Форма № Н-9.02

Міністерство освіти і науки України

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

Відділення інформаційних технологій, менеджменту, туризму і підготовки іноземних громадян
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі ПП "GALIT "**

Виконав: студент IV курсу, групи КІ-418

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

_____ Павло ПАВЛЮК
(ім'я та прізвище)

Керівник _____ Володимир ШТОКАЛО
(ім'я та прізвище)

Рецензент _____ _____
(ім'я та прізвище)

Тернопіль - 2024

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

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

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"03" квітня 2024 року

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

Павлюку Павлу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проєкту комп'ютерної мережі ПП "GALIT"

керівник роботи Штокало Володимир Ярославович
(прізвище, ім'я, по батькові)

Затверджені наказом ВСП «Тернопільський фаховий коледж ТНТУ імені Івана Пулюя» від 02.04.2024 р №4/9-157.

2. Строк подання студентом роботи: 17 червня 2024 року.

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

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

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

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК 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	04.04	04.04
2	Збір і узагальнення інформації	13.05	13.05
3	Написання першого розділу	20.05	20.05
4	Розробка технічного та робочого проекту	27.05	27.05
5	Написання спеціального розділу	3.06	3.06
6	Розрахунок економічної частини	5.06	5.06
7	Написання розділу охорони праці	7.06	7.06
8	Виконання графічної частини	10.06	10.06
9	Оформлення проекту	12.06	12.06
10	Погодження нормоконтролю	14.06	14.06
11	Попередній захист роботи	17.06	17.06
12	Захист кваліфікаційної роботи	25.06	25.06

7. Дата видачі завдання: 04 квітня 2024 року

Студент _____ Павло ПАВЛЮК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Володимир ШТОКАЛО
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Павлюк П.О. Розробка проєкту комп'ютерної мережі ПП “GALIT”: кваліфікаційна робота на здобуття освітнього ступеня фаховий молодший бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2024. 80 с.

Розробляється сучасна структура мережі, що дозволить об’єднати структурні одиниці приватного підприємства «GALIT», встановить надійний та швидкий обмін даними між ними, забезпечить безпечний обмін інформацією та надає користувачам відповідний до їх потреб доступ до мережі Internet. Логічні сегменти, що є підмережами відображають структуру підприємства з його відділами. Забезпечено захищений віддалений доступ через VPN-тунель до мережі для дистриб’юторів підприємства.

Ключові слова: комп’ютерна мережа, топологія, комутатор, сервер, маршрутизатор, віртуальні мережі, вита пара.

ANNOTATION

Pavlyuk P.O. Development of a computer network project of PE "GALIT": qualifying work for obtaining a professional junior bachelor's degree, majoring in 123 Computer Engineering. Ternopil: SSS «TPC TNTU», 2024. 80 p.

A modern network structure is being developed, which will allow uniting the structural units of the private enterprise "GALIT", establish reliable and fast data exchange between them, ensure secure information exchange and provide users with access to the Internet according to their needs. Logical segments that are subnets reflect the structure of the enterprise with its departments. Secure remote access through a VPN tunnel to the network for enterprise distributors is provided.

Key words: computer network, topology, switch, server, router, virtual networks, twisted pair.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

CSMA/CD (Carrier Sense Multiple Access/Collision Detection; Carrier Sense Multiple Access with Collision Detection) – множинний доступу з контролем несучої та виявленням колізій.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного автоматичного призначення вузлам мережі IP-адрес.

DNS (Domain Name System) – сервер доменних імен.

EIA (Electronic Industries Association) – Асоціація електронної промисловості

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

IP (Internet Protocol) – Інтернет-протокол.

LAN (Local Area Network) – локальна мережа.

MAC (Media Access Control) - апаратна адреса ПК.

NAT (Network Address Translation) – мережева трансляція адес.

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

ЛМ – локальна мережа.

ОС – операційна система.

ПК - персональний комп'ютер.

СКС – структурована кабельна система;

ВСТУП

Сучасна комп’ютерна техніка та локальні комп’ютерні мережі є тісно інтегрованими у повсякденне життя. Приватний сектор економіки використовує сучасні технології. Коефіцієнт корисної дії працівників фірми чи компанії буде на порядок вище від використання сучасних засобів обробки та пересилки даних. Кожна хвилина затримки в передачі інформації може вилитися в дуже відчутні грошові втрати. Такі величезні потенційні можливості, які несе в собі мережа і той новий потенційний підйом, який при цьому переносить інформаційний комплекс, а також значне прискорення виробничого процесу не дають нам право не приймати це до уваги і не застосовувати їх на практиці [1].

Локальні мережі – це об’єднання комп’ютерів, зосереджених на невеликій території, зазвичай в радіусі не більш 1-2 км, хоча в окремих випадках локальна мережа може мати і більш протяжні розміри, наприклад у кілька десятків кілометрів. У загальному випадку локальна мережа є комунікаційною системою, що належить одній організації.

Завдяки локальним мережам ми одержали можливість одночасного використання мережевих ресурсів, таких як мережеві, доступ до глобальної мережі і баз даних декількома користувачами, які не мають безпосереднього з’єднання з цими ресурсами.

Кваліфікаційна робота передбачає розробку локальної мережі приватного підприємства, яке займається виробничою діяльністю по виготовленню стоматологічних установок та сервісному обслуговування стоматологічного обладнання.

.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Відповідно до тематики у кваліфікаційній роботі необхідно розробити комп'ютерну мережу приватного підприємства "GALIT", яке виготовляє та виконує сервісне обслуговування стоматологічне стоматологічного обладнання.

Для вирішення даної задачі потрібно скласти технічне завдання врахувавши всі поставлені до мережі вимоги, проаналізувати план.

Дана розробка знайде своє практичне застосування для локальних мереж фірм, підприємств, установ враховуючи ряд переваг перед аналогічними рішеннями.

До особливостей мережі можна віднести:

- порівняно невеликі затрати на її реалізацію;
- сегментованість локальної мережі з можливістю передачі трафіку між сегментами та налаштування правил фільтрації останнього;
- можливість спільного використання мережевих ресурсів;
- спільне використання мережі Інтернет та централізований захист локальної мережі;
- зебезпечити можливість безпровідного підключення до мережі до 25% корстувачів;
- можливість віддаленого доступу до мережі дилерів із різних регіонів України через захищені VPN-тунелі.

1.1.2 Призначення розробки

В процесі проектування мережі ПП "GALIT" слід забезпечити наступні вимоги, які були поставлені замовником:

- об’єднати в єдину інформаційну структуру ПК всіх структурних підрозділів;

- забезпечити захищений віддалений доступ дилерів, розташованих в різних регіонах до певних мережевих ресурсів та сервісів всередині мережі;

- можливість масштабування мережі шляхом підключення нових вузлів при розширені підприємства;

- зручний доступ до служб і сервісів мережі Інтернет;

- швидкість передачі в мережі повинна забезпечувати потреби мультимедійних додатків до смуги пропускання каналу;

- розмежування доступу різних підрозділів підприємства до окремих інформаційних ресурсів;

- централізоване адміністрування та захист мережевих ресурсів та коистувачів;

- всі витрати на процес розробки проекту та монтажу мережі повинні не перевищувати вказаних замовником.

Для виконання поставлених завдань потрібно розробити локальну мережу, спроектувати кабельну систему із її прокладанням по каналах у вигляді коробів різних січень та відповідно до фізичної топології мережі. Тип кабелю буде напряму залежати від вибраного стандарту, який описано в розділі 2.1 “Опис та обґрунтування вибору логічного типу та технології мережі”.

На наступному етапі потрібно зконфігурувати служби локальної мережі та мережеве обладнання.

1.1.3 Вимоги до апаратного і програмного забезпечення

Будь-яка комп’ютерна мережа є поєднанням двох складових: апаратної та програмної. Апаратне забезпечення поділяється на активне та пасивне. При цьому активне мережеве обладнання аналізує та здійснює певну обробку даних, що передаються, тоді як пасивне обладнання лише передає сигнали, а також може бути лише аксесуарами для під’єднання або розширення мережі.

Пасивне обладнання мережі повинно забезпечувати фізичну можливість гарантування необхідної швидкості передачі мережевого трафіка. У випадку проектованої мережі швидкість передачі повинна бути не меншу 1 Гбіт/с. Для цього необхідно здійснити обгрунтований вибір мережевої технології. В даному випадку слід використати мережеву технологію Gigabit Ethernet.

Активне обладнання мережі до якого в даній мережі відносяться комутатори робочих груп, сегментуючі комутатори та маршрутизатор повинне задовольняти вимогам вибраної мережевої технології, забезпечувати логічну сегментацію та фільтрацію мережевого трафіку, можливість поділу мережі на віртуальні підмережі. Для цього комутатори мережі повинні підтримувати стандарти IEEE 802.3ab, IEEE 802.1Q

До програмного забезпечення локальної мережі відносять операційні системи серверів та робочих станцій.

Для вибору серверної операційної системи потрібно враховувати цілий ряд критеріїв, серед яких: вартість, надійність в роботі, безпека систем захисту від хакерських атак та періодичність оновлення.

Для вибору операційної системи робочих станцій також важливим є простота і зручність у використані, оскільки ними працюють рядові користувачі, які не є глибоко обізнаними спеціалістами в галузі адміністрування на відміну від серверних ОС з якими працюють підготовленні адміністратори. Ще одною суттєвою вимогою буде підтримка операційною системою стеку протоколів TCP/IP, на якому буде побудована проектована мережа.

1.1.4 Вимоги до документації

Документація відіграє важливу роль в процесі експлуатації мережі. Буде використано для:

- усунення несправностей – документація може служити інструкцією при пошуку і усунення несправностей мережі;

- допомогою в підготовці нового персоналу – якщо в підприємстві з'явився новий співробітник, то його буде легше підготувати до роботи, у випадку коли доступна документація по ділянці, де йому належить працювати;

- допомогою для постачальників і консультантів – послуги цих спеціалістів, як правило, є вельми дорогими. І якщо їм потрібно знати певні деталі мережевої інфраструктури, то наявність документації дозволить виконати швидше.

До пакету документації слід віднести:

- логічна топологія;
- фізична топологія;
- таблиця адресації вузлів мережі;
- інструкції з налаштування ключових вузлів мережі№
- інструкції з тестування та звіт по тестуванню (дана інформація буде корисною при виявленні несправностей та їх пошуку).

1.1.5 Техніко-економічні показники

Основні техніко-економічні показники локальної мережі ПП "GALIT":

- топологія мережі – гібридна;
- стандарт мережі – Gigabit Ethernet та Wi-Fi;
- базові технології – 1000Base-T та IEEE 802-11ac;
- швидкість безпровідного та провідного сегменту мережі 1 Гбіт/с;
- операційна система файлового сервера – FreeBSD;
- технологія віддаленого доступу до локальної мережі – IPSec VPN;
- тип маршрутизації між підмережами – статична;
- тип віртуальних підмереж – IEEE 802.1Q;
- тип сервера – файловий, DHCP;
- трудомісткість проектування і інсталяції мереж – до 100 люд/год.
- матеріальні витрати на мережу – до 250 000 грн;
- собівартість мережі – до 350 000 грн;

- Повна вартість мережі - до 500 000 грн.

1.1.6 Стадії та етапи розробки

Проектування мережі для ПП «GALIT» можна розділити на такі етапи:

- ознайомлення з технічним завданням;
- розробка логічної топології мережі;
- розробка фізичної топології мережі;
- налаштування мережевого обладнання комутаторів та VLAN;.
- налаштування маршрутизатора;
- налаштування VPN-тунелю;
- налаштування файлового сервера;
- налаштування програмного забезпечення клієнтів;
- тестування мережі.

1.1.7 Порядок контролю та прийому

На завершальному етапі проектування комп'ютерної мережі необхідно виконати тестування основних технічних показників мережі. Вони повинні відповідати поставленим вимогам. Для їх контролю будуть використані апаратні та програмні засоби. До апаратних віднесемо кабельний тестер сертифікований згідно вимог стандарту 1000 Base-TX та програмні утиліти.

Здача мережі в експлуатацію та її прийом відбувається відповідно до затверджених актів прийому-передачі об'єктів, спеціальною комісією, до складу якої повинні входити представники замовника та виконавця.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства

Тема кваліфікаційної роботи передбачає розробку комп'ютерної мережі приватного підприємства "GALIT", яке займається виробничою діяльністю по

виготовленню стоматологічних установок та сервісному обслуговування стоматологічного обладнання.

Дане підприємство розташоване в с. Байківці, Тернопільксого району і займає три поверхи спеціалізованої 3-ох поверхової будівлі, яка власне йому і належить.

При розробці мережі потрібно забезпечити можливість об'єднання робочих станцій всіх відділів в єдину інформаційну інфраструктуру; вести в експлуатацію служби локальної мережі; надати доступ до служб глобальної мережі Інтернет.

Одна з основних задач – це сегментувати локальну мережу на невеликі логічні групи, які будуть відображати реальну структуру ПП «GALIT».

Проаналізувавши структуру ПП «GALIT» і вимоги щодо захисту інформації прийнято рішення про створення наступних груп користувачів:

- загальне керівництво;
- бухгалтерія;
- відділ контролю якості;
- відділ збуту;
- відділ маркетингу;
- відділ постачання;
- сервісний центр;
- експортний відділ.

Структурні підрозділи компанії займають перший та другий поверх трьохповерхової власної будівлі компанії. Третій мансардний поверх містить відпочинкові та обідні зони, архів та інші допоміжні приміщення. Отже, розміщення кабінетів на 1 та 2 поверсі наведено на кресленні «План приміщень».

Також на плакаті «Фізична топологія» наведено схему локальної мережі, що є перенесеною з логічної топології на вище згаданий план приміщення

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу та технології мережі

Для провідного з'єднання робочих станцій мережі пропонується використати технологію Gigabit Ethernet, яка є більш швидкісною модифікацією базової технології Ethernet, що забезпечує обмін даними на рівні 1 Гбіт/с.

Технологія Ethernet передбачає використання системи керування доступом до середовища (MAC), яка дозволяє під'єднаним мережевим пристроям спільно використовувати середовище передачі.

В основі технологій Ethernet є принцип множинного доступу з контролем несучої та виявленням колізій (CSMA/CD).

CSMA/CD – це клас протоколів, які: прослухують кабель перед передачею; виявляють колізії; ініціалізують повторні передачі (через випадковий час) [2].

Абонентська система може почати передачу, якщо у цей момент жодна з інших систем не передає дані. Якщо в процесі передачі абонентська система виявляє, що паралельно почалася інша передача, то вона припиняє свою передачу, з тим щоб пізніше почати її з початку.

Стандарт Gigabit Ethernet базується на технології Ethernet і включає в себе ряд покращень, які дозволяють підвищити швидкість передачі даних, зменшити пакетну затримку та підвищити ефективність передачі даних в мережі. При цьому кабелі та окремі частини активного мережевого обладнання мало чим відрізняються від попередніх технологій Fast Ethernet та базової Ethernet [3].

Відповідна швидкість передачі даних із подібністю до попередніх технологій забезпечується за рахунок збільшення мінімально допустимий розмір кадру до 512 байт (4096 bit). Крім цього, існує можливість пакетної передачі кадрів (frame bursting), коли пристрій, який отримав доступ до

середовища, після передачі кожного кадру посилає спеціальну послідовність, після якої йде наступний кадр. Тоді як раніше виникали паузи. Кадри пакету можуть адресуватися різним одержувачам. При цьому скорочуються витрати на отримання доступу до середовища ─ між кадрами пакету середовище для інших вузлів виглядає зайнятим [3].

Враховуючи вимоги до високої пропускної здатності мережі підприємства «GALIT» для забезпечення необхідної динамічної обробки та обміну великими об'ємами даних вибір даної технології є цілком виправданим.

Технологія Gigabit Ethernet передбачає два види середовища передачі даних із використанням одномодового та багатомодового оптичного волокна та кабелів типу "скручена пара".

Використання одномодового та багатомодового оптоволоконна регулюється стандартом IEEE 802.3z із специфікаціями 1000BaseSX, 1000BaseLX, 1000BaseLX10, 1000BaseLH 1000BaseZX та 1000BASE-BX10 і передбачає передачу даних на великі відстані від 550 м (1000BaseSX) до 70 км (1000BASE-ZX).

З точки зору економії дешевшим варіантом для створення мереж із з'єднанням на невеликі відстані (до 100 м) в межах офісу чи будівлі є використання середовища передачі даних на основі кабелю скрученої пари, які регламентуються специфікаціями 1000BASE-T та 1000BASE-TX. При чому специфікація 1000BASE-TX вимагає використання кабелю категорії Cat-6 та Cat-7, тоді як 1000BASE-T дозволяє використовувати більш дешевші варіанти кабелю категорії Cat-5, Cat-5e та Cat-6. Отже, з точки зору економічності специфікація 1000BASE-T є більш прийнятною.

Специфікація 1000BASE-T, регламентується стандартом IEEE 802.3ab і передбачає повнодуплексну передачу одночасно по чотирьох парах провідників по кожній парі відразу в обох напрямах. Кінцеві ланцюги виділяють з суміші сигнал протилежного передавача. Рішення цієї задачі на надвисоких частотах стало можливим завдяки застосуванню сучасних сигнальних процесорів [1].

