Міністерство освіти і науки України

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

Відділення телекомунікацій та електронних систем
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: Розробка проекту комп'ютерної мережі комп'ютерного клубу „Ceber Hub“

Виконав: студент VI курсу, групи КІб-602

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

Максим ЗАБЛОЦЬКИЙ
(ім'я та прізвище)

Керівник Андрій ЛЯПАНДРА
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2024

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

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

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"08" травня 2024 року

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

Заблоцькому Максим Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проекту комп'ютерної мережі комп'ютерного клубу „Cyber Hub"

керівник роботи Ляпандра Андрій Степанович
(прізвище, ім'я, по батькові)

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

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

3. Вихідні дані до роботи: план приміщення, документація на мережеве обладнання, завдання на проектування.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): *1. ЗАГАЛЬНИЙ РОЗДІЛ, 2. РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ, 3. СПЕЦІАЛЬНИЙ РОЗДІЛ, 4. ЕКОНОМІЧНИЙ РОЗДІЛ, 5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ,ВИСНОВОК*

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

План розташування обладнання в головному комутаційному вузлі

Характеристики активного комутаційного обладнання мережі

Тексти для програмування активного комутаційного обладнання, серверні скріпти

Характеристики серверів

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

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

7. Дата видачі завдання: 08 травня 2024 року

Студент _____ Максим ЗАБЛОЦЬКИЙ
(підпис) (ім'я та прізвище)

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

ЗМІСТ

АНОТАЦІЯ

Заблоцький М.І. Розробка проекту комп’ютерної мережі комп’ютерного клубу „Cyber Hub“ : кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2024. 97с.

Основною метою є створення ефективної, безпечної та надійної мережі, яка забезпечить високопродуктивне обслуговування користувачів. Виконано аналіз вимог до мережі, вибрано необхідне комутаційне обладнання, програмне забезпечення, виконано аналіз вимог до засобів захисту мережі. Проведено розробку логічної та фізичної топології мережі. Виконано моделювання та тестування мережі, розроблено інструкції з інсталяції та налаштування обладнання і програмного забезпечення. В роботі також розглядаються економічні аспекти проекту та вимоги до охорони праці і техніки безпеки. Висновки містять оцінку досягнення поставлених цілей.

Ключові слова: комп'ютерний клуб, комп'ютерна мережа, комутаційне обладнання, програмне забезпечення, мережевий захист, тестування мережі, моделювання мережі, економічні аспекти, охорона праці, техніка безпеки.

ANNOTATION

Zablotskyi M.I. Development of the computer network project of the computer club "Cyber Hub": qualifying work for obtaining a bachelor's degree, specialty 123 Computer Engineering. Ternopil: VSP "TFC TNTU", 2024. 97p.

The main goal is to create an efficient, secure and reliable network that will provide high-performance user service. An analysis of network requirements was performed, the necessary switching equipment and software were selected, and an analysis of network protection requirements was performed.

The logical and physical topology of the network has been developed. Modeling and testing of the network was carried out, instructions for installation and configuration of hardware and software were developed. The work also considers the economic aspects of the project and the requirements for occupational health and safety. The conclusions contain an assessment of the achievement of the set goals.

Keywords: computer club, computer network, switching equipment, software, network protection, network testing, network modeling, economic aspects, labor protection, safety technology.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

НС – Недзвичані Ситуації;

ЕОМ – Електронно-обчислювальна машина;

ДСанПін – Державні санітарні норми та правила;

ПЗЗ – Прилад із зарядовим зв'язком;

АЦП – Аналого-цифровий перетворювач;

ПК – Персональний комп’ютер;

Ч\Б – Чорно-білий;

п. –пункт;

рис. –Рисунок;

с. (стр.) – сторінка

ВСТУП

Сучасний розвиток інформаційних технологій та мережевих рішень набуває дедалі більшого значення у різних сферах діяльності. Зокрема, комп'ютерні клуби, як один із видів закладів громадського користування, активно використовують комп'ютерні мережі для забезпечення якісного обслуговування своїх клієнтів. Комп'ютерні клуби пропонують своїм відвідувачам широкий спектр послуг, включаючи доступ до Інтернету, мережеві ігри, а також інші форми цифрових розваг та навчання. У зв'язку з цим, виникає потреба у створенні високопродуктивних, надійних та безпечних комп'ютерних систем.

На сьогоднішній день багато комп'ютерних клубів стикаються з проблемами низької продуктивності мережі, недостатньою безпекою даних, частими збоями обладнання та програмного забезпечення. Це, в свою чергу, негативно впливає на якість обслуговування клієнтів та рентабельність бізнесу. Тому розробка ефективного проекту комп'ютерної мережі для комп'ютерного клубу є надзвичайно актуальною.

