJ-45	шт	150	1.3	195
7	Керований комутатор	HP/V1910-24G	шт	1	11200	11200
8	Керований комутатор	D-link DGS-1216T	шт	2	3200	6400
9	Сервер	HP ProLiant DL360 Gen9 SFF	шт	1	29800	29800
10	Маршрутизатор	Mikrotik RB/1100	шт	1	8700	8700
11	Комутаційна шафа	24U	шт	1	8000	8000
12	Патчпанель	UTP 5e, 24 портів	шт	1	2000	2000
13	Патчпанель	UTP 5e, 16 портів	шт	2	1800	3600
Разом, грн.						84775

Загальна сума матеріальних витрат на розробку мережі становить 84775.00 грн.

#### 4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

$$Z_e = W \cdot T \cdot S \quad (4.7)$$

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		62

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 – 1,68 грн.

Тому витрати на електроенергію будуть становити:

$$Z_e = 0,5 \cdot 10 \cdot 1,68 = 8,40 \text{ грн.}$$

#### 4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8 – 10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

$$T_e = Z_{м.в.} \cdot 0,08 \dots 0,1, \quad (4.8)$$

де  $T_e$  – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$T_e = 84775,00 \cdot 0,08 = 6782,00 \text{ грн.}$$

#### 4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімумально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{B_B \cdot H_A}{150\%} \cdot T, \quad (4.9)$$

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						63
Зм.	Арк	№ докум.	Підпис	Дата		

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

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

$H_A$  – норма амортизації, %;

$T$  – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК – 16500 грн., тому:

$$A = \frac{16500 \cdot 0,05}{150} \cdot 10 = 82,50 \text{ грн.}$$

#### 4.7 Обчислення накладних витрат

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

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$H_6 = B_{o.n.} \cdot 0,2 \dots 0,6, \quad (4.10)$$

де,  $H_6$  – накладні витрати.

$$H_6 = 7532,22 \cdot 0,3 = 2259,66 \text{ грн.}$$

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		64



#### 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.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	4760,00	4,78
Відрахування на соціальні заходи	714,00	0,71
Матеріальні витрати	84775,00	85,30
Витрати на електроенергію	8,40	0,01
Транспортні витрати	6782,00	6,82
Амортизаційні відрахування	82,50	0,08
Накладні витрати	2259,66	2,27
Собівартість	99381,56	100,00

Собівартість ( $C_B$ ) НДР розраховуємо за формулою 4.11:

$$C_B = B_{o.n.} + B_{c.z.} + Z_{m.v.} + Z_B + T_B + A + H_B \quad (4.11)$$

Отже, собівартість дорівнює:  $C_B = 99381,56$  грн.

#### 4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

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

де  $C_v$  – собівартість виконання НДР;

$P_{рен.}$  – рівень рентабельності, 30 %

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

$$\mathcal{C} = 99381,56 \cdot (1+0,3) \cdot (1+0,2) = 167954,83 \text{ грн.}$$

#### 4.10 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:

$$\mathcal{P} = \mathcal{C} - C_v \quad (4.13)$$

$$\mathcal{P} = 167954,83 - 99381,56 = 68573,27 \text{ грн.}$$

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

$$E_p = \mathcal{P} / C_v, \quad (4.14)$$

де  $\mathcal{P}$  – прибуток;

$C_v$  – собівартість.

$$E_p = 68573,27 / 99381,56 = 0,68$$

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

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

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						66
Зм.	Арк	№ докум.	Підпис	Дата		

Допустимим вважається термін окупності до 5 років. В даному випадку  $T_p=1/0,68=1,47$ .

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	99381,56 грн.
2.	Плановий прибуток, грн.	68573,27грн.
3.	Ціна, грн.	167954,83
4.	Економічна ефективність	0,68
5.	Термін окупності, рік	1,47

Загальна вартість розробленої комп'ютерної мережі для офісної будівлі ПП «ВебКатТехнік» становить 167954,83грн.

Зважаючи на високі показники економічної ефективності - 0,68, кошти, вкладені в проведення проектних робіт окупляться за 1,47року.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						67
Зм.	Арк	№ докум.	Підпис	Дата		

## **5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ**

Охорона праці є комплексною системою, що включає правові, соціально-економічні, організаційно-технічні, санітарно-гігієнічні та лікувально-профілактичні заходи та засоби, спрямовані на збереження життя, здоров'я та працездатності людей під час їх трудової діяльності.