Враховуючи вищеописані аргументи вирішено використати для провідного сегменту мережі специфікацію 1000Base-T.

Згідно із завданням замовника в проектованій мережі слід забезпечити 25% користувачів безпровідним доступом. Тому, крім провідного сегменту потрібно розробити можливість доступу до ресурсів мережі по безпровідній технології Wi-Fi.

У технології Wi-Fi для поширення радіохвиль можуть використовуватися діапазони частот 2,4 ГГц, 5 ГГц або 6 ГГц. Всередині діапазону є окремі канали для підключення. Для Wi-Fi на частоті 2,4 ГГц використовуються три канали, що не перетинаються із шириною по 20 МГц кожен. Для частоти 5 ГГц використовується 33 канали, 19 із яких не перетинаються. Кожен канал має ширину 40 МГц. І нарешті для частоти 6 ГГц використовується 59 каналів різної ширини З’являються 14 додаткових канали шириною 80МГц і сім шириною 160 МГц [2].

При цьому слід зауважити, що чим більше буде каналів і чим більша їх ширина тим менше буде завад при одночасній роботі декількох мереж.

Технологія Wi-Fi є набором стандартів IEEE-802-11, які регламентують різні смуги частот та швидкості передачі даних (таблиця 2.1).

Таблиця 1.1 – Стандарти та покоління Wi-Fi

Назва покоління	Стандарт IEEE	Прийнятий	Максимальна швидкість з'єднання (Мбіт/с)	Смуги радіочастот (ГГц)
Wi-Fi 7	802.11be	(2024)	≤ 46120	2.4 / 5 / 6
Wi-Fi 6E	802.11ax	2020	≤ 9608	6
Wi-Fi 6		2019		2.4 / 5
Wi-Fi 5	802.11ac	2014	≤ 6933	5
Wi-Fi 4	802.11n	2008	≤ 600	2.4 / 5
Wi-Fi 3	802.11g	2003	≤ 54	2.4
Wi-Fi 2	802.11a	1999	≤ 54	5
Wi-Fi 1	802.11b	1999	≤ 11	2.4
Wi-Fi 0	802.11	1997	≤ 2	2.4

Оскільки, для проектованої мережі потрібно забезпечити швидкість передачі даних до 1 Гбіт/с, то слід використати специфікацію IEEE-802-11ac, яка здійснює передачу даних в діапазоні частот 5-6 ГГц зі швидкістю до 1 Гбіт/с. Також протокол передбачає застосування до 8 антен MU-MIMO та розширення каналу до 80 – 160 МГц.

Для проекту локальної мережі буде використано принцип поділу мережі на віртуальні підмережі. При цьому необхідна маршрутизація між сегментами буде виконуватись через віртуальні порти маршрутизатора, який одночасно виконую роль шлюзу доступу до Інтернет. Згідно із технічним завданням мережу слід поділити на чотири віртуальні сегменти VLAN у відповідно до плану приміщення представленому на Додатку А:

- перша VLAN1 повинна об’єднувати комп’ютери керівництва підприємства (директор, прийомна), експортний відділ та відділ контролю якості;
- друга VLAN2 включає ПК, що належать до бухгалтерії;
- третя VLAN3 на логічному рівні повинна утворювати окремий сегмент

із комп’ютерів працівників підрозділу маркетологів;

- четверта VLAN4 буде об’єднувати робочі станції на яких працюють співробітники сервісний центр та відділу збуту.

Окремо від віртуальних мереж необхідно також під’єднати до мережі З міркувань додаткової безпеки його слід виділити в окремий сегмент мережі, не пов’язаний із жодною VLAN робочих станцій.

Саме підприємство розташоване на двох поверхах триверхової будівлі і фізично підмережі VLAN3 та VLAN4 розміщені на першому поверсі, а VLAN1 та VLAN2 відповідно на другому.

Для реалізації подібного логічного поділу найбільш прийнятним для ядра мережі (провідної частини мережі) буде використання фізичної топології розширеної зірки. Згідно із завданням замовника, для 25% кінцевих вузлів мережі слід забезпечити доступ до мережі за допомогою безпровідного середовища WiFi, тому в цілому фізичною топологією мережі буде гібридна топологія.

Фізичне об’єднання пристроїв в одну віртуальну мережу реалізовано за допомогою комутаторів другого рівня OSI моделі із підтримкою VLAN, розташованих по два на кожному поверсі. Згідно із технічним завданням, всього в мережі передбачено 52 робочі станції розподілених по віртуальних мережах. У таблиці 2.2 представлено кількісний розподіл ПК по сегментах мережі.

В таблиці 2.2 – Кількісний розподіл робочих станцій по сегментах

Назва логічного сегменту мережі	Структурний підрозділ підприємства	Кількість робочих станцій	
		Разом	З них безпровідні
VLAN1	Директор	2	1
	Прийомна	1	1
	Експортний відділ	2	-

	Відділ постачання	8	5
	Відділ контролю якості	3	-
VLAN2	Бухгалтерія	7	-
VLAN3	Відділ маркетингу	10	5
VLAN4	Сервісний центр	15	2
	Відділ збуту	4	
Разом		52	14

Як видно із таблиці 2.1 загальна кількість вузлів VLAN1, є достатньою, щоб частину портів 24-х портового комутатора використати для під'єднання комутаторів інших трьох сегментів, налаштувавши їх в транковому режимі віртуальних мереж. Тому з метою економії коштів на розробку мережі, комутатор VLAN 1, можна поєднати із функцією центрального (головного) комутатора всієї мережі (рисунок 2.1). Також, на одному із портів цього комутатора слід встановити з'єднання із маршрутизатором, який буде здійснювати маршрутизацію між VLAN та виконувати роль шлюзу доступу до Інтернет. До окремого порту маршрутизатора слід під'єднати FTP та IPSec сервер. Логічна топологія мережі представлена на рисунку 2.1.

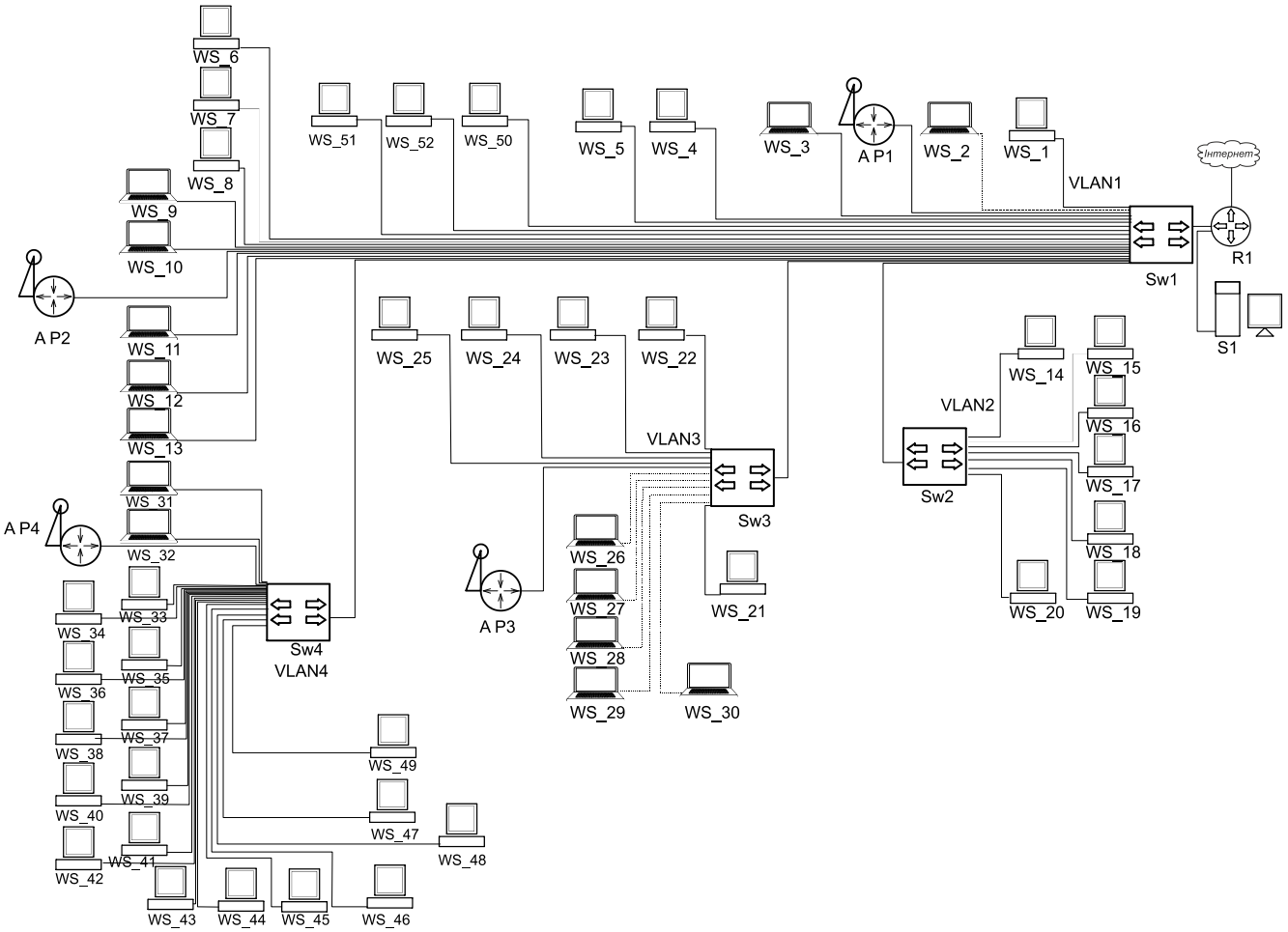


Рисунок 2.1 – Топологія мережі ПП «GALIT»

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з’єднань та їх прокладання

Схеми розміщення кабельних сегментів будувалися з врахуванням вимог замовника та відповідно до стандартів побудови структурованих кабельних систем. Всі вузли мережі та схема їх зв’язку показані на рисунку 2.1 та додатку Б.

Локальна мережа побудовано на базі неекранованої витої пари категорії 6. Фізична топологія ядра мережі - розширена зірка. Дану топологію зображено на рисунку 2.1.

Кабельні сегменти проектованої мережі, що ідуть по кабельних каналах від розеток мережі до хостів заходять в патч-панель комутаційної шафи, де за допомогою патч-кордів буде здійснюватись перекомутація з’єднань.

Максимальна довжина кабелю між розетками або між розеткою і патч-панелю – 96 метрів. Це виходить із обмеження стандарту для кабелю крученої пари на максимальну довжину до 100 метрів між комп'ютер і комутатором. Чотири метри, що залишились, відводяться на патч-корд між розеткою і робочою станцією, а також між патч-панелю і комутатором.

Оскільки в локальній мережі використовуються безпровідні точки доступу, то реально отримаємо гібридну фізичну топологію.

Кабель – це один з основних компонентів структурованих кабельних систем. Основна функція кабелю – передача електричних сигналів або оптичних променів (в залежності від типу кабеля) від одного пристрою до іншого. Від правильної прокладки кабелів залежить рівень якості сигналу, що передається по ньому. Кожен кабель має технічні вимоги до монтажу, і лише при дотриманні цих умов кабельна система в цілому відповідатиме заявленим виробником характеристикам [4].

Згідно технічного завдання кабельна система повинна забезпечити швидкість передачі даних по каналах з’єднання 1 Гбіт/с.

Після аналіз всіх технічних характеристик на відповідність вимогам замовника, а також врахування вартості та можливості легкої модернізації для локальної мережі використано неекрановану виту пару категорії 6.

Прокладання кабелів буде виконуватись в коробах із профілем 50х40 IBOCO. Прохід через стіни кабелем виконано в ПВХ трубках діаметром 16 мм. Для чого необхідно просвердлити отвори відповідного діаметру у місцях представлених на монтажній схемі кабельних мереж (див. додаток В).

Для з’єднання приміщень відділу маркетологів та сервісного центру через коридор із підвісною стелею кабелі поміщаються у гофрованому ПВХ шланзі діаметром 32 мм і довжиною 4,2 м (див. додаток В).

Між поверхами прокладання кабелю здійснюється теж у гофрованому ПВХ шланзі діаметром 32 мм і довжиною 6,5 м. через вентиляційну шахту, що знаходиться між приміщеннями відділу збуту та маркетологів (див. додаток В).

Для встановлення структурованої кабельної системи в мережі потрібно визначити загальну кількість кабелю. Для цього потрібно підрахувати загальну довжину кабелю на кожен поверх, як суму всіх довжин від персонального комп'ютера, точки доступу або сервера до комутатора, від комутатора до сегментуючого комутатора та від нього від нього до роутера. При чому довжина кабелю буде визначатись із множенням визначеної довжини на коефіцієнт запасу 1,3, який враховує особливості прокладки кабелю (спуски, підйоми, повороти та ін., а також запас на оброблення кабелю на кінцях.

Згідно з параметрами розмірів приміщення, представлених на плані мною позначено в таблиці Г.1.

Виходячи із підрахунків, представлених в таблиці Г.7 загальна довжина кабелю скручена пара для першого поверху будівлі становить L_1=534,90 м і другого поверху – L_2=456,65 м. Разом довжина кабелю горизонтальної структурованої кабельної системи становить:

$$L_г=L_1+ L_2= 534,90 + 518,65 = 1190,55 \text{ м.} \quad (2.1)$$

Вертикальна кабельна системи, враховуючи висоту поверху рівну 3 м, становить L=6 м. Враховуючи коефіцієнт запасу 1,3, отримаємо:

$$L_в=L\cdot 1,3=18\cdot 1,3=23,4 \text{ м.} \quad (2.2)$$

Отже. Із врахуванням запасу довжина необхідного кабелю горизонтальної структурованої кабельної системи становить:

$$L= L_г \cdot 1,3=1053,55 \cdot 1,13= 1190,5 \quad (2.3)$$

Загальна довжина всього кабелю структурованої кабельної системи становить:

$$L=L_г+ L_в=1190,5 +23,4 = 1259,82 \text{ м} \sim 1214 \text{ м} \quad (2.4)$$

Враховуючи, що в бухті знаходиться 305 м кабелю розрахуємо необхідну кількість бухт кабелю:

$$K \geq \frac{L}{305} = 3,98 \quad (2.5)$$

Отже потрібно 4 бухти кабелю

2.2.2 Типи та розташування вузлів мережі

Локальна мережа в нашому проекті складається з таких вузлів:

- мережева розетка. Використовується для підключення персональних комп'ютерів або периферійних пристроїв, наприклад, принтерів, до локальної мережі. Мережеві розетки буде розміщується на стіні біля під'єднуваних вузлів;
- комутаційна шафа, де буде розміщено основне активне мережеве обладнання мережі для його впорядкування;
- безпровідні точки доступу дозволяють розширити провідний сегмент мережі на безпровідне обладнання. Дозволяють підключити у даний сегмент віртуальної пристрої по безпровідній технології Wi-Fi;
- комутатор сегментів мережі, що призначені об'єднати між собою кінцеві мережеві пристрої певної підгрупи, окремого сегменту мережі;
- центральний комутатор локальної мережі, що об'єднує між собою вузли локальної мережі або безпосередньо або через комутатори сегментів мережі;
- маршрутизатор. Здійснює маршрутизацію трафіку між віртуальними

підмережами та створює шлюз і забезпечує надання послуг Інтернет для відповідних вузлів локальної мережі;

- сервери локальної мережі. Забезпечує локальну мережу службами віртуальних VPN-тунелів для віддаленого доступу працівників ресурсів мережі підприємства та надає сервіс файлового сховища для зберігання і обміну документами з якими працюють співробітники підприємства по протоколу FTP.

Головний комутатор, який також виконує роль сегментуючого комутатора VLAN1, маршрутизатор, сервер, блок безперебійного живлення, патч-панель будуть об’єднані у головний комутаційний вузол локальної мережі (серверну), що розташована в приміщені під номер 12 (див. додаток А, Б та В).

Враховуючи територіальну близькість кінцевих вузлів підмережі VLAN 2 та для оптимального впорядкування кабельних систем прийнято рішення сегментуючий комутатор цієї підмережі теж розмістити в серверній кімнаті (див. додаток В).

Все активне мережеве обладнання серверної буде поміщене у комутаційну шафу із патч-панелю та патчкордами для впорядкування мережевих кабелів.

Для впорядкування активного мережевого обладнання першого поверху будівлі у приміщенні кольороподілу слід розмістити комутаційну шафу. В цій шафі будуть розміщені сегментуючі комутатори підмереж VLAN 3 та VLAN 4. Такому централізованому розташуванню активного мережевого обладнання сприяє фізична близькість приміщень із кінцевими вуздами підмереж.

Також, це надасть більш централізований фізичний доступ адміністратору мережі до активного мережевого обладнання.

Крім провідного обладнання, в мережі передбачено безпровідний доступ для 25% мережевих хостів із збереженням резервної можливості підключення цих пристроїв кабельним зв’язком.

Для цього у приміщеннях кабінету директора, кабінеті редакторів та коректорів, на другому поверсі та у відділеннях менеджменту та маркетингу і верстки та дизайну на першому поверсі встановлено чотири безпровідних точки

доступу (див. додатки Б та В). Кріплення точок доступу передбачено до стелі, а кабель від горизонтального короба прокладено у вертикальному коробі із профілем 15Х10.