Метою даної кваліфікаційної роботи є створення проекту комп'ютерної мережі для комп'ютерного клубу, яка забезпечить високу продуктивність, надійність та безпеку мережі. В процесі розробки проекту будуть розглянуті наступні завдання:

1. Аналіз сучасного стану проблеми та виявлення основних вимог до комп'ютерної системи комп'ютерного клубу.
2. Вибір оптимального комутаційного обладнання та програмного забезпечення, яке забезпечить максимальну ефективність роботи мережі.
3. Розробка логічної та фізичної схем мережі, а також їх обґрунтування.
4. Обґрунтування вибору засобів захисту мережі, що забезпечить безпеку даних та захист від кібератак.

5. Проведення моделювання та тестування мережі з метою виявлення та усунення можливих недоліків.

6. Розробка інструкцій з інсталяції, налаштування та експлуатації обладнання і програмного забезпечення.

7. Оцінка економічних аспектів проекту та визначення його рентабельності.

8. Розгляд вимог до охорони праці, техніки безпеки та екологічних вимог.

Необхідність проведення проектних робіт зумовлена високими вимогами до якості обслуговування в комп'ютерних клубах, а також потребою в забезпеченні безпеки та надійності мережевої інфраструктури. Використання сучасного комутаційного обладнання та програмного забезпечення дозволить досягти високої продуктивності мережі, що є критично важливим для надання якісних послуг клієнтам.

Розроблена мережа знайде своє застосування не лише у комп'ютерних клубах, але й у інших закладах з аналогічними вимогами до мережевої інфраструктури, таких як освітні заклади, офісні центри та інші комерційні структури. Запропоновані апаратні і програмні рішення можуть бути адаптовані під специфічні потреби різних підприємств, що забезпечить їх універсальність та гнучкість у використанні. Таким чином, даний дипломний проект має на меті створення сучасної, ефективної та безпечної комп'ютерної системи для комп'ютерного клубу, що дозволить забезпечити високу якість обслуговування клієнтів та підвищити рентабельність бізнесу.

1. ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Найменування роботи: «Розробка проекту комп’ютерної мережі комп’ютерного клубу „Cyber Hub“. Коротка назва роботи: «Проект мережі комп'ютерного клубу».

Область застосування: розробка даної роботи передбачає створення комп'ютерної мережі, що буде функціонувати в комп'ютерному клубі. Комп'ютерний клуб є закладом, що надає своїм клієнтам доступ до комп'ютерів з високопродуктивним обладнанням, мережевими іграми, Інтернетом та іншими цифровими ресурсами. Основними користувачами комп'ютерного клубу є геймери, студенти, IT-фахівці та інші клієнти, які потребують високошвидкісного доступу до мережевих ресурсів та стабільної роботи комп'ютерних систем.

Характеристика об’єкту: комп'ютерний клуб, для якого розробляється проект мережі, розташований у міському центрі та має на меті обслуговувати велику кількість відвідувачів щодня. Заклад оснащений сучасними комп'ютерами, периферійним обладнанням, а також забезпечує доступ до Інтернету та локальних ресурсів. Мережа клубу повинна забезпечувати високу продуктивність та надійність роботи всіх підключених пристроїв, а також мати ефективну систему безпеки для захисту даних та користувачів від кібератак.

Ключові аспекти проекту:

− продуктивність.

− безпека.

− надійність.

− масштабованість.

– економічна ефективність.

Мережа повинна забезпечувати високу швидкість передачі даних для одночасного обслуговування великої кількості користувачів без затримок та збоїв [1]. Необхідно забезпечити захист від несанкціонованого доступу, вірусів та інших кіберзагроз за допомогою сучасних засобів мережевої безпеки. Мережа повинна працювати безперебійно, мінімізуючи можливі простої та технічні збої. Проект повинен передбачати можливість розширення мережі з урахуванням майбутнього зростання кількості користувачів та пристроїв. Вибрані апаратні та програмні рішення повинні забезпечувати оптимальне співвідношення вартості та продуктивності.(див.рис.1.1)

Реалізація даного проекту дозволить комп'ютерному клубу надавати своїм клієнтам послуги найвищої якості, забезпечуючи стабільну та безпечну роботу мережі.(див.рис.1.2)