Охорона праці, як соціально-технічна дисципліна, досліджує теоретичні та практичні аспекти забезпечення безпеки праці, запобігання виробничому травматизму, професійним захворюванням і отруєнням, аваріям, пожежам і вибухам на робочих місцях. Її метою є навчання майбутніх фахівців необхідним знанням і навичкам у сфері правових і організаційних аспектів охорони та гігієни праці, виробничої санітарії, техніки безпеки, а також розвиток активної позиції щодо практичної реалізації головного принципу Конституції України - пріоритетності охорони життя та здоров'я працівників порівняно з результатами виробничої діяльності.

### **5.1 Основні травми і професійні захворювання користувачів комп'ютерних та інформаційних технологій.**

Виробнича травма виникає внаслідок впливу різних небезпечних виробничих факторів на організм. Найбільш поширеним є механічний вплив, що може виникнути внаслідок зіткнень або контакту з механічним обладнанням.

Травмування можливо внаслідок дій:

- хімічних чинників, наприклад, отрутохімікатів, у вигляді отруень або опіків;
- електричного струму – опіки, електричні удари та ін.;
- високої або низької температури (опіки або обмороження);
- поєднання різних факторів

Розрізняють декілька причин виробничого травматизму:

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		68

1. Технічні, що виникають внаслідок конструкторських недоліків, несправностей машин, механізмів, недосконалість технологічного процесу, недостатньої механізації та автоматизації важких і шкідливих робіт.

2. Санітарно-гігієнічні, пов'язані з порушенням вимог санітарних норм відсутністю санітарно-побутових приміщень і пристроїв, недоліками в організації робочого місця та ін.

3. Організаційні, пов'язані з порушенням правил експлуатації транспорту і обладнання, поганою організацією вантажно-розвантажувальних робіт, через порушення режиму праці та відпочинку порушенням правил техніки безпеки, несвоєчасним інструктажем, відсутністю попереджувальних написів.

4. Психофізіологічні, пов'язані з порушенням працівниками трудової дисципліни, сп'янінням на робочому місці, перевтомою, поганим здоров'ям і ін.

5. Професійне захворювання – захворювання, яке виникло внаслідок професійної діяльності застрахованого та зумовлено виключно або переважно тривалим впливом шкідливих речовин, певних видів робіт та інших факторів, пов'язаних з роботою.

Список професійних захворювань ділиться на сім основних груп:

1. Захворювання, що зумовлені гострим впливом хімічних факторів. До цього пункту належать хронічні отруєння та їх наслідки, самостійні чи в поєднанні з іншими ураженнями: анемією, нефропатією, гепатитом, ураженням очей, кісток, нервової системи, органів дихання токсичного характеру. Сюди ж відносять хвороби шкіри, металеву лихоманку тощо.

2. Захворювання, що виникли через вплив промислових аерозолів. Це різні пневмоконіози, професійні бронхіти, бісиноз, емфізема легенів, дистрофічні зміни верхніх дихальних шляхів.

3. Хвороби, що виникли в результаті впливу фізичних факторів. Очолює цей список променева хвороба і променеві ураження в гострих і хронічних стадіях, розлади вегетосудинної системи, ангіоневроз. Сюди ж

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						69
Зм.	Арк	№ докум.	Підпис	Дата		

належать електроофтальмія, вібраційна хвороба, нейросенсорна приглухуватість, катаракта, кесонна хвороба, перегріву, механічні епідермози, опіки і поразки лазерним випромінюванням.

4. Захворювання, що виникли в результаті фізичних перевантажень та окремих перенапружень систем і органів тіла. У цьому списку — координаторні неврози, полі- і мононевропатії, радикулопатії шийно-плечової та попереково-крижової частин, хронічні міофібрози плеча та передпліччя, тендовагініти, периартроз, варикозне розширення вен, неврози і багато інших хвороб, у тому числі деякі розлади статевої сфери.

5. Хвороби, зумовлені впливом біологічних факторів. Це — інфекційні та паразитарні хвороби, набуті в процесі професійної діяльності в результаті контакту з хворими, дисбактеріози і кандидози, обумовлені контактом із зараженими речовинами, мікози відкритих ділянок шкіри.

6. Алергічні захворювання: риніти, бронхіти й інші прояви алергії, що виникли в результаті необхідного контакту з речовинами та сполуками, які містять алергени.

7. Новоутворення злоякісного характеру (рак). Це пухлини печінки, шкіри, сечового міхура, лейкоз, ракові захворювання шлунка, пухлини рота та органів дихання, кісток, спричинені впливом шкідливих речовин, присутніх на робочому місці.