Детальний план прокладки кабельних з'єднань та розташування вищеописаних вузлів представлено у таблиці Г.1на додатку Г.

2.3 Обґрунтування вибору комунікаційного обладнання

2.3.1 Обґрунтування вибору пасивного мережевого обладнання

Розглянемо більш детально обладнання потрібне для побудови локальної комп'ютерної мережі ПП «Galit».

При побудові комп'ютерної мережі використовується активне та пасивне комунікаційне обладнання. До пасивного обладнання в першу чергу відносяться кабельні системи, комутаційні шафи, патчкорди, роз'єми мережеві розетки та ін.

Для вибору кабельної системи потрібно враховувати тип мережі і її топологією. Необхідні для стандарту фізичні характеристики кабелю закладаються при його виготовленні, про що і свідчать нанесені на кабель маркування. У результаті, сьогодні практично всі мережі проектуються на базі UTP і волоконно-оптичних кабелів.

Для горизонтальної та вертикальної (з'єднання між поверхами будівлі) кабельної системи вибрано кабель U/UTP Cat.6 4Pr (виробник Одескабель), який має наступні конструктивні особливості [13]:

- струмопровідна жила: мідний м'який провідник;
- діаметр: 0,57 мм (23 AWG);
- ізоляція: поліетилен;
- діаметр провідника: 1,05 мм.;
- відповідність вимогам: ISO/IEC 11801:2002, EN 50173-1:2002, ANSI/TIA/EIA-568-B.2-1-2002, IEC 61156-5:2002.

Для магістральної кабельної системи з’єднання локальної мережі із провайдером Інтернет вибрано кабель ОПТ-24А4, фірма-виробник Південкабель, який має наступні конструктивні особливості [14]:

- кількість волокон – 24;
- тип оптичного волокна: одномодовий з розширеним діапазоном хвиль;
- діаметр кабеля: 10х19±0.5 мм.

Для розміщення мережевого обладнання в серверній буде використано шафу комутаційну висотою 22U, габарити – 600х600х1196мм. Комутаційна шафа містить патч-панелі, комутатор, блок безперебійного живлення (APC 1500VA), кабельні організатори.

Для кросування з’єднань буде використано патч панель та комутаційна шафа. Комутаційні шафи містять патч-панелі (Panduit, 19", 24 порти, кат. 6) [15].

Патч-панель 19" розташовується в серверні комутаційної шафи. Поставляється з конекторами RJ-45. Для підключення не вимагає спеціальних інструментів. Конектор конструктивно обладнанні автоматичним прорізанням ізоляції провідників. Поставляється з кріпильними деталями і хомутами Colring. Відповідає стандарту EIA / TIA 568 B.2-1.

Для розміщення мережевого обладнання (комутаторів та маршрутизатора) буде використано шафу комутаційну висотою 6U, габарити – 600х450х375 мм [14]. Зовнішній вигляд представлено на рисунку 2.2.

Рисунок 2.2 – Комутаційна шафа 6U ZT-NET AL-WDR06U-64G

Блок безперебійного живлення забезпечує безперервну подачу живлення на вузли мережі. Для даної мережі вибрано – APC Back-UPS Pro 1500VA.

В таблиці 2.3 наведено технічні характеристики APC Back-UPS Pro 1500VA [16].

Таблиця 2.3 – Технічні характеристики APC Back-UPS Pro 1200VA

Кількість вихідних розеток	4
Діапазон вхідної напруги	175 - 295 В
Потужність	1500 Вт
Ефективна потужність	1200 Вт
Захист телефонної лінії	Так
Індикація	Так
Час роботи від батареї	При половинному навантаженні 36 хв
Час зарядки батареї	8 год
Габарити	301 x 112 x 382 мм
Вартість	3625 грн

При виборі мережевих розеток, необхідно врахувати, щоб вони мали подвійні роз’єми як RJ-45 для піл’єднання мережевого кабелю, так і RJ-11 – телефонного. Для даної мережі вибрано телекомунікаційні розетки Sedna SDN5200160 [17] вартістю 125 грн.

2.3.2 Обґрунтування вибору пасивного мережевого обладнання

Головний комутатор призначений об’єднати між собою всі пристрої мережі, через сегментуючі комутатори віртуальних мереж, а також до нього буде безпосередньо під'єднано маршрутизатор шлюзу доступу до Інтернет, розташовані в серверній кімнаті. Як вже повідомлялось, що із економічних

міркувань та особливостей плану приміщення, вирішено головний комутатор поєднати із сегментуючим комутатором VLAN1.

Для забезпечення більшої однотипності обладнання інші два сегментуючі комутатори вирішено вибрати тієї ж моделі. Під'єднання кінфевих вузлів, сегментуючих комутаторів та маршрутизатора буде здійснюватися через порти скручено пари. Враховуючи, що максимальна кількість вузлів в одній VLAN не перевищує 22, то одним із критеріїв вибору є наявність 24 портів RJ-45.

Порівняльна характеристика центральних комутаторів наведена в таблиці Д.1 «Порівняльні технічні характеристики комутаторів» додатку Д. Для мережі вибрано комутатор Allied Telesyn AT-x600-24Ts (рисунок 2.3) враховуючи співвідношення ціна/відповідність технічним параметрам [18]. Всього для проектування мережі слід придбати 4 комутатори цієї моделі. По одному в кожну для кожного сегменту мережі.

Рисунок 2.3 – Центральний та сегментуючий комутатор
Allied Telesyn AT-x600-24Ts

Оскільки, маршрутизатор буде з'єднувати локальну мережу із провайдером Інтернет через оптоволоконний кабель, то одним із критеріїв вибору є наявність SFP-модуля та підтримка протоколів IPSec, відповідно до технічного завдання. Враховуючи ці критерії вирішено в якості маршрутизатора вибрати модель Cisco ISR4221/K9 (зовнішній вигляд на рис. 2.4).

Рисунок 2.4 – Зовнішній вигляд маршрутизатора Cisco ISR4221/K9

Даний пристрій обладнаний двома SFP-портами, двома портами LAN FastEternet із роз'ємом на RJ-45 та двома додатковими слотами розширення NIM для інтерфейсних модулів. Цей пристрій відрізняється високою продуктивністю та швидкістю передачі до 2 Гбіт/с, обладнаний оперативною пам'яттю об'ємом 4 ГБ із можливістю розширення до 16 ГБ. Об'єм запам'ятовуючого пристрою на основі флеш-пам'яті 4 ГБ. Маршрутизатор підтримує VPN сервіси та роботу протоколів NAT, RIP v1/v2, OSPF, EIGRP, BGP, PBR, PfR, адресацію IPv4 та IPv6. Характеристики маршрутизатора представлено в таблиці 2.4 [19].

Таблиця 2.4 – Основні технічні характеристики маршрутизатору Cisco ISR4221/K9 [12]

Характеристика	Значення
Макс. Кількість VLAN	20
швидкість передачі	2 Гбіт/с
Оперативна пам’ять	4 ГБ із можливістю розширення до 16 ГБ.
Флеш пам’ять	4 ГБ
Підтримувані VLAN	802.1q Tag-на основі, на основі портів
Локальний сервер DNS	+
Захист від атак DoS	+
Захист від спуфінгу	+
Пропускна здатність NAT	2.2 Гбіт/с
Маршрутизація	Статична, RIP v1/v2, OSPF, EIGRP, BGP
Підтримка IPSec	+

Монтаж в стійку	4U
WAN-порт	SFP – 2 шт.
LAN-порт	Gigabit Ethernet RJ-45
Розмір (мм)	273 x 171 x 45 мм
Вартість	24 706 грн.

Як вже відмічалось у проектованій мережі передбачено використання чотирьох безпровідних точок доступу, які будуть розташовані у приміщеннях кабінету директора, відділу постачання, відділу маркетологів і сервісного центру. Враховуючи, що пристрої, які будуть використовувати дане під'єднання повинні також мати можливість під'єднатись по провідному з'єднанні із тією ж статичною IP-адресою, то для реалізації цієї можливості потрібно використати саме точку доступу, а не маршрутизатор чи міст (щоб лише продовжити існуючий сегмент провідної мережі на безпровідну).

Для даної цілі вирішено вибрати модель TP-LINK EAP110 (рис. 2.4) із оптимальними технічко-економічними показниками саме для невеликого офісу із можливістю легкого встановлення на стіну або підвішування до стелі.

Точка доступу EAP110 має оригінальний дизайн, що нагадує стильову лампу, тому гармонійно вписується в інтер'єр офісу. Підтримує живлення по станларту EoP і не вимагає додаткового підведення кабелю живлення. EAP110 має підтримує режим аутентифікації користувачів.

Рисунок 2.5 – Точка доступу TP-LINK EAP110

Програмне забезпечення EAP Controller даної точки доступу підтримує централізоване управління бездротовими мережами, що дозволяє адміністратору одночасно керувати великою кількістю точок доступу. Даний пристрій також має моніторингу у реальному часі, графічний аналіз мережного трафіку та групове оновлення вбудованого ПЗ.

2.4 Планування IP-адресації пристроїв

Для адресації пристроїв у локальній мережі ПП «GALIT» прийнято рішення використати приватну IPv4-адресу класу С для локальним мереж 192.168.0.0/24, яка передбачає використання до 254 мережевих адреси, що для даної мережі із 52 кінцевих вузлів цілком достатньою.

Мережа підприємства повинна містити чотири локальні віртуальні мережі, VLAN 1 – VLAN 4 із кількостями комп'ютерів представлених в таблиці 2.5, та підмережу для сервера із двох вузлів.

Таблиця 2.5 – Кількість комп'ютерів в підмережах

VLAN 1	VLAN 2	VLAN 3	VLAN 4	Серверна
16+1=17	7+1=8	10+1=11	19+1=20	1+1=2

В кожну мережу слід додати ще по одній IP-адресі для інтерфейсу маршрутизатора та шлюзу у зовнішню мережу. Загальна кількість вузлів мережі 16+8+11+20+2=58.

Для економії адресного простору підмережі вирішено побудувати використовуючи маску змінної довжини VLSM. Для цього буде використано метод безкласової адресації CIDR.

Маски змінної довжини будемо визначати для підмереж у порядку зменшення кількості їх вузлів, щоб утворився адресний простір, що перекривається. Найбільша підмережа VLAN 4 із 20 вузлів. Найближчий мінімальний блок адрес, щоб забезпечив цю кількість 32. Обчислюємо останній октет маски підмережі: 256-32=224, тому маска підмережі 255.255.255.224.

Тобто для маски підмережі в останньому октеті від адреси хоста забирається три старших біти на маску підмережі. Отже, адреса підмережі VLAN 4 буде 192.168.0.0/27. Адресний простір для вузлів мережі буде 192.168.0.1 до 192.168.0.30, а широкосмугова адреса 192.168.0.31/27.

Друга за кількістю вузлів мережа VLAN 1 із 16 адрес. Найближчий мінімальний блок адрес, щоб забезпечив цю кількість – 32. В останньому октеті маски буде число 256-32=224, тому маска цих підмереж 255.255.255.224. Для маски в останньому октеті буде забрано чотири біти, тому адреса другої мережі 192.168.0.32/28.

Подібним чином визначаються адресний простір та маска для інших підмереж. Результати розрахунків розподілу на підмережі представлені в таблиці 2.6.

Таблиця 2.6 – Розрахунок адресного простору для підмереж

Назва підмережі	Кількість вузлів	Обчислення останнього октету	Доступна кількість адрес	Адреса підмережі	Діапазон адрес для вузлів	Широкосмугова адреса
VLAN 4	20	256-32=224	30 (вільно 10)	192.168.0.0/27	192.168.0.1 – 192.168.0.30	192.168.0.31
VLAN 1	16	256-32=224	30 (вільно 14)	192.168.0.32/27	192.168.0.33 – 192.168.0.62	192.168.0.63
VLAN 3	11	256-16=240	14 (вільно 3)	192.168.0.64/28	192.168.0.65 – 192.168.0.78	192.168.0.79
VLAN 2	8	256-16=240	14 (вільно	192.168.0.80/28	192.168.0.81 –	192.168.0.95

			6)		192.168.0.94	
Серверна	2	256-4=252	2 (вільно 0)	192.168.0.96 /30	192.168.0.97 – 192.168.0.98	192.168.0.99

Відповідно до таблиці 2.3 всього вільних адрес в мережі – 33, що забезпечить можливість масштабування мережі новими пристроями в майбутньому.

Згідно технічного завдання кінцевим вузлам мережі слід призначити статичну адресацію. Її представлено в таблиці Е.1 додатку Е. Віртуальним інтерфейсам маршрутизатора слід призначити останні доступні адреси діапазаон доступних адрес для кожної VLAN, тобто: для VLAN 1 – 192.168.0.62/27, VLAN 2 – 192.168.0.94/28, для VLAN 3 – 192.168.0.78/28, для VLAN 4 – 192.168.0.30/27.

2.5 Реалізація моделі комп’ютерної мережі

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

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

На наступному етапі потрібно призначити мережевим пристроям IP-адреси у відповідності із даними таблиці Е.1, додатку Е. Для цього слід

клікнути на назві робочої станції та у вікні, що відкриється вибрати вкладку Desktop, а тоді застосунок IP Configuration (рисунок 2.1) і вказати IP-адресу зі маскою та шлюз – віртуальний порт на маршрутизаторі, заданий на етапі проектування VLAN.

Призначення IP-адреси кінцевим вуздам мережі представлено на рисунку 2.6 на прикладі робочої станції WS_1.

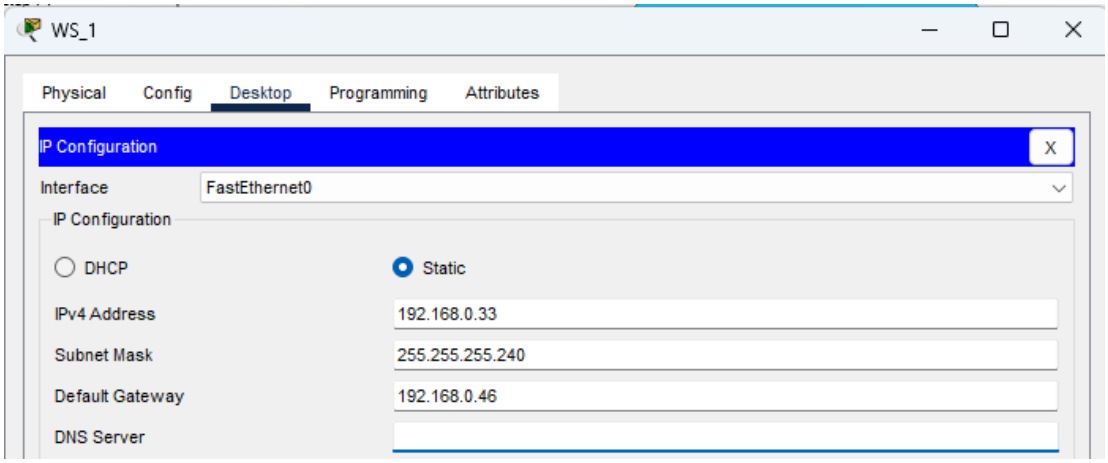


Рисунок 2.6 – Встановлення IP-адрес робочих станцій

Для налаштування безпровідних точок доступу потрібно відкрити вікно налаштування пристрою і у вкладці Config вибрати ліворуч розділ Port 1 і ввести SSID мережі, вказати тип аутентифікації WPA2-PSK та вказати пароль і тим шифрування, як це представлено на рисунку 2.7 для точки доступу AP1.

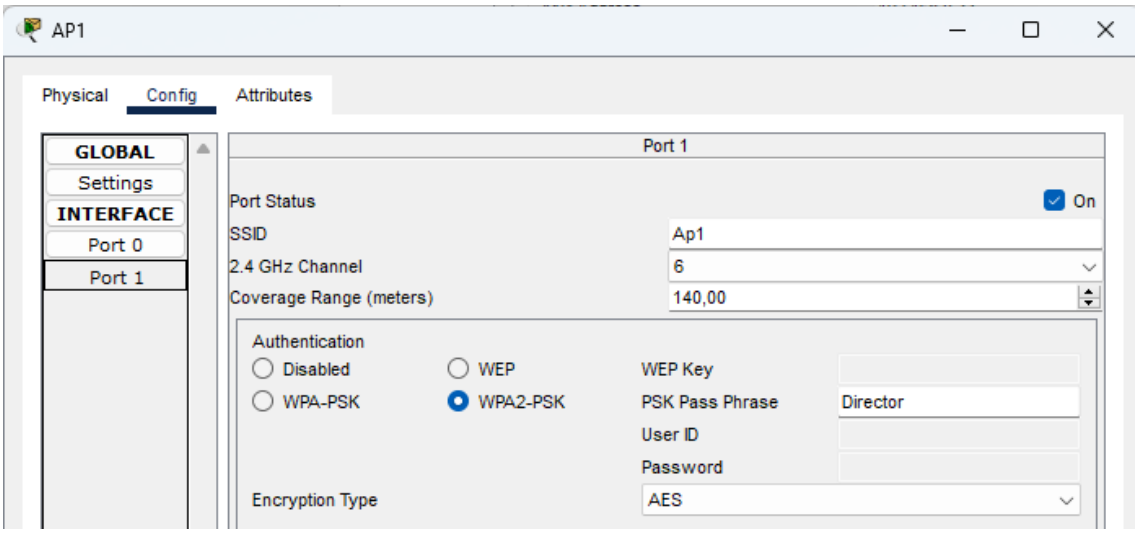


Рисунок 2.7 – Налаштування безпровідної точки доступу

При цьому потрібно для кожної точки доступу вказати свій SSID та пароль.