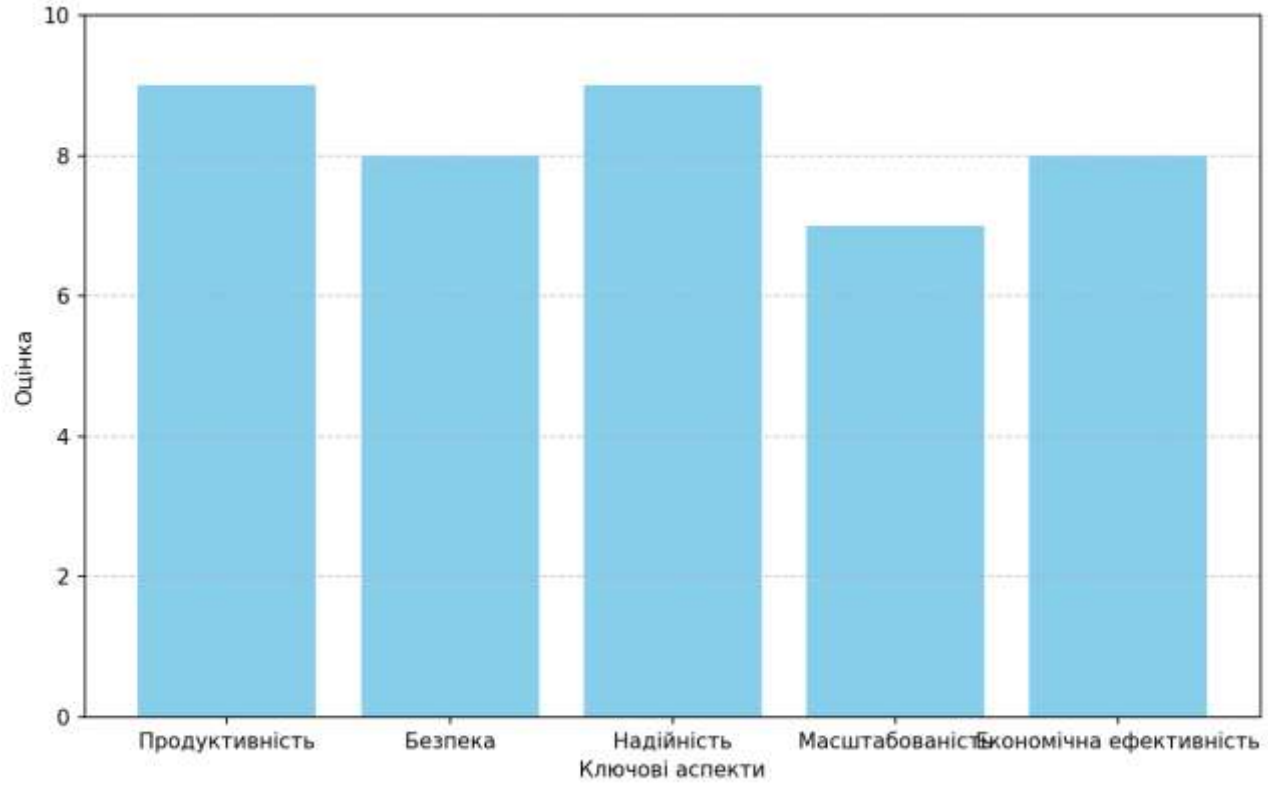

Рисунок 1.1 – Оцінка ключових аспектів проекту

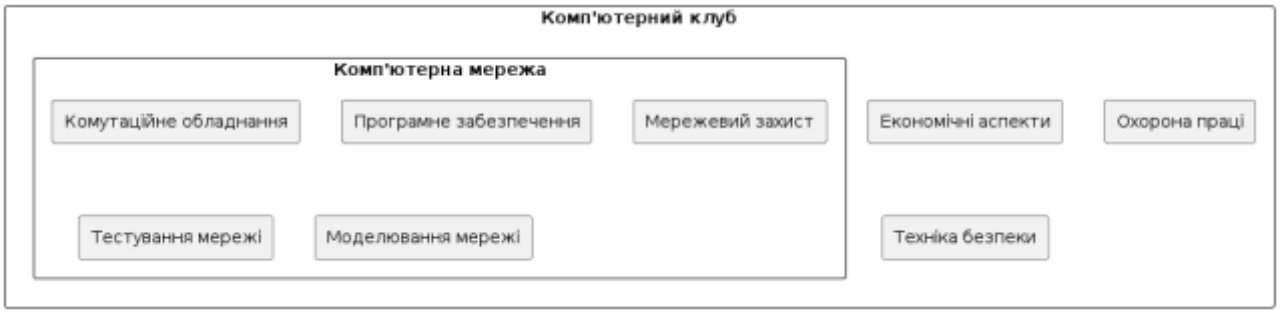

Рисунок 1.2 – Область застосування комп’ютерного клубу

1.1.2 Призначення розробки

Призначенням даної розробки є створення високоефективної, надійної та безпечної комп'ютерної мережі для комп'ютерного клубу. Ця мережа має забезпечувати стабільний та швидкісний доступ до Інтернету, локальних ресурсів і мережевих ігор для всіх користувачів клубу, а також підтримувати безперебійну роботу всіх підключених пристроїв. Експлуатаційне призначення комп'ютерної мережі визначається цілями та завданнями, які вона виконує під час повсякденного функціонування [2]. Основними аспектами експлуатаційного призначення є забезпечення надійного і швидкого обміну даними між пристроями в мережі, доступ користувачів до необхідних ресурсів, а також забезпечення безпеки і захисту мережі від потенційних загроз. Однією з основних функцій комп'ютерної мережі є можливість передавати дані між різними пристроями, такими як комп'ютери, сервери, принтери тощо [3]. Це забезпечує ефективну комунікацію між користувачами та доступ до ресурсів. Користувачі мережі повинні мати можливість спільного використання ресурсів, таких як файли, документи, друкарні, сканери тощо. Комп'ютерна мережа дозволяє легко обмінюватися даними та робити спільні ресурси доступними для всіх користувачів мережі. Комп'ютерна мережа надає можливість користувачам спілкуватися між собою, обмінюватися повідомленнями та файлами, спільно працювати над проектами тощо [4]. Одним з ключових аспектів експлуатаційного призначення є забезпечення безпеки даних і мережі. Це включає захист від

несанкціонованого доступу, вірусів, атак хакерів та інших загроз безпеці, як показано в таблиці 1.1.

Таблиця 1.1 – Основні цілі розробки

№	Ціль	Опис
1	2	3
1	Забезпечення високої продуктивності мережі:	Проектована мережа повинна мати високу пропускну здатність для одночасної роботи великої кількості користувачів, забезпечуючи низькі затримки і високу швидкість передачі даних.
2	Гарантія надійності та безпеки	Мережа повинна бути стійкою до збоїв та атак, з використанням сучасних засобів захисту від несанкціонованого доступу, вірусів, шпигунських програм та інших кібератак. Це включає в себе як апаратні, так і програмні засоби захисту.
3	Забезпечення масштабованості	Система повинна бути гнучкою та легко розширюваною, щоб мати можливість підключення додаткових пристроїв і користувачів без значних змін в існуючій інфраструктурі.
4	Оптимізація витрат	Проектування мережі має бути економічно вигідним, з використанням оптимального поєднання апаратного та програмного забезпечення для досягнення найкращого співвідношення ціни та якості.