## 5.2 Організація пожежної безпеки в компанії “ВебКатТехнік”

Протипожежна безпека на підприємстві в Україні - невіддільна частина організації робочого простору і процесів згідно з нормами чинного законодавства.

Зокрема, цю сферу регламентують Правила пожежної безпеки в Україні, затверджені наказом Міністерства внутрішніх справ України, зі змінами, які періодично вносяться відповідними наказами.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						70
Зм.	Арк	№ докум.	Підпис	Дата		

Вимоги пожежної безпеки, як визначено на законодавчому рівні, обов'язкові для всіх суб'єктів господарювання, незалежно від їх приналежності та розміру статутного капіталу, оборотів, кількості співробітників, форми власності, кодів ЗЕД, сфери роботи та інших аспектів. Ці вимоги поширюються на будь-які організації, що здійснюють свою діяльність на території України.

Пожежна безпека входить в комплекс заходів з охорони праці, і організаційна робота в цій сфері на об'єктах господарювання включає широкий спектр заходів, а саме:

- створення умов для безпечної праці;
- мінімізації ризику виникнення пожеж;
- своєчасне і повноцінне забезпечення технічними засобами для запобігання займанню та усунення самих пожеж та їх наслідків;
- контроль дотримання протипожежних вимог і норм законодавства;
- розробка і впровадження регламентів по гасінню пожеж, евакуації та порятунку з місць пожежі й задимлення людей і майна (матеріальних цінностей);
- внутрішнє і зовнішнє навчання співробітників.

У разі, якщо підприємство орендує площі в іншої особи, сторони повинні в письмовій формі домовитися про те, хто з них і на яких умовах здійснює ці роботи.

Протипожежний захист повинний досягатися застосуванням одного з наступних способів чи їхньою комбінацією:

- застосуванням засобів пожежогасіння і відповідних видів пожежної техніки;
- застосуванням автоматичних установок пожежної сигналізації і пожежогасіння;
- застосуванням основних будівельних конструкцій і матеріалів, у тому числі використовуваних для облицювань конструкцій, з нормованими показниками пожежної небезпеки;

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						71
Зм.	Арк	№ докум.	Підпис	Дата		

- застосуванням просочення конструкцій об'єктів антипіренами і нанесенням на їхнє поверхні вогнезахисних фарб (складів);
- пристроями, що забезпечують обмеження поширення пожежі;
- організацією за допомогою технічних засобів, включаючи автоматичні, своєчасного оповіщення й евакуації людей;
- застосуванням засобів колективного й індивідуального захисту людей від небезпечних факторів пожежі;
- застосуванням засобів протидимного захисту.

Існує чотири основних принципи припинення горіння:

- охолодження зони горіння, або речовини, що горить;
- розведення речовин – учасників реакції горіння, тобто зниження їх концентрації;
- ізоляція реагуючих речовин (горючого або окисника) від зони горіння;
- інгібування – хімічне гальмування реакції горіння.

Спосіб охолодження ґрунтується на тому, що горіння речовини можливе тільки тоді, коли температура її верхнього шару вища за температуру його запалювання. Якщо з поверхні горючої речовини відвести тепло, тобто охолодити її нижче температури запалювання, горіння припиняється.

Спосіб розведення базується на здатності речовини горіти при вмісті кисню у атмосфері більше 14-16% за об'ємом. Зі зменшенням кисню в повітрі нижче вказаної величини полум'яне горіння припиняється, а потім припиняється і тління внаслідок зменшення швидкості окислення. Зменшення концентрації кисню досягається введенням у повітря інертних газів та пари іззовні або розведенням кисню продуктами горіння (у ізольованих приміщеннях).

Спосіб ізоляції ґрунтується на припиненні надходження кисню повітря до речовини, що горить. Для цього застосовують різні ізолюючі вогнегасні речовини (хімічна піна, порошок та інше).

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		72



Спосіб хімічного гальмування реакцій горіння полягає у введенні в зону горіння галоїдно-похідних речовин (бромисті метил та етил, фреон та інше), які при потраплянні у полум'я розпадаються і з'єднуються з активними центрами, припиняючи екзотермічну реакцію, тобто виділення тепла. У результаті цього процес горіння припиняється.

Спосіб механічного гасіння полум'я сильним струменем води, порошку чи газу.

Спосіб вогнеперешкоди заснований на створенні умов, за яких полум'я не поширюється через вузькі канали, переріз яких менше критичного.