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

На наступному етапі слід творити та налаштувати віртуальні мережі VLAN. Для цього необхідно на кожному комутаторі вибрати вікно налаштувань та перейти в закладку CLI для роботи із командним рядком Cisco IOS та ввести всі команди налаштування VLAN, представлені в розділі 3.2.

Так само потрібно налаштувати інтерфейси на маршрутизаторі. Для цього слід клікнути на ньому і вибрати закладку CLI та ввести команди налаштування описані в розділі 3.2

Крім цього потрібно налаштувати маршрут за замовчуванням, який буде направляти всі пакети даних із адресами, які не належать до локальної мережі на інтерфейс пристрою ISP провайдера (IP-адреса 109.200.3.12) до кого під’єднано дану локальну мережу. Для цього в режимі глобального конфігурування необхідно ввести команду:

R(config)#ip route 0.0.0.0 0.0.0.0 109.200.3.12

Для налаштування FTP-сервера потрібно відкрити вікно його налаштування вказати йому статичну адресу 19.168.0.81/30 із шлюзом 192.168.0.82, так само як це виконано для робочих станцій. а тоді перейти до вкладки Sevices і вибрати розділ FTP (рисунок 2.8) для активування FTP-сервера.

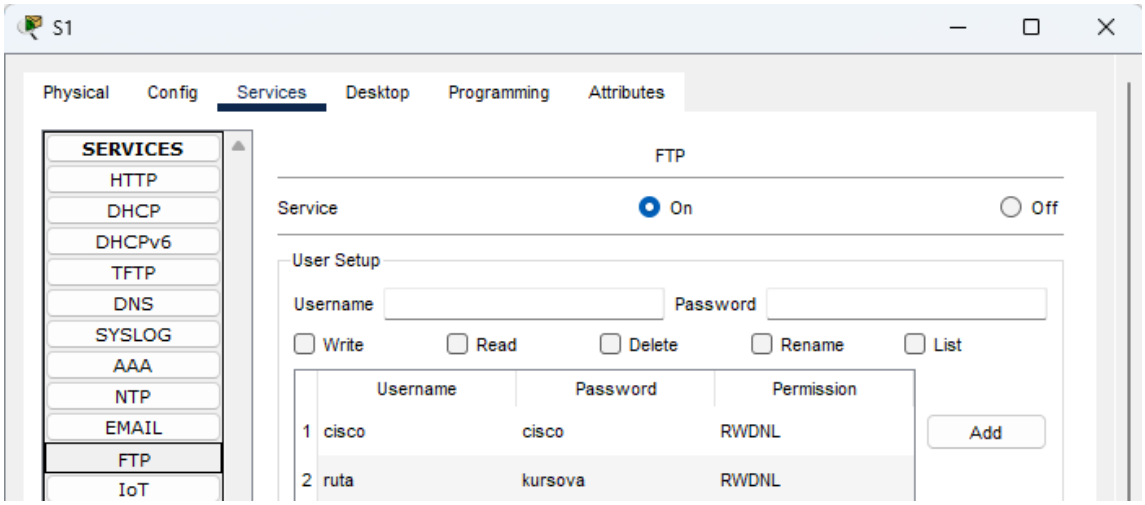


Рисунок 2.8 – Розгортання FTP-сервера у Cisco Packet Tacert

Остаточний проект мережі представлено у додатку Ж.

2.6 Обгрунтування вибору програмного забезпечення

Для функціонування серверів у мережі ПП «GALIT» потрібно вибрати та встановити серверні операційні системи та відповідне програмне забезпечення для них, в даному випадку програмне забезпечення FTP- та IPSec-сервера.

Для вибору серверної операційної системи потрібно врховувати цілий ряд критеріїв, серед яких: вартість, надійність в роботі, безпека систем захисту від хакерських атак (це найбільш фундаментальний критерій для серверної ОС) та періодичність оновлення. Для вибору операційної системи робочих станцій також важливим є простота і зручність у використані, оскільки ними працюють рядові користувачі, які не є глибоко обізнаними спеціалістами в галузі

адміністрування на відміну від серверних ОС з якими працюють підготовленні адміністратори.

Найбільш поширеними варіантами серверних ОС є продукти на платформі: Microsoft Windows Server, Ubuntu, Debian, Red Hat Enterprise Linux та FreeBSD.

До найбільш вагомих переваг Microsoft Windows Server відноситься в першу чергу універсальність її серверних служб та ролей (додатків, поштових серверів, файлових серверів та ін.). Однак, одним із проблемних місць цієї ОС є безпека, оскільки більшість вірусів пишуть спеціально для програмного забезпечення Microsoft. Хоча в останніх версіях системи питання безпеки значно покращено. Також недоліком цієї ОС можна вважати високу комерційну вартість цього продукту [2].

Debian – це один із найстаріших різновидів Linux-систем, який в першу чергу відзначається стабільністю в роботі. Дана ОС підтримує практично всі архітектури процесорів і може бути встановлено практично на будь-якому сервері. Ще одною перевагою є велика кількість репозиторій (програмних пакеті) для встановлення різноманітних служб. Сама операційна систем поширюється безкоштовно, проте техпідтримка є платною. Основним недоліком цієї ОС є дуже тривалі періоди між її оновленнями, оскільки всі оновлення дуже старанно і довго тестуються. Як наслідок в цій ОС дуже довго впроваджуються нові технології [9].

На відміну від попередньої ОС Ubuntu набагато частіше оновлюється і побудований на аналогічному ядрі та має спільну з Debian пакетну базу. Проте цей продукт є менш стабільним, проте значно швидше впроваджується підтримка нововведень апаратних технологій. Основні напрямки застосування цих ОС є сервери малих компаній із невеликим навантаженням.

Операційні система FreeBSD найстаріша із оглянутих операційна систем, що відзначається високою надійністю в роботі. Враховуючи високу надійність та стабільність у роботі, а також той фактор що вона відноситься до ОС із відкритим кодом та безкоштовною ліцензією, набула широкого поширення

серед мережевих адміністраторів. За статистикою її використовують 2/3 корпоративних серверів у світі [9].

Важливою перевагою цієї ОС є також одна із найбільш розширених підтримок мережевих протоколів та технологій. В чому вона значно випереджає системи на ядрі Linux. До недолік можна відзначити складнісь у адмініструванні та складність оновлення [9].

Проаналізувавши описані вище серверні операційні системи прийнято рішення використати для розгортання FTP та IPSec сервера операційну систему FreeBSD 14.0. При цьому для розгортання FTP-сервера буде використано програмне забезпечення proftpd, а для IPSec сервера – mpd5+racoon [10].

2.7 Тестування та налагодження мережі

Процес налагодження мережі включає наступні етапи:

- фізичне підключення пристроїв;
- встановлення мережевих IP-адрес кінцевим пристроям відповідно до таблиці IP-адрес представленої в додатку Е.1;
- налаштування конфігурації комутаторів робочих груп;
- налаштування конфігурації сегментуючих та центрального комутаторів;
- налаштування конфігурації маршрутизатора та маршрутизації VLAN;
- конфігурування FTP та IPSec севрера.

Після завершення розробки та практичної реалізації мережі необхідно перевірити її роботоздатність шляхом діагностики та тестування.

Процес тестування мережі складається із двох етапів. На першому етапі потрібно виконати фізичну перевірку кабельних з’єднань, візуально оглянувши роз’єми на правильність розташування провідників та їх фізичний контакт. Після цього протестувати наявність з’єднання за допомогою кабельних тестерів.

На другому етапі слід перевірити правильність налаштування протоколів TCP/IP для якісного проходження пакетів даних. Для цього існують як спеціалізоване програмне забезпечення так і утиліти вбудовані в самій операційні системи. В більшість операційних систем входять такі утиліти перевірки з'єднання як ping та tracert. Перша із них перевіряє якість з'єднання відправляючи пакети даних по IP-адресі або імені цільового вузла і очікуючи відповіді від нього. При цьому визначається затримки часу проходження пакетів.

Якщо замість відповіді буде отримано повідомлення "Request timed out" (перевищено час отримання відповіді), то це може означати відсутність з'єднання або час отримання пакету-відповіді перевищує допустимих 750 мілісекунд.

Утиліта tracert дозволяє визначити маршрут проходження пакету даних від комп'ютера відправника до вузла одержувача. Таким чином можна перевірити роботу протоколів маршрутизації, в даному випадку проектованої мережі ПП ПП «GALIT» маршрутизації між віртуальними підмережами.

Для перевірки мережевих налаштувань вузла слід скористатись утилітою ipconfig, яка показує фізичну MAC-адресу пристрою, логічну IP-адрсеу, адрсу шлюза виходу в Інтернет та DNS-сервера.

За допомогою утиліти netstat можна визначити статистику TCP/IP з'єднань, стан з'єднань, включаючи відкриті на комп'ютері порти та віддалені з'єднання.

А операційній системі Linux вбудовано утиліту tcpdump, яка дозволяє перехоплювати та аналізувати мережевий трафік на комп'ютері, дозволяючи визначити проблеми із мережевим з'єднанням та визначити, які саме пакети даних проходять через ПК.

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

На наступному етапі діагностики необхідно перевірити роботу та налаштування серверів.

На останок слід перевірити захищеність та швидкість Інтернет з’єднання.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

На серверному обладнані мережі слід розгорнути роботу сервісів FTP-сервера та IPSec-сервер. В якості серверної операційної системи використано FreeBSD (див. розділ 2.6).

FTP-сервер – це серверна роль, яка відповідає за зберігання великих сховищ файлів та мережевого доступу до них користувачів по протоколу прикладного рівня OSI-моделі, який має ідентичну назву – FTP. Цей протокол забезпечує передачу файлів між севром та клієнтом. При цьому підтримується аутентифікація користувачів за допомогою логіну та паролю. Також для під'єднання до FTP-сервера необхідно вказати його ім'я та порт (за замовчуванням 21 порт).

FTP-сервер може підтримувати анонімних користувачів, які авторизуються без власного паролю.

Підключення до FTP може відбуватись як в активному так і в пасивному режимі. В активному режимі з'єднання встановлюється надсиланням команди PORT. Але при використанні фаєрвола таке з'єднання може бути заблоковане. Тому необхідно використовувати пасивне з'єднання, коли клієнт отримує номер TCP-порту, до якого йому дозволено підключитися.

Передача фалів може здійснюватися у двох режимах: текстовий – для передачі файлів у текстовому форматі (звичайний текст, HTML, різні типи скриптів) та бінарному.

Основна проблема даного протоколу в тому, що дані передаються відкрито, тобто не захищено і не зашифровано, навіть дані аутентифікації передаються «відкритим» текстом. Щоб запобігти перехопленню даних, варто додатково використовувати шифрування даних, наприклад методом SSL [9].

ProFtpd + TLS. TLS – це популярний криптографічний протокол для захищеної передачі пакетів даних між вузлами, що можна налаштувати на операційній системі FreeBSD.

Приклад налаштування ProFtpd + TLS [9].

Інсталяці і запуск:

cd /usr/ports/ftp/proftpd

make config

make install

Змінимо proftpd.conf:

ee /usr/local/etc/proftpd.conf

DefaultRoot ~ – установка для кожного клієнта домашнього каталогу як кореневий і поточний;

IdentLookups off – відключення затримок передачі пакетів даних.

Далі слід створити SSL сертифікат для протоколу TLS. Для використання TLS нам необхідно створити сертифікат SSL в каталозі

/Usr/local/etc/proftpd/ssl.

Створимо каталог – # Mkdir /usr/local/etc/proftpd/ssl.

Далі генеруємо сертифіката [9]:

#Openssl req -new -x509 -days 365 -nodes -out

/usr/local/etc/proftpd/ssl/proftpd.cert.pem -keyout

/usr/local/etc/proftpd/ssl/proftpd/key/pem

Далі необхідно вказати реєстраційні дані.

Включаємо TLS в ProFtpd. Для цього необхідно зняти символи коментарів в конфігураційному файлі proftpd.conf:

ee /usr/local/etc/proftpd/proftpd.conf

Include /usr/local/etc/proftpd/tls.conf

Наступним кроком редагуємо конфігураційний файл tls.conf [9]:

ee /usr/local/etc/proftpd/tls.conf

TLSLog /var/log/proftpd/tls.log

TLSProtocol SSLv23

TLSOptions NoCertRequest

TLSACertificateFile /etc/proftpd/ssl/proftpd.cert.pem

TLSACertificateKeyFile /etc/proftpd/ ssl/proftpd.key.pem

TLSVerifyClient off

TLSRequired on

Перезапускаємо ProFtpd.

/usr/local/etc/rc.d/proftpd.sh

На завершальному етапі необхідно спробувати підключитися клієнтом, який підтримує SSL з'єднання.

Якщо в процесі конекту виникла проблема, то переглядаємо її опис в файлі /var/log/proftpd/tls.conf.

Якщо створені правила для ipfw, то необхідно додати правила, щоб вільно пропускати обидва типи з’єднань. В іншому випадку вонри будуть заблоковані фаєрволом.

Отже правила виключень:

ipfw add pass tcp from any to any 20

ipfw add pass tcp from any 21 to any

ipfw add pass tcp from any to any 21

ipfw add pass tcp from any 21 to any

Бажано під час конфігурування передбачити загальнодоступну папку для обміну даними клієнтів в мережі. Для цього створимо папку /home/public/files для зберігання загальнодоступних файлів (можна задати будь-яку іншу назву):

mkdir /home/public/files

Додаємо ProFTPd в автозавантаження операційної системи. Для цього у файлі /etc/rc.conf пропишемо рядок:

proftpd_enable = «YES»

Перезавантажуємо систему командою:

Shutdown -r now

На цьому базові налаштуванн FTP-серверу завершено. В процесі експлуатації даного серверу, налаштування можна змінювати шляхом відповідного написання додаткових правил.

3.1.2 Інструкція з налаштування IPSec-сервера

IPSec – набір протоколів тунелювання та безпеки мережевого рівня (шляхом шифрування та підтвердження справжності IP-пакетів), що дозволяють створити гнучке та надійне VPN-з'єднання. Для захищеності з'єднання IPSec використовує процедуру обміну ключами шифрування і є надбудовою над протоколом IP. В стек IPSec входять такі протоколи як:

- AH – відповідає за аутентифікацію та запобігання повторної передачі пакетів;
- ESP – шифрування інформації, що передається;
- SA – пов'язує алгоритми шифрування та аутентифікації (AH та ESP);
- ISAKMP – здійснює передачу та перевірку автентичності ключів.

Кожен із цих протоколів може працювати або в режимі транспортування (IP-заголовки залишаються незмінними, а шифрується вміст пакету) та тунелю (пакет разом із заголовком шифрується та інкапсулюється в новий пакет із тимчасовим заголовком.

У VPN побудованих по набору протоколів IPSec формування захищеного тунелю здійснюють компоненти віртуальної мережі, які діють на двох вузлах, між якими створюється тунель. Їх ще називають ініціатором та термінатором тунелю [7].

При цьому ініціатор створює нові пакети інкапсулюючи та шифруючи в них існуючі пакети і додають до них новий заголовок із адресою відправника та отримувача мережі VPN. При цьому у новий пакет може бути інкапсульовано дані будь-якого протоколу, а не лише IP, а в новому пакеті вони будуть перетворені в пакети IP. Після створення нового пакету він передається по логічному тунелю VPN, фізично використовуючи різну інфраструктуру Інтернет або іншої мережі. Після отримання IP-пакету термінатором він здійснює зворотну декапсуляції та дешифрування даних, видобуваючи заголовок внутрішнього пакету і зчитує з нього адресу одержувача в локальній

мережі і передає його для подальшого транспортування вже по локальній мережі [9].

В даній мережі слід налаштувати IPSec-сервер для підключення віддалених дистрибюторів до мережі ПП «GALIT». Для цього буде використано авторизацію по протоколу PSK і буде реалізовано на FreeBSD-сервері.

Для початку необхідно підготувати ядро системи і встановити декілька доповнень для роботи IPSec [9].

```
# cd /usr/
# fetch http://tech4u.pro/files/ipsec-patches-FBSD-14.0.diff
# patch < ipsec-patches-FBSD-14.0.diff
```

Далі слід відредагувати конфігураційний файл:

```
 # cp /usr/src/sys/Intel/conf/GENERIC /usr/src/sys/Intel/conf/IPSEC
 # ee /usr/src/sys/Intel/conf/IPSEC
 -ident          GENERIC
 +ident          IPSEC
 +options        IPSEC
 +options        IPSEC_NAT_T
 +options        IPSEC_DEBUG
 +options        IPSEC_FILTERTUNNEL
 +device         crypto
 +evice          enc
```

Тепер слід оновити ядро та перезавантажити систему:

```
# cd /usr/src
# make -j4 buildkernel KERNCONF=IPSEC
# make installkernel KERNCONF=IPSEC
# shutdown -r now
```

Після перезавантаження слід оновити порти та пакетний менеджер.

```
# cd /usr/ports/security/ipsec-tools/
# make extract
```

Після завершення інсталяції слід заблокувати пакет, оскільки після оновлення всі налаштування зникнуть:

pkg lock ipsec-tools

Далі слід налаштувати Racoon и IPSec:

#cp/usr/local/share/examples/ipsec-tools/racoon.conf /usr/local/etc/racoon/racoon.conf

cp /usr/local/share/examples/ipsec-tools/psk.txt /usr/local/etc/racoon/psk.txt

Відкриється текстовий файл, де потрібно в рядку isakmp вказати адресу даного IPSec-сервера (див.таблицю 2.3):

isakmp 192.168.0.81

Далі після рядка “authentication_method pre_shared_key;” вказати PSK ключ аутентифікації.