5	Підвищення якості обслуговування клієнтів	Завдяки стабільній та швидкісній роботі мережі, клієнти комп'ютерного клубу отримають високоякісний сервіс, що включає безперебійну роботу під час мережевих ігор, швидкий доступ до Інтернету та інших цифрових ресурсів.

Продовження таблиці 1.1

1	2	3
6	Забезпечення легкості адміністрування та моніторингу	Проект повинен передбачати зручні засоби управління і моніторингу мережі для адміністраторів, що дозволить оперативно реагувати на можливі проблеми та ефективно керувати ресурсами.

Функціональне призначення комп'ютерної мережі визначається рядом завдань та функцій, які вона виконує для забезпечення ефективної роботи та взаємодії пристроїв та користувачів. Основними аспектами функціонального призначення є передача даних, доступ до ресурсів, комунікація та безпека. У майбутньому, з огляду на швидкий розвиток технологій, комп'ютерна мережа може бути модернізована для підтримки нових стандартів та технологій [5]. Це може включати:

– оновлення комутаційного обладнання для підтримки вищих швидкостей передачі даних.

– розширення мережі для підключення додаткових пристроїв та користувачів.

– вдосконалення системи безпеки для захисту від нових загроз.

– впровадження нових сервісів та додаткових можливостей, таких як віртуалізація ресурсів або хмарні технології.

Розробка даної комп'ютерної мережі спрямована на створення інфраструктури, яка буде відповідати всім вимогам сучасних користувачів комп'ютерного клубу, забезпечуючи їм комфортне та безпечне користування послугами закладу.

1.1.3 Вимоги до апаратного та програмного забезпечення

Наступні вимоги мають забезпечити належне функціонування комп'ютерної мережі, враховуючи як апаратні, так і програмні аспекти. Вимоги до апаратного забезпечення:

1) Комп'ютери для користувачів.

1.1) Кожен комп'ютер повинен бути достатньо потужним для виконання різноманітних завдань, що включають в себе роботу з офісними програмами, мультимедійними даними, а також веб-переглядачами.

1.2) Мінімальні конфігураційні вимоги повинні бути такими, щоб вони забезпечували безперебійну роботу операційних систем та програмного забезпечення, яке використовується в мережі.

2) Серверне обладнання.

2.1) Сервери повинні мати достатні ресурси, такі як потужний процесор, достатній обсяг оперативної пам'яті та зберігання даних, щоб забезпечити безперебійне функціонування мережі.

2.2) Рекомендується використовувати серверне обладнання з можливістю розширення, щоб в майбутньому легко можна було розширити мережу.

3) Комутаційне обладнання.

3.1)Комутатори та маршрутизатори повинні мати достатню пропускну здатність для обробки потоку даних в мережі, особливо в разі великої кількості одночасних підключень.