Реалізація способів припинення горіння досягається використанням вогнегасних речовин та технічних засобів. До вогнегасних належать речовини, що мають фізико-хімічні властивості, які дозволяють створювати умови для припинення горіння. Серед них найпоширенішими є вода, водяна пара, піна, газові вогнегасні склади, порошки, пісок, пожежостійкі тканини тощо. Кожному способу припинення горіння відповідає конкретний вид вогнегасних засобів. Наприклад, для охолодження використовують воду, водні розчини, снігоподібну вуглекислоту; для розведення горючого середовища - діоксид вуглецю, інертні гази, водяну пару; для ізоляції вогнища - піну, пісок; хімічне гальмування горіння здійснюється за допомогою брометилу, хладону, спеціальних порошків.

Пожежні засоби поділяються на такі:

- установки автоматичного пожежогасіння;
- системи пожежної сигналізації;
- система притипожежного водопостачання;
- пожежні автомобілі, пожежні машини;
- первинні засоби пожежогасіння (пожежний не механізований інвентар, інструмент, вогнегасники тощо);

Протипожежний захист будинків, споруд, людей, які в них перебувають зокрема досягається застосуванням пожежної автоматики.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		73

Пожежна безпека у ПП “ВебКатТехнік“ зображена на рисунку 5.1

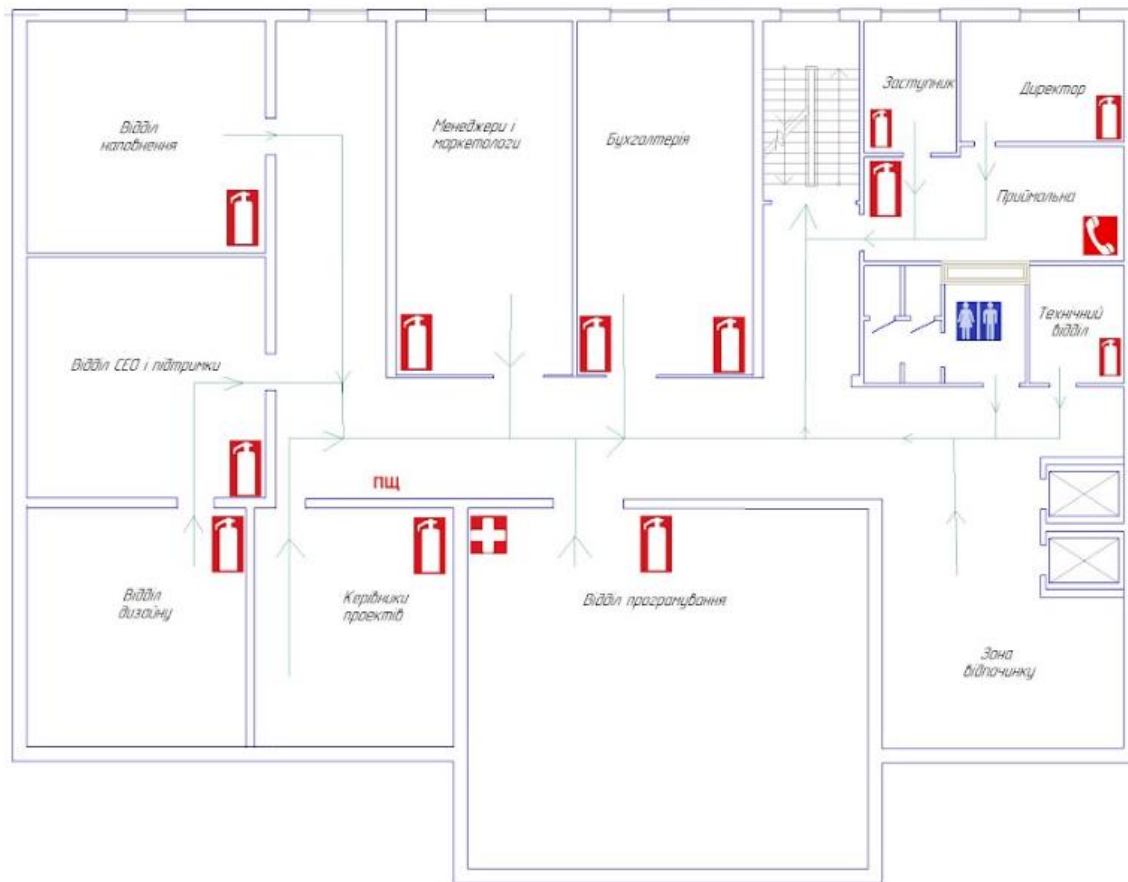


Рисунок 5.1 Зображено план пожежної безпеки

На рисунку 5.1 було детально описано план пожежної безпеки у ПП “ВебКатТехнік“ на ньому ми бачимо 4 вогнегасники які знаходять у: відділі наповлення, керівників проєктів, менеджерів та маркетингологів, та у приймальній, також видно аптечку яка знаходиться у відділі програмування, та телефон який знаходиться у приймальній, та план евакуації.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		74