Після цього на відредагований файл psk.txt потрібно задати права доступу:

chmod 0600 psk.txt

На наступному кроці слід задати політику шифрування [9]:

ee /etc/ipsec.conf

+flush;

+spdflush;

+spdadd 0.0.0.0/0[0] 0.0.0.0/0[1701] udp -P in ipsec esp/transport//require;

+spdadd 0.0.0.0/0[1701] 0.0.0.0/0[0] udp -P out ipsec esp/transport//require;

Тепер можна встановити md5-vpn сервер:

ee /etc/ipsec.conf

pkg install mpd5

По закінчені інсталяції сервер слід перезавантажити ще раз.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування комутаторів та створення віртуальних підмереж

Для забезпечення розподілу мережі на відокремлені логічні підмережі із можливістю обмеження доступу між ними слід на канальному рівні поділити мережу на віртуальні мережі на основі стандарту 802.1q.

Віртуальні локальні мережі або VLAN – це логічне об’єднання окремих вузлів мережі (підмережа), які можуть перебувати в різних її сегментах і повністю ізольовані на канальному рівні OSI-моделі від інших вузлів, що не належать цьому об’єднанню. Отже, виходить, що не можливо по MAC-адресах передавати кадри між різними VLAN по їх MAC, тоді як всередині віртуальної мережі вони вільно передаються на канальному рівні не залежно від фізичної приналежності пристрою до певно сегменту мережі. Тобто, можна створити логічну підмережу незалежно до котрого із комутаторів під’єднано вузли, з’єднуючи у VLAN пристрої які значно віддалені територіально.

У мережі ПП «GALIT» , побудованій на основі 3 комутаторів потрібно створити чотири віртуальні мережі vlan_1, vlan_2, vlan_3, vlan_4 (див. рисунок 2.1), три із яких vlan_2, vlan_3, vlan_4 під'єднані до різних портів одного і того ж комутатора vlan1. Частину інтерфейсів цього комутатора використовується як порти доступу для кінцевих вузлів мережі vlan1.

Для створення віртуальних мереж VLAN на комутаторі потрібно увійти в режим глобального конфігурування комутатора Sw1 і ввести команду vlan <номер>, де <номер> – це номер створюваної мережі. Після цього слід вказати назву мережі командою name <назва>. Згідно із завданням, потрібно створити чотири мережі із номерами 101, 102, 103 та 104. Отже, для створення цих мереж потрібно вказати на кожному комутаторі наступні команди:

```
Sw1(config)#vlan 101
Sw1(config-vlan)#name vlan_1
Sw1(config-vlan)# vlan 102
Sw1(config-vlan)#name vlan_2
Sw1(config-vlan)# vlan 103
Sw1(config-vlan)#name vlan_3
```

Sw1(config-vlan)# vlan 104

Sw1(config-vlan)#name vlan_4

Sw1(config-vlan)#exit

Далі потрібно вибрати тип портів на комутаторах, які приймають участь у функціонуванні VLAN. При цьому інтерфейси комутатора, до яких безпосередньо підключені комп'ютери, що входять у VLAN (серед них буде і точка доступу, яка продовженням адресного простору провідної мережі на безпровідну) потрібно визначити як access-порти, оскільки, вони приймають і відправляють нетегований трафік окремої VLAN.

Тоді, як порти, що з'єднують комутатори між собою та під'єднують мережу до маршрутизатора слід визначити як trunc-порти, так як вони передають вже теговані пакети усіх VLAN разом.

У таблиці 3.1 представлено приналежність інтерфейсів кожного комутатора до відповідної мережі VLAN або до танкового типу. Позначення комутаторів відповідають рисунку 2.1.

Таблиця 3.1 – Типи інтерфейсів комутаторів та їх під’єднання

Комутатор	Назви інтерфейсів	Тип порту	Під’єднано	Номер VLAN або інтерфейс під’єднаного пристрою
1	2	3	4	5
Sw1	Fa0/1	Trunk	R1	Fa0/0
	Fa0/2	Trunk	Sw2	Fa0/1
	Fa0/3	Trunk	Sw3	Fa0/1
	Fa0/4	Trunk	Sw4	Fa0/1
	Fa0/5	Access	AP1	101
	Fa0/6 – Fa0/10	Access	WS_1 – WS_5	101
	Fa0/11	Access	AP2	101
	Fa0/12 – Fa0/19	Access	WS_6 – WS_13	101

	Fa0/20 – Fa0/22	Access	WS_50 – WS_52	101
Sw2	Fa0/1	Trunk	SW1	Fa0/2
	Fa0/3 – Fa0/8	Access	WS_14 – WS_20	102

Продовження таблиці 3.1

1	2	3	4	5
Sw3	Fa0/1	Trunk	SW1	Fa0/3
	Fa0/2	Access	AP3	103
	Fa0/3 – Fa0/12	Access	WS_21 – WS_30	103
Sw4	Fa0/1	Trunk	SW1	Fa0/4
	Fa0/2	Access	AP4	104
	Fa0/3 – Fa0/24	Access	WS_31 – WS_49	104

Для налаштування портів в режимі доступу до vlan1 виконується командами, приклад яких представлено для інтерфейсу FastEthernet0/5 комутатора Sw1

Sw1(config)# interface fa0/5

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 101

Для налаштування транкових портів виконується командами, приклад яких представлено для портів Fa0/1 та Fa0/2 комутатора Sw1:

Sw1(config)# interface fa0/1

Sw1(config-if)#switchport mode trunk

Sw1(config-if)# interface fa0/1

Sw1(config-if)#switchport mode trunk

Таким чином, аналогічними командами потрібно налаштувати усі порти комутаторів Sw1 – Sw4, відповідно до даних таблиці 3.1.

3.2.2 Інструкції з налаштування маршрутизатора доступу до Інтернет

На другому етапі розробки віртуальних мереж потрібно на інтерфейсі FastEthernet 0/0 маршрутизатора R, до якого підключено комутатор Sw1, створити три віртуальні підінтерфейси fastethernet0/0.101, fastethernet0/0.102, fastethernet0/0.103 та fastethernet0/0.104. Створюються підінтерфейси командою interface <назва> та командою ip address <адреса> <маска>, яка встановлює IP-адреси для них. Також потрібно вказати метод енкапсуляції пакетів командою encapsulation <метод>. В даному випадку використовувався метод DOT1Q.

Отже, для створення віртуальних підінтерфейсів потрібно увійти в режим глобального конфігурування маршрутизатора R та ввести наступні команди:

```
R(config)#interface fa0/0
R(config-if)#interface fastethernet0/0.101
R(config-subif)#encapsulation dot1Q 101
R(config-subif)#ip address 192.168.0.62 255.255.255.224
R(config-if)#interface fastethernet0/0.102
R(config-subif)#encapsulation dot1Q 102
R(config-subif)#ip address 192.168.0.94 255.255.255.240
R(config-if)#interface fastethernet0/0.103
R(config-subif)#encapsulation dot1Q 103
R(config-subif)#ip address 192.168.0.78 255.255.255.240
R(config-if)#interface fastethernet0/0.104
R(config-subif)#encapsulation dot1Q 104
R(config-subif)#ip address 192.168.0.30 255.255.255.224
R(config-if)#no shutdown
R(config-subif)#exit
```

Також на маршрутизаторі потрібно налаштувати інтерфейси для під’єднаня в окрему мережу сервера (IP-адреса 192.168.0.98/30) та для виходу в Інтернет (IP-адреса (109.200.3.100 /8):

```
R(config)#interface GigabitEthernet0/1/0
R(config-if)#ip address 109.200.3.100 255.0.0.0
R(config-if)#no shutdown
```

R(config-if)# interface FastEthernet0/1

R(config-if)#ip address 192.168.0.98 255.255.255.252

R(config-if)#no shutdown

R(config-if)#exit

3.3 Інструкції з налаштування засобів захисту мережі

Дуже важливим аспектом функціонування комп'ютерних мереж є питання їх захисту від загроз, які призводять до збоїв в роботі мережі, втрат або несанкціонованого доступу до інформації. Під загрозою слід розуміти набір певних факторів та умов які призводять до порушення роботи комп'ютерної мережі в цілому та даних, що передаються.

В загальному загрози можна поділити на умисні (свідоме заподіяння шкоди) та випадкові. До першої групи можна віднести порушення функ-ціонування мережі, несанкціоноване отримання даних, пошкодження даних та інші загрози. До другої – помилки внаслідок збоїв пристроїв, природні явища, нещасні випадки та інші форс-мажорі обставини. Значну частку всіх загроз становлять загрози пов'язані із людським фактором – не дотримання інструкцій (наприклад, порушення політик паролів), недостатня компетентність та інші [2].

З точки зору спрямованості загрози можна поділити на загрози конфіденційності, цілісності та доступності інформації..

Один зі способів захисту локальної мережі – це застосування фірмових мережевих пристроїв, таких як маршрутизатори, комутатори та брандмауери, які дозволяють установлювати правила безпеки на різних рівнях. Наприклад, на рівні маршрутизації можуть бути встановлені правила для фільтрації пакетів, що проходять через мережу, на рівні комутації - правила для контролю доступу до різних мережних портів.

Загроза конфіденційності полягає у отриманні доступу до інформації осіб які не маю на це повноважень. Це може відбутись, наприклад, внаслідок

випадкового делегування прав одного користувача іншому або шляхом несанкціонованого отримання зловмисником облікових даних користувача.

Загроза цілісності даних пов’язана із пошкодженням даних або їх модифікацією. Ці загрози можуть виникнути як внаслідок випадкового пошкодження в результаті збоїв обладнання або некваліфікованих дій користувача так і умисних дій зловмисника.

Загрози доступності полягає в унеможливленні або ускладненні доступу до даних, тобто коли дані можна отримати не із затримкою відносно відведеного для цього часу.

Також загрози можна поділити на внутрішні – виникають всередині певної інформаційної системи, в даному випадку комп’ютерної мережі, та зовнішні – внаслідок впливу зовнішніх факторів, наприклад, хакерська атака.

При розробці мережі слід врахувати всі можливі загрози та вразливості.

Для забезпечення безпеки локальної мережі також можуть використовуватись інші заходи, такі як:

- налаштування паролів та прав доступу до різних системних ресурсів і мережевих пристроїв;
- використання зашифрованого з'єднання (наприклад, за допомогою протоколу SSL/TLS) при передачі конфіденційної інформації;
- для віддаленого з’єднання до мережі слід створювати VPN мережі із зашифрованим трафіком. Досить дієвим рішенням цього завдання є використання набору протоколів IPSec для створення віртуальних VPN-тунелів між віддаленим користувачем і локальною мережею. Саме таку функцію реалізовано у даному проекті мережі (див. розділ 3.1.2);
- використання програмного забезпечення для виявлення та блокування потенційно шкідливих програм та кібератак;
- регулярне оновлення програмного забезпечення та операційної системи на мережевих пристроях та комп'ютерах, що підключені до мережі;
- проведення навчання користувачів з питань безпеки та захисту від кібератак.

Захист локальної мережі є комплексним процесом, який вимагає поєднання різних технічних та організаційних заходів.

Основними механізмами захисту мережевих пристроїв є налагодження паролів аутентифікації та механізмів авторизації, відключення протоколів та інших сервісів, які не використовуються в роботі корпоративної мережі, застосування функцій автоматичного підключення компонентів захисту, встановлення часових проміжків для підключення та активного використання, дозвіл виведення системних застережень.

Використовується три рівні парольного захисту це паролі на консольний доступ до пристрою, віддалений доступ по SSH або Telnet і пароль на вхід до привілейованого режиму.

Для введення паролю на консольний режим, потрібно вказати номер консолі (для більшості випадків консоль одна із порядковим номером 0) і задати пароль командою password. Після цього необхідно ввести команду login, щоб дозволити аутентифікацію під паролем. На наступному етапі потрібно активувати службу шифрування паролів, оскільки за замовчуванням пароль на консоль і віддалений доступ зберігаються у незашифрованому вигляді.

На всіх комутаторах та маршрутизаторі локальної мережі потрібно виконати наступні команди встановлення парою на консоль:

```
R(config)#line console 0
R(config-line)#password diplom
R(config-line)#login
R(config-line)#exit
R(config)#service password-encryption
```

При цьому в даній роботі в якості паролю введено “diplom”. Команда service password-encription призначена для того щоб пароль зберігався в зашифрованому вигляді.

На відмін від консолі через Telnet або SSH можна здійснити вхід на пристрій лише тоді коли на ньому встановлений пароль. Поки не налаштовано пароль віддалений доступ до пристрою неможливий. Крім цього, для доступу

пристрій повинен мати налаштовано IP-адресу. Для введення паролю на віддалений режим, потрібно перейти із режиму конфігурування у налаштування віртуальних терміналів "vty 0 4" (цифри це номери цих терміналів від 0 до 4). А далі налаштування аналогічні до консолі:

R(config)# line vty 0 4

R(config-line)#password diplom

R(config-line)#login

R(config-line)#exit

Команду шифрування паролів вказано при налаштуванні консолі, тому не потрібне її повторне введення.

Дуже важливим є встановити пароль на привілейований режим роботи, коли користувач вводить команду enable. Для того, щоб пароль на вхід у привілейований режим зберігався в зашифрованому вигляді слід ввести команди:

R(config)#enable secret diplom

Ще один рівень захисту мережі шляхом створення VPN-тунелів для підключення віддалених користувачів мережі розглянуто в розділі 3.1.2 даної кваліфікаційної роботи.

3.3 Інструкція з використання тестових наборів та тестових програм

Розглянемо основні етапи діагностики працездатності спроектованої комп’ютерної мережі ПП «GALIT».

На першому етапі слід протестувати мережу на фізичному рівні, тобто рівні фізичного з’єднання. На цьому рівні помилки пов’язані із відсутністю фізичного з’єднання між ПК та комутатором, або між комутаторами чи комутатором і маршрутизатором. Така помилка може бути викликана неправильним під’єднанням провідників в кабелі або його обривом.

Для усунення даної проблеми слід візуально перевірити якість контактів, роз'ємів та правильність розташування провідників в роз'ємі. Після цього перевірити з'єднання за допомогою кабельного тестера.

Також можна перевірити з'єднання під'єднаши роз'єм до мережєвої плати і візуально оглянути стан світлових індикаторів на платі і на порті комутатора. Він повинен світитись зеленим кольором. Якщо індикатор відсутній або червоного кольору, то фізичне під'єднання через кабель відсутнє.

Для тестування з'єднання за допомогою кабельного тестера необхідно [5]:

- перший кінець кабелю слід увести в роз'ємом на тестері, а інший під'єднати до роз'єму на кінцевику;
- натиснути кнопку початку на тестері;
- при справному кабелі будуть загоряться індикатори на кожному з модулів. Якщо один із індикаторів не загоряється, то зв'язку на даному провіднику немає.

На завершальному етапі потрібно виконати тестування мережі на програмному рівні.

Існує велика кількість утиліт, які можна використовувати для тестування роботи локальної мережі, як в будованих в операційну систему так і спеціалізованих. Серед них можна відзначити:

- ping – дозволяє перевірити доступність мережевого пристрою по його IP-адресі;
- Traceroute: – відстежує маршрут, який проходить пакет в мережі, від комп'ютера відправника до комп'ютера одержувача;
- Netstat – перевіряє статус з'єднань між комп'ютерами в мережі, включаючи відкриті порти та інформацію про з'єднання;
- Nmap – здійснює сканування мережі на наявність активних комп'ютерів та відкритих портів. Її часто використовують для виявляти Вона уразливості в мережевій інфраструктурі;
- iperf – дозволяє визначати швидкість передачі даних між кінцеивми вузлами в мережі;

- Wireshark – надзвичайно потужна утиліта для аналізу мережевого трафіку. Допомогає знайти проблеми з мережевим з'єднанням, такі як затримки, пакетні втрати, помилки та інші.

3.4 Інструкція з експлуатації та моніторингу в мережі

Моніторинг роботи мережевих сервісів та мережевих вузлів вцілому вузлів є наріжним каменем успішної експлуатації локальної мережі. Він базується на централізованому зборі критичної інформації, необхідної для роботи мережі. Дана інформація включає в себе мережеві метрики, які сигналізують про значення параметрів, пов'язані з певними часовими мітками.

Аналізуючи відповідні мітки на протязі фіксованих проміжків часу, можна зробити висновки про рівень використання системних ресурсів. Для збору міток з серверів будуть використані програми nope_exporter та Prometheus, які забезпечують агрегацію та зберігання даних у базі даних [4].

Для аналізу цих даних та побудови графіків буде використано програмний продукт Grafana [4].