3.2) Повинна бути забезпечена підтримка сучасних стандартів Ethernet та інших мережевих протоколів.

Вимоги до програмного забезпечення:

1) Операційна система

1.1) Встановлюється на комп'ютерах мережі, повинно бути надійною, стабільною та забезпечувати безпеку даних.

1.2) Повинна підтримувати мережеві протоколи.

1.3) Забезпечувати зручний інтерфейс для адміністрування мережі.

2) Програмне забезпечення для мережі.

2.1) Необхідно встановити програмне забезпечення для управління мережею, яке дозволить ефективно контролювати та адмініструвати роботу мережі.

2.2) Це може включати системи моніторингу, конфігурації мережевих пристроїв та системи безпеки.

Важливо, щоб програмне забезпечення було здатним працювати з різними типами мережних пристроїв і підтримувати різні мережеві протоколи.

3) Засоби безпеки.

3.1)Забезпечення безпеки мережі вимагає використання спеціалізованого програмного забезпечення для захисту від вірусів, шкідливих програм та несанкціонованого доступу.

3.2) Програмне забезпечення має здійснювати постійний моніторинг активності в мережі, виявляти потенційні загрози та негайно реагувати на них для захисту від інцидентів безпеки.

4) Резервне копіювання та відновлення.

4.1) Для забезпечення надійності та відновлення даних у випадку виникнення непередбачуваних ситуацій, необхідно встановити програмне забезпечення для резервного копіювання та відновлення.

4.2) Має дозволяти забезпечувати безперебійну роботу мережі після випадків втрати даних або збоїв.

5) Підтримка та оновлення.

5.1) Програмне забезпечення має регулярно оновлюватися для забезпечення сумісності з новими технологіями та вразливостями безпеки.

5.2) Підтримка і оновлення програмного забезпечення є ключовими аспектами для забезпечення ефективності та безпеки мережі протягом тривалого періоду експлуатації.

Вказані вимоги до програмного забезпечення спрямовані на забезпечення надійності, безпеки та ефективності комп'ютерної мережі, а також на забезпечення зручності управління та адміністрування.

1.1.4 Вимоги до документації

Документація мережі повинна бути зрозумілою та структурованою. Усі відомості щодо апаратного та програмного забезпечення, конфігурації мережевих пристроїв, параметрів безпеки та іншої важливої інформації мають бути легко доступні та зрозумілі для персоналу, який відповідає за управління та експлуатацію мережі. Усі документи мають створюватися на основі єдиних стандартів документування мережі. Це включає використання однорідних шаблонів, форматів та термінології для забезпечення консистентності та зручності в сприйнятті. Документація мережі повинна містити всю необхідну інформацію про апаратне та програмне забезпечення, конфігурацію мережевих пристроїв, налаштування безпеки та інші важливі аспекти [6]. Крім того, ця інформація має бути постійно оновлюватися та відображати актуальний стан мережі. Документація повинна бути доступною для усіх співробітників, які мають потребу у використанні чи управлінні мережею. Це може включати внутрішній портал або систему управління документами, яка забезпечить легкий доступ до інформації, як показано в таблиці 1.2.

Таблиця 1.2 – Розробка стандартного бланку для документування мережі

№	Назва	Опис
1	2	3
1	Шаблон звіту про стан мережі	Має містити інформацію про стан мережі, підключені пристрої, мережевий зв'язок та

		виявлені проблеми.

Продовження таблиці 1.2

1	2	3
2	Формат опису мережевих пристроїв.	Міститиме опис кожного мережевого пристрою, його характеристики, конфігурацію та призначення в мережі
3	Протоколи та параметри безпеки	Буде містити інформацію про застосовані мережеві протоколи, параметри безпеки та правила доступу для керування доступом до мережевих ресурсів
4	Інструкції з експлуатації та технічна підтримка.	Міститиме інструкції з експлуатації мережі, рекомендації щодо вирішення проблем та контактну інформацію для технічної підтримки
5	Топологічна схема мережі	Повинна включати всі вузли мережі (комп'ютери, сервери, комутатори, маршрутизатори), а також зв'язки між ними.
6	Список IP-адрес та підмереж	Включає список всіх IP-адрес, присвоєних пристроям у мережі, разбитих за підмережами
7	Список мережевих пристроїв	Перелік усіх мережевих пристроїв із зазначенням їхніх характеристик (модель, виробник, версія ПЗ)
8	Налаштування безпеки	Опис правил файрвола, VPN-з'єднань, списків керування доступом тощо.
	Процедури резервного копіювання та	Інструкції щодо регулярного створення резервних копій конфігурацій мережних

	відновлення	пристроїв та процедур відновлення після збоїв

Вищевказані вимоги та стандартні бланки допоможуть забезпечити належний рівень документації, який буде корисним для управління, підтримки та розвитку комп'ютерної мережі.