## ВИСНОВКИ

Для проекту локальної мережі розроблено: логічну топологію, фізичну топологію, таблицю IP-адрес. Описано процедуру моніторингу та перелік кроків з пошуку та виявлення несправностей мережі. Вибрано оптимальну з точки зору руху інформаційних потоків фізичну та логічну топологію.

Додатково розроблено детальні інструкції з налаштування центрального комутатора, файлового сервера, особливу увагу приділено налаштуванню маршрутизатора.

У економічному розділі зроблено розрахунок собівартості робіт по розробці, встановленню та налаштуванню мережі для ПП «ВебКатТехнік».

У розділі охорона праці описано основи травми та професійні захворювання користувачів комп'ютерних та інформаційних технологій. Та організацію пожежної безпеки у ПП «ВебКатТехнік».

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						75
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

## ПЕРЕЛІК ПОСИЛАНЬ

1. Гищук М. В. Основи охорони праці: Підручник. -К.: Кондор, 2005. - 238с
2. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Навчальний посібник. – Вид. 2-ге., доп. – Львів.: Афіша, 2000. – 176с.
3. Методичні вказівки до виконання дипломного проекту за спеціальністю 123 «Комп'ютерна інженерія»
4. Персональні компютери в мережах TCP/IP. Крейг Хант ; з англ. - ВНУ-Київ, 2012.
5. Охорона праці – Москальова В.М. URL: <http://studentbooks.com.ua/content/view/1327/76/> (дата звернення: 30.05.2023).
6. CentOS [електронний ресурс] – URL: <https://wiki.centos.org/Manuals/ReleaseNotes/CentOS8.1911> (дата звернення: 18.06.2023).
7. Fluke Networks LinkRunner Pro Network Multimeter. [електронний ресурс] – URL: <http://www.testequipmentdepot.com/flukenetworks/network-testers/linkrunner-pro.htm> . (дата звернення: 18.06.2023).
8. MikroTik documentation [електронний ресурс] – URL: <http://wiki.mikrotik.com/wiki/Manual> :ТОС (дата звернення: 18.06.2023).
9. Zabbix Network Monitoring [електронний ресурс] – URL: [https://www.zabbix.com/network\\_monitoring](https://www.zabbix.com/network_monitoring) (дата звернення: 18.06.2023).
10. Коммутатори HP [електронний ресурс] – URL: <http://www.hp.com/rnd/support/manuals/2510.htm> (дата звернення: 18.06.2023).
11. Сайт забезпечення розрахунку [електронний ресурс] – URL: <https://www.proliant.com/> (дата звернення: 18.06.2023)..
12. Сервер HP ProLiant DL360 [електронний ресурс] – URL: <https://servak.com.ua/ua/servers/servery-hp/server-hp-proliant-dl360-g6-4bay.html> (дата звернення: 18.06.2023).

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
Зм.	Арк	№ докум.	Підпис	Дата		76

13. Інформація про NAT [електронний ресурс] – URL: <https://uk.wikipedia.org/wiki/NAT> (дата зверення: 18.06.2023).

14. . Воробієнко П., Нікітюк Л., Резниченко П. Телекомунікаційні та інформаційні мережі. Саміт-книга, 2010. 640 с

15. Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі: навчальний посібник. КПІ ім. Ігоря Сікорського, 2020. 336 с.

16. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Львівська політехніка, 2022. 228 с

17. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Київ: "Юніор", 2015. 397 с

18. Рамський Ю., Олексюк В., Балик А. Адміністрування комп'ютерних мереж та систем. Богдан НК, 2010. 196 с

19. Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій. Київ: КПІ ім. І. Сікорського, 2018. 225 с.

20. Олексюк В., Балик Н., Балик А. Організація комп'ютерної локальної мережі. Тернопіль: Підручники та посібники, 2006. 80 с.

21. Микитишин А.Г., Митник М.М., Стухляк П.Д., В.В. Пасічник. Комп'ютерні мережі: навчальний посібник. Львів: «Магнолія 2006», 2013. 256 с.

					<b>2023.КРБ.123.602.08.00.00 ПЗ</b>	Арк
						77
<i>Зм.</i>	<i>Арк</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		