Для отримання комплексної інформації слід збирати і аналзувати інформацію із log-файлів, які створюються і збираються серверами мережі. Для цього буде використано:

- стек ElasticSearch – це база даних подій;
- Fluent-Bit – здійснює збір файлів та їх пересилка в базу;
- Kibana – візуалізації даних, їх аналіз шляхом запитів до бази.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Економічна частина кваліфікаційної роботи використовується для здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для приватного підприємства «GALIT» і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Ці розрахунки необхідно повести в декілька етапів:

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

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно звести у таблицю 4.1 дані витрат часу по окремих операціях технологічного процесу. Виконавцями стадій технологічного процесу будуть: керівник, інженер, технік.

В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Постановка задачі, формування технічного завдання на проект локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проекту	15
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі ПП «GALIT». Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури ПП «GALIT» для сегментування локальної мережі на підмережі.	Інженер	15
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Технік	25

Продовження таблиці 4.1

1	2	3	4
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	20
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
		Разом	80

Сумарний час виконання операцій технологічного процесу проектування мережі становить 80 години, з них 15 годин – робота керівника проекту, 40 години – інженера, 25 години – техніка.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці – грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого власником підприємства працівникові за виконану роботу.

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

Основна заробітна плата розраховується за формулою:

$$З_{осн} = Т_с \cdot К_г, \quad (3.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Виходячи з рекомендованих тарифних ставок встановимо таку ставку для керівник проекту – 100 грн, інженера – 90 грн./год. а для техніка – 60 грн./год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 15 \cdot 100 = 1\ 500$ грн.
- інженера – $З_{осн2} = 40 \cdot 90 = 3\ 600$ грн.
- техніка – $З_{осн3} = 25 \cdot 60 = 1\ 500$ грн.

Сумарна основна заробітна плата становить

$$З_{осн}=1\ 500 +3\ 600 + 1\ 500 =6\ 600 \text{ грн.}$$

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

$$З_{дод.}=З_{осн.} \cdot К_{допл.}, \quad (3.2)$$

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника $З_{дод1}=1\ 500 \cdot 0,13= 195$ грн.
- інженера $З_{дод1}=3\ 600 \cdot 0,13= 468$ грн.
- техніка $З_{дод3}=1\ 500 \cdot 0,13= 195$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=195 + 468 + 195= 858 \text{ грн.}$$

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

$$В_{о.п.}=З_{осн.} + З_{дод} \quad (3.3)$$

Отже, загальні витрати на оплату праці становлять:

$$В_{о.п.}= 6\ 600 + 858 = 7458 \text{ грн.}$$

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

$$В_{с.з.} = ФОП \cdot 0,22, \quad (3.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з}= 7458 \cdot 0,22= 1640,76 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/	Категорія працівників	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тарифна ставка, грн.	К-сть відпрац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	100	15	1500	195		
2	Інженер	90	40	3600	468	-	-
3	Технік	60	25	1500	195	-	-
			Разом	6600	858	1640,76	9098,76

Отже, загальні витрати на оплату праці становлять 9098,76 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{BI} = q_i \cdot P_i \qquad (3.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{Bi} \qquad (3.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

п/п	Найменування матеріальних ресурсів	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа 6U	шт.	2	3800	7600
2	Патчпанель 24 порти, кат. 6	шт.	2	1200	2400
3	Розетка RJ-45 (категорія 6)	шт.	53	117	6201
4	Роз’єм 8P8C (пачка 100 шт)	шт.	2	631	1262
5	Короб (середня ціна для різного січення)	м.	130	120	15600
6	Гофрована трубка	м.	10	35	350
7	Кабель UTP (кат. 6) (бухта)	шт.	4	5310	21240
8	Патчкорди (кат. 6)	шт.	53	52	2756
9	Кабель опотоволоконний	м.	2	25	50
10	Конектор SC	шт.	2	35	70
11	Маршрутизатор Cisco ISR4221/K9	шт.	1	54706	54706
12	Комутотар Allied Telesyn AT-x600-24Ts	шт.	4	16680	66720
13	Безпровідна точка доступу TP-LINK EAP110	шт.	4	1399	5596
14	Джерело безперебійного живлення APC Back-UPS Pro 1200VA	шт.	2	3625	7250
Р а з о м			-	-	191801

Отже, загальна сума матеріальних витрат на розробку мережі становить 191801 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \quad (3.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

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

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

4.5 Визначення транспортних затрат

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

$$Т_в = З_{м.в} \cdot 0,08...0,1, \quad (3.8)$$

де $Т_В$ – транспортні витрати.

Отже,

$$Т_В = 191801 \cdot 0,08 = 15344,08 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

В процесі використання основних фондів виконуються заходи що до їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації. Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення. Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%} \cdot Т \qquad (3.9)$$

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

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

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 26500 грн., тому, то амортизаційні відрахування становлять:

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

4.7 Обчислення накладних витрат

Накладні витрати – це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом

певних умов роботи по організації, управлінню та обслуговуванню виробництва.

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

$$Н_в = В_{о.п.} \cdot 0,2...0,6,, \qquad (3.10)$$

де $Н_В$ – накладні витрати.

$$Н_В = 7458 \cdot 0,5 = 3729 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

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

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

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	7458	3,39
Відрахування на соціальні заходи	1640,76	0,75
Матеріальні витрати	191801	87,15
Витрати на електроенергію	35	0,02
Транспортні витрати	*15344,08*	6,97
Амортизаційні відрахування	70,67	0,03

Накладні витрати	3729	1,69
Собівартість	220078,51	100

В таблиці 3.4 зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати, тобто собівартість ($С_в$) НДР розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + Т_в + А + Н_в \quad (3.11)$$

Отже, собівартість дорівнює C_B=*220078,51* грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{С_в \cdot (1 + Р_{рен}) + К \cdot В_{ні}}{К} \cdot (1 + ПДВ) \quad (3.12)$$

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

$К$ – кількість замовлень, од.;

$B_{і.н}$ - вартість носія інформації, грн.;

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

Отже, ціна НДР становить:

$$Ц = 220078{,}51 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 343322{,}47 \text{ грн}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності (ТОК).

$$\text{ЧТВ} = -K_{\text{В}} + \sum_{i=1}^{t} \frac{\Gamma_{\text{в}}}{(1+i)^t} \geq 0, \quad (3.13)$$

де $K_в$ – затрати на проект;

$Г_В$ – грошовий потік за t-ий рік;

t - відповідний рік проекту;

i –величина дисконтної ставки (10-15%).

$$\text{ЧТВ} = -220078{,}51 + \frac{202001{,}96}{1+0{,}1} + \frac{202001{,}96}{(1+0{,}1)^2} = 130503{,}41 \text{ грн}$$

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

Термін окупності визначається за формулою:

$$T_{ОК} = T_{\text{ПВ}} + \frac{H_В}{\Gamma_{\text{пр}}} \quad (3.14)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років;

$H_В$ – невідшкодовані витрати на початок року, грн.;

$Г_{ПР}$ – грошовий потік на початку року, грн..

$$T_{ОК} = 1 + \frac{36440{,}36}{202001{,}96} = 1{,}2$$

Всі дані внесемо в зведену таблицю 3.5 економічних показників.

Таблиця 3.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	220078,51 грн.
2.	Плановий прибуток, грн.	123243,96 грн.
3.	Ціна, грн.	343322,47 грн.
4.	Чиста теперішня вартість	130503,41 грн.
5.	Термін окупності, рік	1,2

Загальна вартість розробленої комп'ютерної мережі для ПП «GALIT» становить 343322,47 грн. Термін окупності становить 1,2 роки, що є хорошим

показником. Таким чином, можна зробити висновок, що проведення робіт по розробці даної мережі є доцільним та економічно вигідним

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Безпека експлуатації електрообладнання в ПП “GALIT”

Приватне підприємство “Galit” виготовляє та виконує сервісне обслуговування стоматологічного устаткування. Цей процес пов’язаний із використанням виробничого обладнання робота якого заснована на використані електрики, тому на перший план виступають заходи щодо дотримання техніки безпеки при експлуатації електрообладнання. Ці заходів, спрямовані на запобігання небезпечному впливу електричного струму на персонал.

Для зниження існуючої небезпеки ураження персоналу ПП «GALIT»електричним струмом передбачені наступні заходи:

- використання сучасного технічно досконалого обладнання;
- обдумане розміщення устаткування, що забезпечує його вільне і зручне обслуговування;
- надійне і швидкодіюче автоматичне відключення частин електро-обладнання, що випадково опинилися під напругою;
- заземлення всіх металевих частин електроустаткування і елементів електроустановок, які можуть опинитися під напругою внаслідок пошкодження ізоляції;
- застосування попереджувальної сигналізації, написів і плакатів;
- занулення, захисне заземлення і зрівнювання потенціалів;
- при ремонтах передбачається місцеве керування;
- застосовується подвійна ізоляція приладів, тобто електрична ізоляція, що складається з робочої і додаткової ізоляції;
- використовуються блокування для попередження помилкових дій персоналу при переключеннях у розподільчих пристроях на підстанції;
- струмоведучі частини розташовуються на недоступній висоті та в недоступному місті;

- встановлюється захисне заземлення ($R_{заз}$ = 4 Ом);

- в електроустановках роботи виконуються персоналом, який має 4 групу з електробезпеки (електроустановки вище 1 кВ);

- до робіт на струмоведучих частинах електроустановок під наведеною напругою допускаються працівники, які пройшли навчання з методів безпечного проведення таких робіт та в яких перевірено знання та видано посвідчення про надання права на проведення таких робіт;

- при введенні в експлуатацію нових електроустановок або тих, що вийшли з ремонту, проводяться тестування.

На підприємстві розташовано електропідстанцію. Для захисту від природніх негативних явищ, таких як грозова блискавка на підприємстві встановлено блискавковідводи, які з'єднуються струмовідводами з загальним заземлюючим пристроєм. На підстанції заземлюючий пристрій є спільним з захисним заземленням. Опір блискавковідводів розраховано таким чином, щоб він не перевищував 10 Ом.

У системі електропостачання забезпечено захист людей від ураження електричним струмом як при відсутності пошкодження в електроустановці, так і при його наявності. Для цього застосовано поєднання заходів захисту від прямого і непрямого дотику. Як заходи захисту при непрямому дотику застосовані: автоматичне відключення живлення; ізолюючі зони; система зрівнювання потенціалів; електричне розділення ланцюгів.

Для електрообладнання, яке може зберігати небезпечний електричний заряд після відключення, для запобігання дотику до нього передбачено виконувати попереджувальні написи.

Для забезпечення автоматичного відключення живлення передбачена система заземлення і система зрівнювання потенціалів, а також забезпечена селективність захисних пристроїв, які здійснюють це відключення.

5.2 Способи і засоби гасіння пожеж

Комплекс заходів, спрямованих на ліквідацію пожежі, що виникла, називається пожежогасінням.

Основою пожежогасіння є примусове припинення процесу горіння. На практиці використовують декілька способів припинення 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 із зовні 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).

Спосіб хімічного гальмування реакцій горіння полягає у введенні в зону горіння галоїдно-похідних речовин (бромисті метил та етил, фреон та інше), які ігри 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 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 охолоджування 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.

Вибір вогнегасної речовини залежить від характеру пожежі, властивостей і агрегатного стану речовин, що горять, параметрів пожежі (площі, інтенсивності, температури горіння тощо), виду пожежі (у закритому або відкритому повітрі), вогнегасної здатності щодо гасіння конкретних речовин та матеріалів, ефективності способу гасіння пожежі.

Оскільки вода є основною вогнегасною речовиною, необхідно приділити особливу увагу створенню та працездатності надійних систем водопостачання.

Відповідно до протипожежних норм, кожне промислове підприємство обладнують пожежним водопроводом. Він може бути об’єднаним з господарсько-питним або водопроводом, який використовують у виробничому процесі. Воду також можна подавати до місця пожежі з водоймищ річок або підвозити в автоцистернах.

Основними елементами устаткування водяного пожежогасіння на об’єктах є пожежні гідранти, пожежні крани, пожежні рукави, насоси та ін.

Пожежні гідранти використовують для відбору води із зовнішнього водопроводу. Біля місця їх розташування повинні бути встановлені покажчики з нанесеними на них: літерним індексом “ПГ”, цифровими значеннями відстані в метрах від покажчика до гідранта, внутрішнього діаметра трубопроводу в міліметрах, зазначенням виду водопровідної мережі (тупикова чи кільцева).

Пожежний кран являє собою комплект пристроїв, який складається із клапана (вентиля), встановленого на пожежному трубопроводі і обладнаного пожежною з’єднувальною головкою, та пожежного рукава з ручним стволом.

Пожежні крани повинні розміщуватись у вбудованих або навісних шафах, які мають отвори для провітрювання і пристосовані для опломбування та візуального огляду їх без розкривання. Пожежні рукави необхідно утримувати сухими, складеними в “гармошку” або скатку, приєднаними до кранів та стволів. Не рідше одного разу на 6 місяців їх треба розгортати та згортати заново. На дверцятах пожежних шафок повинні бути вказані після літерного індексу “ПШ” порядковий номер крана та номер телефону для виклику пожежної охорони.

Для ліквідації невеликих осередків пожеж, а також для гасіння пожеж у початковій стадії їх розвитку силами персоналу об’єктів, застосовуються первинні засоби пожежогасіння. До них належать: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна або повсті, ящики з піском, бочки з водою, пожежні відра, совкові лопати), пожежний інструмент (гаки, ломи, сокири тощо). їх застосовують для ліквідації невеликих загорянь до приведення в дію стаціонарних та пересувних засобів гасіння пожежі або до прибуття пожежної команди. Кожне приміщення, відділення, цех, транспортні засоби повинні бути забезпечені такими засобами у відповідності з нормами.

Серед первинних засобів пожежогасіння особливе місце займають вогнегасники. Залежно від вогнегасних речовин, що використовуються, вогнегасники ділять на пінні, газові та порошкові.

Пінні вогнегасники застосовують для гасіння твердих та рідких горючих матеріалів, за виключенням речовин, які здатні горіти та вибухати при взаємодії з піною. Також ними не можна гасити електрообладнання, що знаходиться під напругою.

За способом утворення піни пінні вогнегасники поділяються на хімічні та повітряно-механічні.

Заряд хімічно-пінного вогнегасника ВХП-10 складається з кислотної та лужної частин. При приведенні вогнегасника в дію кислотна та лужна складові змішуються, і відбувається хімічна реакція з інтенсивним виділенням вуглекислого газу. Частина цього газу іде на утворення піни з розчину, який

містить піноутворювач. Інша частина створює тиск (до 1 М Па), необхідний для викиду піни. Час дії вогнегасника – 60 с, довжина струменя – 6-8 м, кратність піни – 8-10. У повітряно-пінних вогнегасниках піна утворюється завдяки механічному перемішуванню розчину піноутворювача стиснутим повітрям, яке міститься у спеціальному балончику. Вони випускаються двох типів: ПП 11-5 та ВПП-10. Кратність піни цих вогнегасників – 55, дальність викиду піни – 4,5 м.

Вуглекислотні вогнегасники випускають трьох типів: ВВ-2, ВВ-5 та ВВ-8 (цифри показують місткість балону у літрах). їх застосовують для гасіння рідких та твердих речовин (крім тих, що можуть горіти без доступу повітря), а також електроустановок, що знаходяться під напругою до 1000 В.

Вуглекислота у вогнегаснику знаходиться у рідкому стані під тиском 6-7 МПа. При відкритті вентиля балона вогнегасника за рахунок швидкого адіабатичного розширення вуглекислий газ миттєво перетворюється у снігоподібну масу, у вигляді якої він і викидається з конусного дифузора вогнегасника. Час дії вогнегасників цього типу 25-40 с, довжина струменя 1,5-3 м.

Вуглекислотно-брометилові вогнегасники ВВБ-3 та ВВБ-7 за зовнішнім виглядом та будовою мало відрізняються від вуглекислотних, їх заряджають сумішшю, що складається із 97% бромистого етилу та 3% вуглекислого газу. Завдяки високій змочувальній здатності бромистого етилу продуктивність цих вогнегасників у 4 рази вища продуктивності вуглекислотних.

Порошкові вогнегасники призначені для гасіння твердих, рідких та газоподібних горючих речовин та електроустановок під напругою до 1000 В. Вид матеріалів та речовин, горіння яких можна гасити, залежить під типу порошку. Промисловість випускає порошкові вогнегасники марок ВП-1, ВП-2, ВП-5, ВП-50 та інші.

Вибір типу і розрахунок необхідної кількості вогнегасників проводиться в залежності від їх вогнегасної здатності, граничної площі, класу пожежі у приміщенні чи об’єкта, що потребує захисту.

Громадські будівлі та споруди промислових підприємств повинні мати на кожному поверсі не менше двох ручних вогнегасників. При захисті приміщень, у яких знаходяться електронно-обчислювальні машини, копіювальна та інша оргтехніка, а також телефонних станцій, архівів тощо, необхідно враховувати специфіку вогнегасних речовин у вогнегасниках, що можуть призвести під час гасіння пожежі до псування обладнання. Такі приміщення рекомендується забезпечувати вуглекислотними вогнегасниками з урахуванням граничнодопустимої концентрації вогнегасної речовини.

Максимально допустима відстань від можливого осередку пожежі до місця розташування вогнегасника має бути: 20 м – для громадських будівель та споруд, 30 м – для приміщень категорії А, Б, В (горючі гази та рідини); 40 м – для приміщень категорії В і Г; 70 м – для приміщень категорії Д.