1.1.5 Техніко-економічні показники

Розробка проекту потребує залучення робочої сили. Обсяг трудових ресурсів вимірюється у людино-місяцях. Планується виділення 2 людино-місяців на розробку комп'ютерної системи комп'ютерного клубу. Цей обсяг включає усі фази розробки, від аналізу вимог до впровадження та підтримки системи. Для розробки програмного забезпечення та моделювання мережі потрібний обчислювальний час комп'ютерів [7]. Обсяг машинних ресурсів вимірюється у годинах машинного часу. Планується виділення 810 годин машинного часу для розробки програмного забезпечення та 75 годин машинного часу для моделювання та тестування мережі. Дані техніко-економічні показники визначають обсяг ресурсів, які будуть витрачені на розробку проекту комп'ютерної системи комп'ютерного клубу. Вони є ключовими для планування бюджету та ресурсів для виконання проекту.

1.1.6 Стадії та етапи розробки

Зміст робіт на стадіях проектування, встановлення і підтримки мережі у відповідності зі стандартами охоплює різні аспекти процесу розробки, реалізації та експлуатації мережевих рішень. Це включає в себе ретельний аналіз вимог, проектування, налаштування обладнання, його тестування та забезпечення стабільної роботи мережі протягом усього життєвого циклу. Кожен етап відіграє ключову роль у створенні надійної та ефективної

мережевої інфраструктури. Нижче наведена таблиця 1.3, що деталізує кожен етап цього процесу:

Таблиця 1.3 – Стадії та етапи розробки

№	Стадія	Етап	Опис
1	2	3	4
1	Стадія проектування	Аналіз вимог	Визначення потреб користувачів та вимог до мережі
			Проведення SWOT-аналізу (аналіз сильних і слабких сторін, можливостей та загроз)
		Проектування мережі	Розробка логічної та фізичної структури мережі
			Вибір інфраструктури та технологій, відповідно до стандартів безпеки та ефективності мережі
2	Стадія встановлення	Підготовка інфраструктури	Встановлення мережевого обладнання (комутатори, маршрутизатори, мережеві кабелі тощо)

		Конфігурування та налаштування	Налаштування мережевих пристроїв згідно з проектною документацією та стандартами безпеки
		Тестування	Проведення тестів для перевірки правильності роботи мережі та виявлення можливих проблем

Продовження таблиці 1.3

1	2	3	4
3	Стадія підтримки	Експлуатація та моніторинг	Забезпечення безперебійної роботи мережі
			Постійний моніторинг та відстеження роботи мережі з метою виявлення та усунення можливих проблем
		Оновлення та модернізація	Впровадження нових технологій та оновлення мережевого обладнання згідно з розвитком технологій та потребами користувачів

1.1.7 Порядок контролю та прийому

Умови контролю працездатності мережі:

- мережа повинна бути доступною для всіх користувачів згідно з встановленими графіками роботи.

- контроль за стабільністю та надійністю з'єднань між пристроями у мережі.

- перевірка швидкості передачі даних в мережі та порівняння її з плановими параметрами.

Контрольні показники:

- перевірка зв'язку між пристроями та вимірювання часу відправки-прийому пакетів даних (Ping тести).

- вимірювання максимальної пропускної здатності мережі для передачі даних.

- спостереження за роботою мережі при великому обсязі трафіку для виявлення можливих перевантажень або проблем зі швидкодією.

Розробка тестової програми:

– розробка набору сценаріїв тестування для автоматизованої перевірки ключових показників мережі.

– запуск розробленої тестової програми для перевірки роботи мережі відповідно до установлених вимог.

– оцінка результатів тестів та виявлення можливих проблем або несоответствій у роботі мережі.

Ці процедури контролю допоможуть переконатися, що мережа працює стабільно, ефективно та відповідає встановленим вимогам та стандартам.

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

Проект полягає у розробці комп'ютерної мережі для підприємства з метою оптимізації робочих процесів, забезпечення ефективного обміну інформацією та підвищення продуктивності працівників. Ключові завдання включають встановлення мережевої інфраструктури, налаштування безпеки та забезпечення надійності і масштабованості мережі. Підприємство

«DJCOM» є середньорозмірною компанією, що діє на ринку послуг. Воно складається з наступних структурних підрозділів, показаних на рисунку 1.3.

Цей проект охоплює створення детального плану, що включає вибір відповідного обладнання та програмного забезпечення. Мережа повинна забезпечувати високий рівень безпеки даних і бути здатною до подальшого розширення. Встановлення мережі здійснюватиметься з урахуванням специфічних потреб кожного підрозділу компанії, щоб забезпечити безперебійну та ефективну роботу всіх служб і відділів. Проект також передбачає регулярне обслуговування та модернізацію мережі для її відповідності зростаючим потребам підприємства та технологічним змінам.