Приміщення, обладнані стаціонарними установками автоматичного пожежогасіння, комплектуються вогнегасниками на 50% їх розрахункової кількості.

Для гасіння великих загорянь у приміщеннях категорій А, Б, В застосовують стаціонарні установки водяного, газового, хімічного та повітряно-пінного гасіння.

5.3 Система менеджменту охорони праці та промислової безпеки на підприємстві

Технологічний прогрес й інтенсивний тиск конкуренції стрімко змінюють умови праці, його процеси й організацію. Першорядне значення належить законодавству, але саме по собі воно недостатнє для того, щоб управляти цими змінами і попереджати нові небезпеки і ризики. Організації теж повинні постійно реагувати на зміни, що відбуваються у сфері охорони і безпеки праці, і розробляти ефективні відповіді у вигляді динамічних стратегій управління.

Питання промислової безпеки за значущістю порівнюють з проблемами охорони навколишнього середовища і питаннями збереження миру. Техносфера почала становити для людини серйозну небезпеку.

Хвороби і травми не є неминучими супутниками трудової діяльності, а бідність не може служити виправданням неуваги до безпеки і здоров'я працівників.

Позитивний вплив впровадження систем охорони здоров'я і безпеки персоналу на рівні організації як на зниження небезпек і ризиків, так і на продуктивність, нині визнано урядами, роботодавцями і працівниками в усьому світі.

Багато організацій виявляють зацікавленість в ефективності і демонстрації можливостей управління охороною праці (охороною здоров'я і безпекою) працівників (персоналу).

Відомий британський стандарт В8 8800-96 «Настанова з систем управління охороною здоров'я і безпекою персоналу» (Сиіде Оссираііопаї ЬеаІШ апд ваГеїу шапа§ешепІ вувіешв) і розроблений на його основі міжнародний стандарт ОН8А8 18001-99 «Системи управління охороною здоров'я і безпекою персоналу. Вимоги» (Оссираііопаї НеаІШ апд 8аГеІу Аввеввшепі 8егіев) орієнтовані на створення системи управління охороною праці організації, яка у вигляді підсистеми могла б бути об'єднана з іншими підсистемами системи управління (менеджменту) в рамках єдиної інтегрованої системи управління (менеджменту) організації.

Завдання Системи менеджменту охорони праці і промислової безпеки (СМОПіПБ)

Система менеджменту охорони праці і промислової безпеки створює основу для здійснення заходів з охорони праці і здоров'я на виробництві, що забезпечує підвищення їх ефективності й інтеграцію в загальну діяльність підприємства.

Системи менеджменту охорони праці і промислової безпеки базуються на стандартах, які чітко визначають процес досягнення безперервного поліпшення роботи з охорони праці і здоров'я, а також виконання вимог законодавства. СМОПіПБ відповідно до вимог ОН8А8 18001 — це система менеджменту, що дозволяє оцінити виробничі небезпеки, ідентифікувати пов'язані з ними ризики

і ефективно управляти ними. Унаслідок впровадження СМОПіПБ можливості виникнення аварійних ситуацій зводяться до мінімуму, знижуються виробничі ризики, забезпечується належний рівень охорони здоров'я персоналу і дотримання техніки безпеки на робочих місцях. Консалтингові компанії пропонують розробити, впровадити і сертифікувати СМОПіПБ за визнаною у всьому світі специфікацією ОН8Л8 18001.

Сертифікація дозволяє:

- зменшити ризики;
- отримати конкурентну перевагу;
- діяти відповідно до вимог законодавства;
- підвищити ефективність роботи в цілому;
- полегшити процедуру контролю з боку державних органів;
- підвищити рівень задоволеності персоналу.

ОН8А8 18001 є стандартом, на базі якого проводиться перевірка Систем менеджменту охорони праці і промислової безпеки. Передумовою його розробки стала потреба компаній в ефективній роботі з охорони праці і здоров'я.

Міжнародний стандарт ОН8А8 18001 був розроблений за участю національних органів зі стандартизації низки країн – Великобританії, Японії, ПАР, Ірландії, а також фірм і дослідницьких організацій.

Створюючи систему, засновану на принципах ОН8А8 18001, організація не зазнає

На додаток до ОН8А8 18001 було видано стандарт 0Н8А8 18002, який містить роз'яснення до вимог стандарту і настанову зі створення системи. Цей інтегрований пакет є зручним засобом для проходження сертифікації і дозволяє:

- виявити аспекти діяльності, що впливають на безпеку та здоров'я, і дістати доступ до відповідних законодавчих актів;

- визначити цілі з поліпшення діяльності і розробити програму щодо їх досягнення з реалізацією постійного контролю, тим самим забезпечуючи постійне вдосконалення.

Початок розробки системи менеджменту охорони праці і промислової безпеки передбачає вибір стратегії розробки системи, побудованої на наступних важливих принципах, на які варто звернути особливу увагу:

Принцип 1. Прихильність керівництва і політика у сфері охорони праці і промислової безпеки.

Принцип 2. Планування і реалізація політики у сфері охорони праці і промислової безпеки організації.

Принцип 3. Впровадження, включаючи розвиток навиків і розробку методик, необхідних для реалізації політики у сфері охорони праці і промислової безпеки.

Принцип 4. Оцінка коригувальних дій і вимірювання ефективності функціонування системи менеджменту охорони праці і промислової безпеки.

Принцип 5. Затвердження і структурне вдосконалення функціонування системи охорони здоров'я і безпеки персоналу.

Компанія може почати підготовку до сертифікації з оцінки переваг уже наявної системи менеджменту охорони праці й промислової безпеки (системи охорони праці) таких, як підтверджене виконання нормативних вимог і відсутність позовів щодо відповідальності.

Первинна оцінка аспектів системи управління охороною праці і промислової безпеки полягає у визначенні фактичного стану справ у компанії, яке повинне бути описане й оцінене.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи розроблено комп'ютерну мережу ПП «GALIT», підібрано та зконфігурувано мережеве обладнання, відповідно основним принципам побудови мереж, методам та засобам їх функціонування. В процесі розробки мережу поділено на чотири віртуальні сегменти шляхом створення віртуальних мереж VLAN 1 – VLAN 4, для них розраховано адресний простір, створено конфігураційні файли для всіх мережевих пристроїв, виконано моделювання мережі засобами Cisco Packet Tracer.

Мережу побудовано на основі гібридної топології, яка поєднала провідну топологію розширеної зірки та безпровідну комірчасту. При цьому забезпечено безпровідний зв'язок більше як для 25% відсотків робочих комп'ютерів (14 із 52 кінцевих вузлів мережі). З метою підвищення надійності для цих пристроїв зарезервовано також можливість провідного під'єднання під тими ж мережевими налаштуваннями та у ту саму VLAN.

Для всіх пристроїв встановлено статичну адресацію по протоколу IPv4 та статичну маршрутизацію із вказанням маршруту за замовчуванням в Інтернет.

Налаштовано захист мережевих пристроїв шляхом їх аутентифікації через пароль на консольний, віддалений доступ по SSH або Telnet.

Для зберігання та обміну файлами налаштовано FTP-сервер під операційною системою FreeBSD, як одною із найбільш стабільних та надійних серверних операційних систем. Крім, цього для віддаленого доступу ПП «GALIT» налаштовано IPSec-сервер на тій ж операційною системою FreeBSD. Це забезпечить створення захищених VPN-тунелів для віддаленого з'єднання із мережею та її ресурсами.

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

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

ПЕРЕЛІК ПОСИЛАНЬ

1. Базові поняття мережевих технологій. Доступно: http://um.co.ua/8/8-17/8-1748.html. Дата звернення: 5.03.2024.

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

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

4. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Навчальний посібник. - Вид. 2-ге., доп. - Львів.: Афіша, 2000. - 176с.

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

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

7. Allied Relesis URL: https://www.alliedtelesis.com/products/switches. - (Дата звернення: 2.06.2024).

8. Cisco 4221 Integrated Services Router URL: https://www.cisco.com/c/en/us/ support/routers/4221-integrated-services-router-isr/model.html. (Дата звернення: 4.06.2024).

9. FreeBSD у деталях. Про плюси та мінуси системи URL: https://hyperhost.ua/info/uk/freebsd-u-detalyax-pro-plyusi-ta-minusi-sistemi. (Дата звернення: 14.05.2024)

10. FreeBSD 14 URL: https://www.freebsd.org/releases/14R/schedule/. (Дата звернення: 20.05.2024)

11. x600-24Ts URL: https://www.alliedtelesis.com/ua/en/products/switches/x600-24ts#accessories-tab. (Дата звернення: 1.06.2024).

12. Джерело безперебійного живлення APC Back-UPS 1500 BA, авторегулювання напруги, 230 В, СНД URL: https://www.apc.com/ua/uk/product/BR1500G-RS. (Дата звернення: 7.06.2024).

13. КПВ-ВП (250) URL: https://lantorg.com/products/odeskabel-kpv-vp-250-4h2h057-utp---cat6-vnutrenniy- korobka-305m/. (Дата звернення: 6.06.2024).

14. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 29.05.2024).

15. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 29.05.2024).

16. Поширені питання про життєвий цикл–Windows URL: https://learn.microsoft.com/uk-ua/lifecycle/faq/windows. (Дата звернення: 19.05.2024).

17. Сервер двопроцесорний TOWER PowerUp #51 Xeon E5 2680 v4 x2/256 GB/HDD 6 TB/SSD 512GB x2 Raid/Int Video. URL: https://powerup.ua/server-dvukhprotsessornyy-tower-powerup-51-xeon-e5-2680-v4-x2-256-gb-hdd-6-tb-ssd-480-gb-kh2-raid-int-video/. (Дата звернення: 24.05.2024)

18. Телефонна + комп'ютерна розетка RJ11 + RJ45, кат. 6, неэкр. UTP з пружинними затискачами, Алюміній, Sedna SDN5200160. URL: https://schneider.kiev.ua/telefonna--kompyuterna-rozetka-rj11--rj45-kat-6-neekr-utp-z-pruzhinnimi-zatiskachami-alyuminij-sedna-sdn5200160. (Дата звернення: 6.06.2024).

ДОДАТОК А

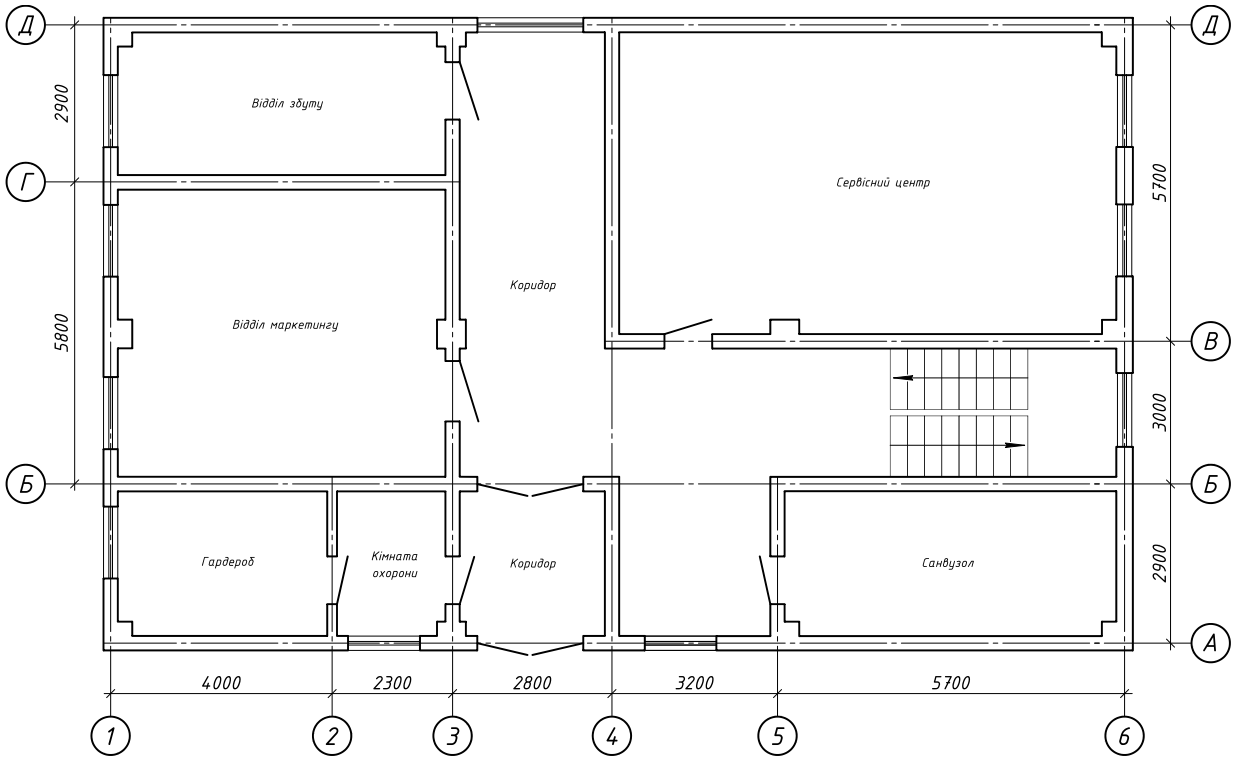


Рисунок А.1 – План першого поверху ПП «GALIT»

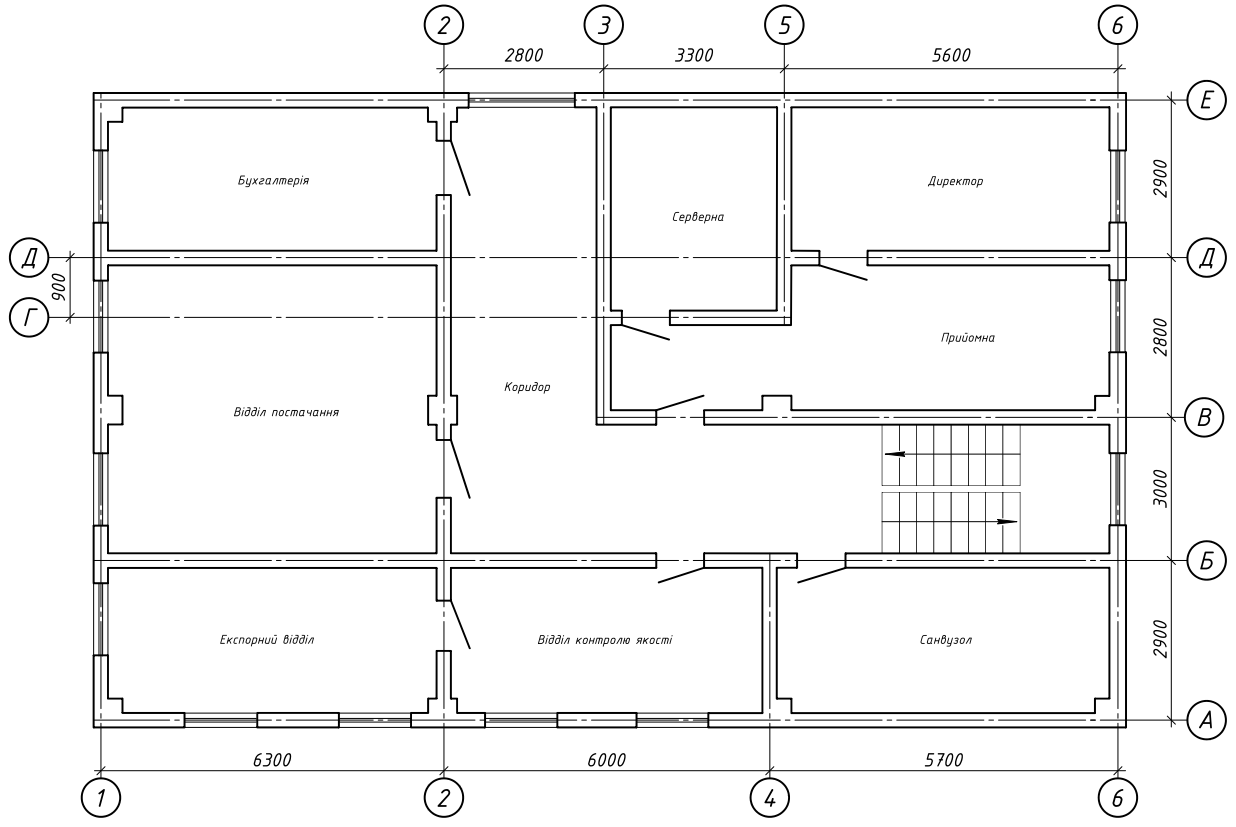


Рисунок А.2 – План другого поверху ПП «GALIT»

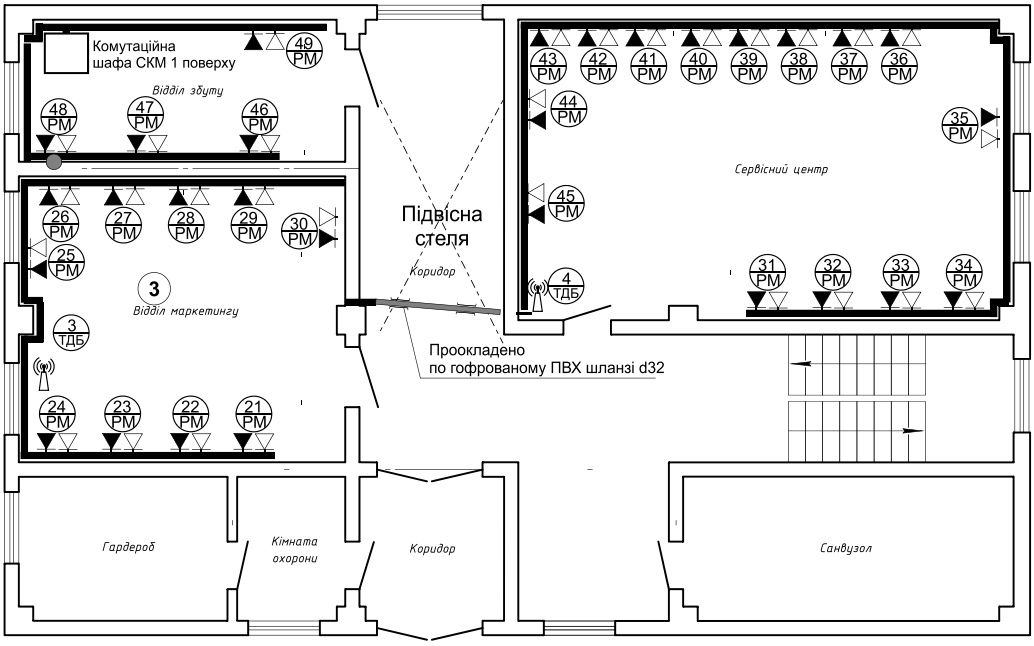
ДОДАТОК Б

Таблиця Б.1 – Експлікація приміщень ПП «GALIT»

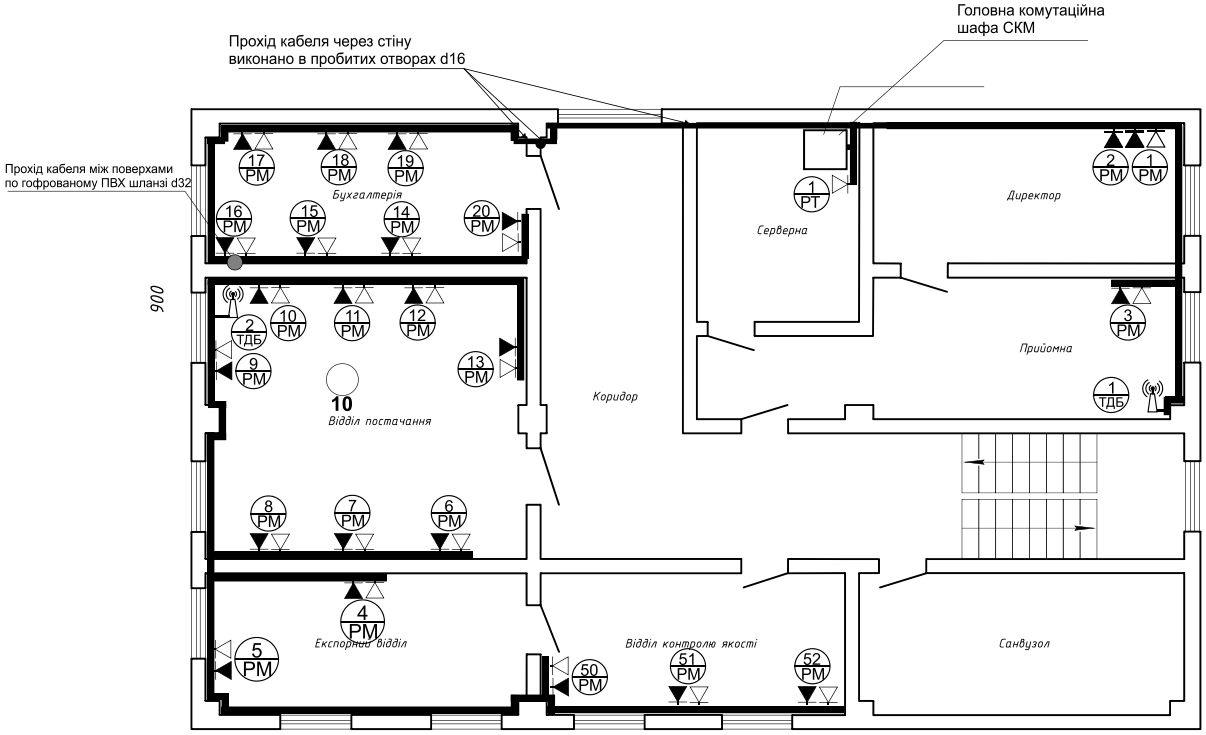
№ приміщення	Назва приміщення
1	Прийомна
2	Відділ збуту
3	Відділ контролю якості
4	Гардероб
5	Кімната охорони
6	Коридор
7	Сервісний центр
8	Санвузол
9	Бухгалтерія
10	Відділ маркетингу
11	Відділ постачання
12	Серверна
13	Директор
14	Експортний відділ

ДОДАТОК В

1 поверх



2 поверх



Розетка телефонна RJ-11
Розетка мережева RJ-45
Безпровідна точка доступу

Монтаж і підключення Ethernet розеток на робочих місцях

1. Прокладка мереж виконана в коробах кабелем UTP Cat 6,ПВХ, 4 пари. Прохід через стіни кабелем виконано в ПВХ трубках
2. Прокладка мереж за підвісною стелею та вентиляційній шахті виконана в ПВХ шланзі діаметром 25 и 32 мм.
3. В приміщенні апаратної кабелі прокладено по кабельних лотках, зв язані нейлоновими стяжками.
3. АТС змонтована у виробничосу приміщенні, на висоті 1,2 м відрівня підлоги, живлення АТС здійснено від електрощита

Рисунок В.1 – План структурованої кабельної системи мережі ПП «GALIT»

ДОДАТОК Г

Таблиця Г.1 Розрахунок довжини кабелю

Перший поверх		Другий поверх	
Між вузлами	Довжина, м	Між вузлами	Довжина, м
1	2	3	4
WS_21 -> Sw3	16	WS_1 -> Sw1	6
WS_22 -> Sw3	14,5	WS_2 -> Sw1	4,5
WS_23 -> Sw3	10,75	WS_3 -> Sw1	30,75
WS_24 -> Sw3	12,45	WS_4 -> Sw1	28,45
WS_25 -> Sw3	13,45	WS_5 -> Sw1	29,45
WS_26 -> Sw3	14,95	WS_6 -> Sw1	31,95
WS_27 -> Sw3	12,25	WS_7 -> Sw1	29,25
WS_28 -> Sw3	10,75	WS_8 -> Sw1	27,75
WS_29 -> Sw3	10,25	WS_9 -> Sw1	20,25
WS_30 -> Sw3	11,00	WS_10 -> Sw1	17,00
AP1-> Sw1	14,25	WS_11 -> Sw1	16,25
AP2-> Sw1	25,25	WS_12 -> Sw1	15,95
WS_31 -> Sw4	26,95	WS_13 -> Sw1	12,40
WS_32 -> Sw4	24,40	WS_50 -> Sw1	35,10
WS_33 -> Sw4	22,90	WS_51 -> Sw1	37,00
WS_34 -> Sw4	20,50	WS_53 -> Sw1	39,50
WS_35 -> Sw4	18,80	AP1-> Sw1	20,15
WS_36 -> Sw4	17,30	WS_14 -> Sw2	17,00
WS_37 -> Sw4	15,70	WS_15 -> Sw2	16,25
WS_38 -> Sw4	13,90	WS_16 -> Sw2	15,95
WS_39 -> Sw4	13,10	WS_17 -> Sw2	12,40
WS_40 -> Sw4	11,80	WS_18 -> Sw2	17,00
WS_41 -> Sw4	10,50	WS_19 -> Sw2	16,25

Продовження таблиці Г.1

WS_42 -> Sw4	9,50	WS_19 -> Sw2	14,80
WS_43 -> Sw4	11,55	Sw2-> Sw1	10,20
WS_44 -> Sw4	13,15	Sw3-> Sw1	13,60
WS_44 -> Sw4	15,50	Sw4-> Sw1	13,60
WS_45 -> Sw4	17,50	Sw1-> R1	1,5
WS_46 -> Sw4	2,5	-	-
WS_47 -> Sw4	4	-	-
WS_48 -> Sw4	4,5	-	-
WS_49 -> Sw4	6	-	-
AP3-> Sw3	6,5	-	-
AP4-> Sw4	16,5	-	-
Всього	534,90	Всього	518,65

ДОДАТОК Д

Таблиця Д.1 – Порівняльні технічні характеристики комутаторів

	Allied Telesyn AT-x600-24Ts	TP-Link T2600G-28TS	Mikrotik CRS125-24G-1S-RM
1	**2**	3	4
Підтримувані функції	**L2, L3**		
Комутація кадрів Гбіт/с	**96**	56	50
Кадрів/пакетів в секунду	**71,4**	41,67	30
К-сть портів 10/100/1000 BASE-TX	**24+4**	24+4	24+1
Вартість, грн	**10680**	10250	982
Засоби віддаленого керування	**WEB, Telnet, SSH**		
Підтримка технології VLAN	**Так**		

ДОДАТОК Е

Таблиця Е.1 – IP-адресація пристроїв мережі ПП «GALIT»

№ п/п	Позначення вузлів	Назва кабінету або відділу	Приналежність до VLAN	IP-адреса
1	2	3	4	5
1	WS_1	Директор	VLAN1	192.168.0.33/28
2	WS_2	Директор	VLAN1	192.168.0.34/28
3	WS_3	Прийомна	VLAN1	192.168.0.35/28
4	WS_4	Експортний відділ	VLAN1	192.168.0.36/28
5	WS_5	Експортний відділ	VLAN1	192.168.0.37/28
6	WS_6	Відділ постачання	VLAN1	192.168.0.38/28
7	WS_7	Відділ постачання	VLAN1	192.168.0.39/27
8	WS_8	Відділ постачання	VLAN1	192.168.0.40/27
9	WS_9	Відділ постачання	VLAN1	192.168.0.41/27
10	WS_10	Відділ постачання	VLAN1	192.168.0.42/27
11	WS_11	Відділ постачання	VLAN1	192.168.0.43/27
12	WS_12	Відділ постачання	VLAN1	192.168.0.44/27
13	WS_13	Відділ постачання	VLAN1	192.168.0.45/27
14	WS_50	Відділ контрою якості	VLAN1	192.168.0.46/27
15	WS_51	Відділ контрою якості	VLAN1	192.168.0.47/27
16	WS_52	Відділ контрою якості	VLAN1	192.168.0.48/27
17	WS_14	Гол. бухгалтер	VLAN2	192.168.0.81/28
18	WS_15	Бухгалтерія	VLAN2	192.168.0.82/28
19	WS_16	Бухгалтерія	VLAN2	192.168.0.83/28
20	WS_17	Бухгалтерія	VLAN2	192.168.0.84/28
21	WS_18	Бухгалтерія	VLAN2	192.168.0.85/28
22	WS_19	Бухгалтерія	VLAN2	192.168.0.86/28
23	WS_20	Бухгалтерія	VLAN2	192.168.0.87/28
24	WS_21	Відділ маркетологів	VLAN3	192.168.0.65/28

Продовження таблиці Г.1

1	2	3	4	5
25	WS_22	Відділ маркетологів	VLAN3	192.168.0.66/28
26	WS_23	Відділ маркетологів	VLAN3	192.168.0.67/28
27	WS_24	Відділ маркетологів	VLAN3	192.168.0.68/28
28	WS_25	Відділ маркетологів	VLAN3	192.168.0.69/28
29	WS_26	Відділ маркетологів	VLAN3	192.168.0.70/28
30	WS_27	Відділ маркетологів	VLAN3	192.168.0.71/28
31	WS_28	Відділ маркетологів	VLAN3	192.168.0.72/28
32	WS_29	Відділ маркетологів	VLAN3	192.168.0.73/28
33	WS_30	Відділ маркетологів	VLAN3	192.168.0.74/28
34	WS_31	Сервісний центр	VLAN4	192.168.0.1/27
35	WS_32	Сервісний центр	VLAN4	192.168.0.2/27
36	WS_33	Сервісний центр	VLAN4	192.168.0.3/27
37	WS_34	Сервісний центр	VLAN4	192.168.0.4/27
38	WS_35	Сервісний центр	VLAN4	192.168.0.5/27
39	WS_36	Сервісний центр	VLAN4	192.168.0.6/27
40	WS_37	Сервісний центр	VLAN4	192.168.0.7/27
41	WS_38	Сервісний центр	VLAN4	192.168.0.8/27
42	WS_39	Сервісний центр	VLAN4	192.168.0.9/27
43	WS_40	Сервісний центр	VLAN4	192.168.0.10/27
44	WS_41	Сервісний центр	VLAN4	192.168.0.11/27
45	WS_42	Сервісний центр	VLAN4	192.168.0.12/27
46	WS_43	Сервісний центр	VLAN4	192.168.0.13/27
47	WS_44	Сервісний центр	VLAN4	192.168.0.14/27
48	WS_45	Сервісний центр	VLAN4	192.168.0.15/27
49	WS_46	Відділ збуту	VLAN4	192.168.0.16/27
50	WS_47	Відділ збуту	VLAN4	192.168.0.17/27
51	WS_48	Відділ збуту	VLAN4	192.168.0.18/27
52	WS_49	Відділ збуту	VLAN4	192.168.0.19/27

ДОДАТОК Ж

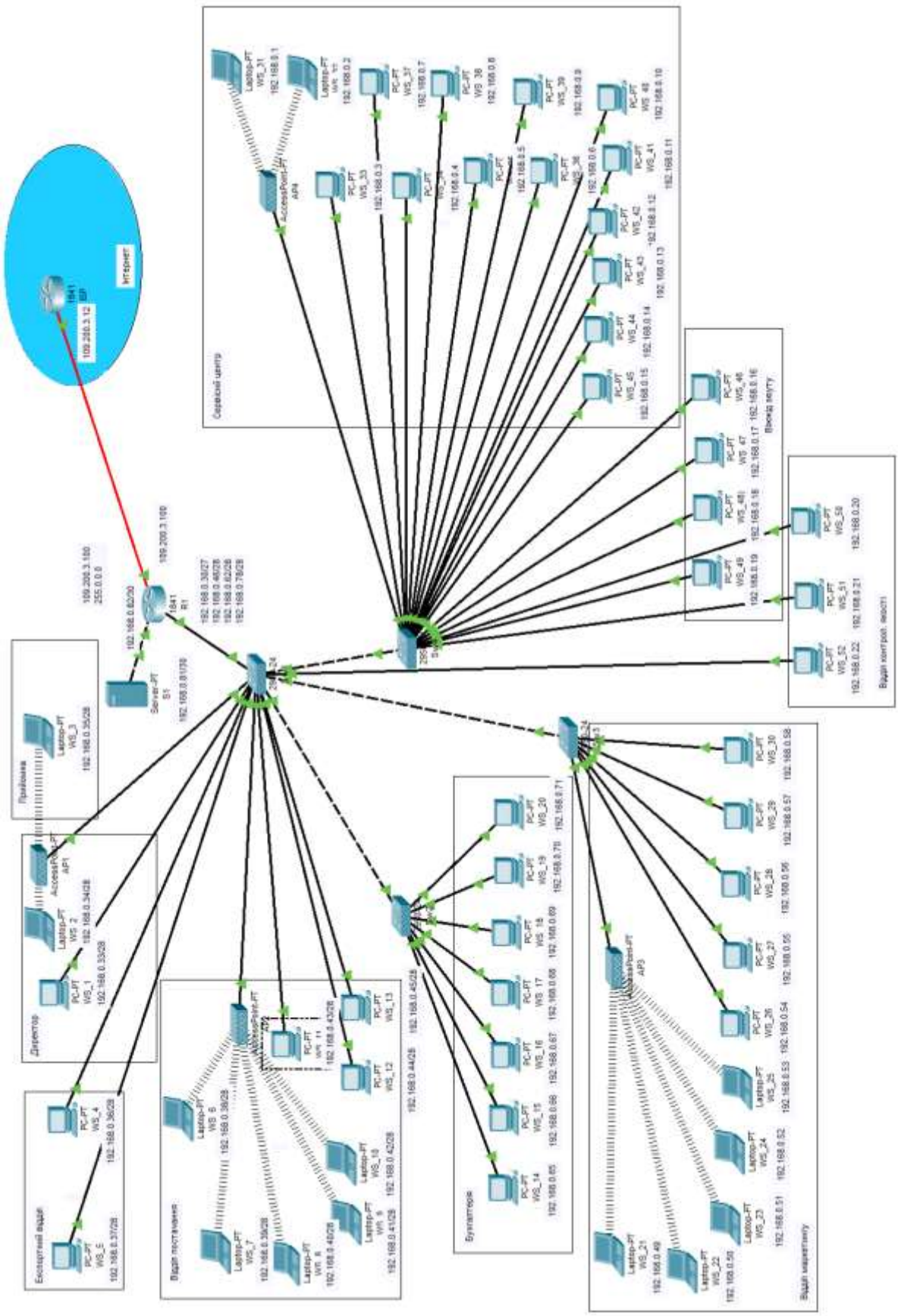


Рисунок Ж.1 – Емуляція мережі в Cisco Packet Tracert