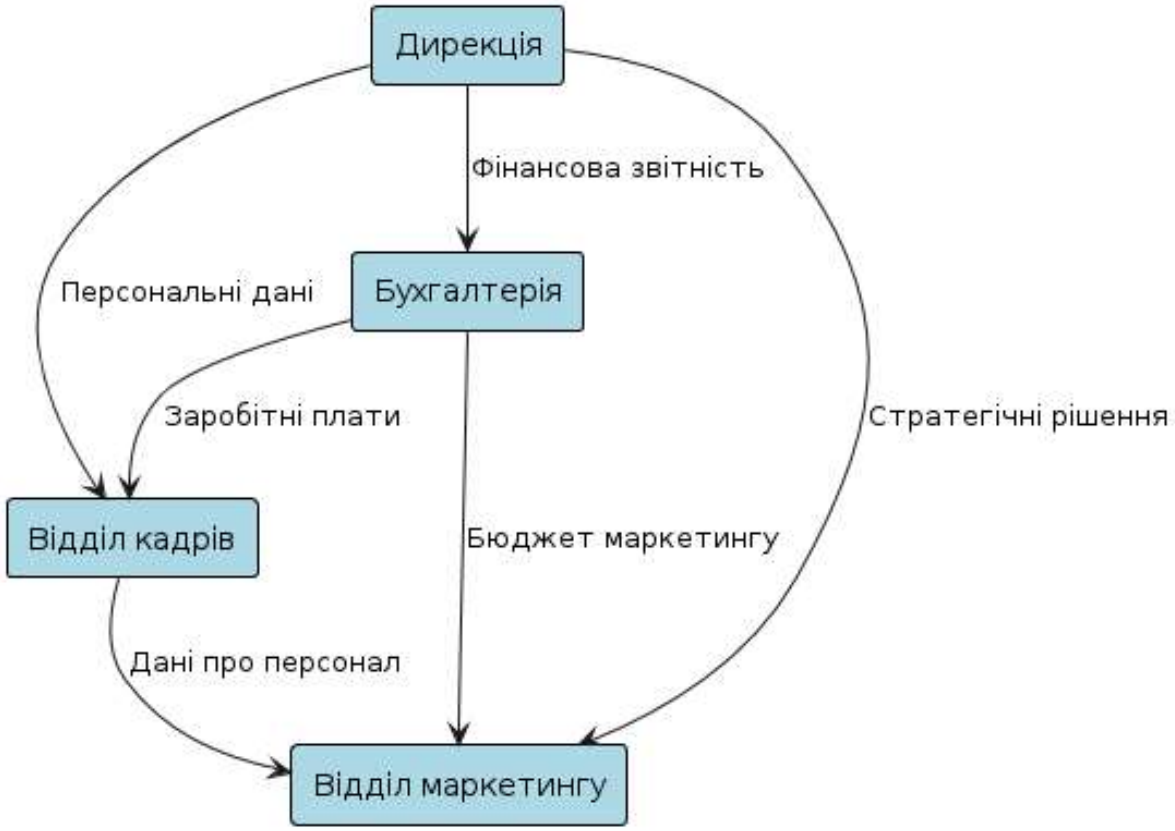

Рисунок 1.3 – Інформаційні потоки між різними підрозділами підприємства

РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

Проектування та реалізація комп'ютерної мережі для комп'ютерного клубу включає декілька важливих етапів: вибір відповідної логічної та фізичної топології, розробка схем розташування кабелів та вузлів, поділ мережі на віртуальні підмережі (VLAN) та конфігурація обладнання. Основною метою проекту є створення надійної, високопродуктивної, масштабованої та безпечної мережі, яка буде ефективно підтримувати всі вимоги клубу. Специфічні особливості:

– для забезпечення безпеки та ефективного управління трафіком, мережа буде розділена на віртуальні локальні мережі (VLAN).

– використання комутаторів третього рівня для маршрутизації трафіку між підмережами.

– використання сучасних технологій Ethernet для забезпечення високої швидкості передачі даних.

– реалізація заходів для забезпечення надійності та безпеки мережі, включаючи резервування обладнання та мережевих з'єднань.

Математичні методи, що використовуються при проектуванні мережі, включають:

– визначення необхідної пропускної здатності для кожного сегмента мережі на основі кількості підключених пристроїв та передбачуваного трафіку.

– аналіз затримок, викликаних обладнанням та мережею, для забезпечення низької латентності.

– прогнозування можливостей збільшення розмірів мережі та забезпечення масштабованості.

2.1 Опис та обґрунтування вибору логічного типу мережі

Для вибору логічного типу мережі було проаналізовано кілька сучасних технологій локальних мереж, включаючи Ethernet, Token Ring, FDDI та ATM, як показано в таблиці 2.1

Таблиця 2.1 – Сучасні технології локальних мереж

№		Переваги	Недоліки
1	2	3	4
1	Ethernet	Висока швидкість передачі даних (до 100 Гбіт/с і більше), низька вартість, легкість у встановленні та налаштуванні, підтримка стандартів IEEE 802.3, широке поширення та сумісність із різним обладнанням	Можливі колізії в мережах великого розміру без належного сегментування
2	Token Ring	Детермінованість доступу до мережевого середовища, що дозволяє уникнути колізій	Вища вартість обладнання, складність у встановленні та налаштуванні, менша швидкість передачі даних у порівнянні з Ethernet
3	FDDI (Fiber Distributed Data Interface)	Висока пропускна здатність, відсутність колізій завдяки двом контурам передачі	Висока вартість обладнання та кабелів, складність у встановленні

		даних, висока надійність.	

Продовження таблиці 2.1

1	2	3	4
4	ATM (Asynchronous Transfer Mode)	Підтримка передачі різних типів даних (відео, аудіо, дані) з високою якістю обслуговування (QoS)	Висока вартість, складність у встановленні та управлінні

Виходячи з аналізу сучасних технологій, для реалізації комп'ютерного клубу обрана технологія Ethernet із топологією «Зірка». Цей варіант забезпечує високу продуктивність, надійність та легкість в адмініструванні.(див.рис.2.1)

Переваги обраного варіанту:

– висока продуктивність. Кожен пристрій підключається до центрального комутатора, що забезпечує максимальну пропускну здатність.

– надійність. Відмова одного з'єднання не впливає на роботу інших вузлів мережі.

– легкість адміністрування. Централізоване управління мережею спрощує моніторинг та контроль за трафіком.

– масштабованість. Легко додавати нові пристрої до мережі.

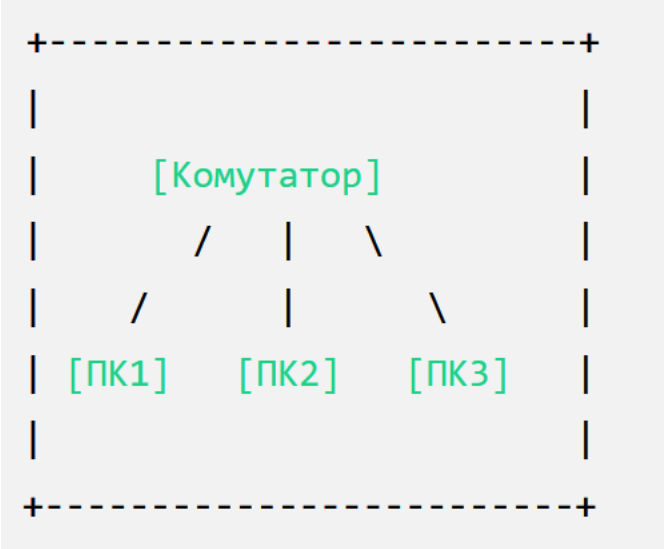

Рисунок 2.1 – Логічна схема топології мережі

Логічну адресацію наведено в таблиці 2.2:

Таблиця 2.2 – Логічна адресація в ЛОМ

Діапазон позначення вузлів	Робоча група/ Кількість вузлів		Приміщення	Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6	7	8
ПК1 - ПК14	Група 1/14		Перший поверх	Кімната 1		10	192.168.1.0/24
ПК15 - ПК38	Група 2/14		Другий поверх	Кімната 2		20	192.168.2.0/24

2.2 Розробка схеми фізичного розташування кабелів та вузлів

Для горизонтальної кабельної системи обрано Cat 6 UTP (неекранована витої пара) кабелі. Вони забезпечують високу швидкість передачі даних (до 10 Гбіт/с) та надійність з'єднання. Кабелі прокладаються у кабель-каналах або підвісних стелях, залежно від конструкції будівлі. Використовуються патч-панелі для організації підключень у серверній кімнаті та кабельні розетки у робочих місцях. Кожне робоче місце (ПК, принтери, інші периферійні пристрої) підключається до мережі через кабель Cat 6, що закінчується розеткою RJ-45.

Для вертикальної кабельної системи обрано многомодовий оптоволоконний кабель. Він забезпечує високошвидкісне з'єднання між поверхами та мінімальні затримки передачі даних. Оптоволоконні кабелі прокладаються у вертикальних шахтах або спеціальних кабель-каналах, що забезпечує їх захист від механічних пошкоджень [8]. Встановлюються оптоволоконні патч-панелі для зручного підключення та управління.

Оптоволоконні кабелі з'єднують комутатори на різних поверхах, забезпечуючи високу пропускну здатність магістральних каналів. На основі стандарту проектування СКС (Структурованих Кабельних Систем) та вимог TIA/EIA-568B, розроблена схема фізичного розташування кабелів та вузлів мережі, як показано на рисунку 2.2 та рисунку 2.3.

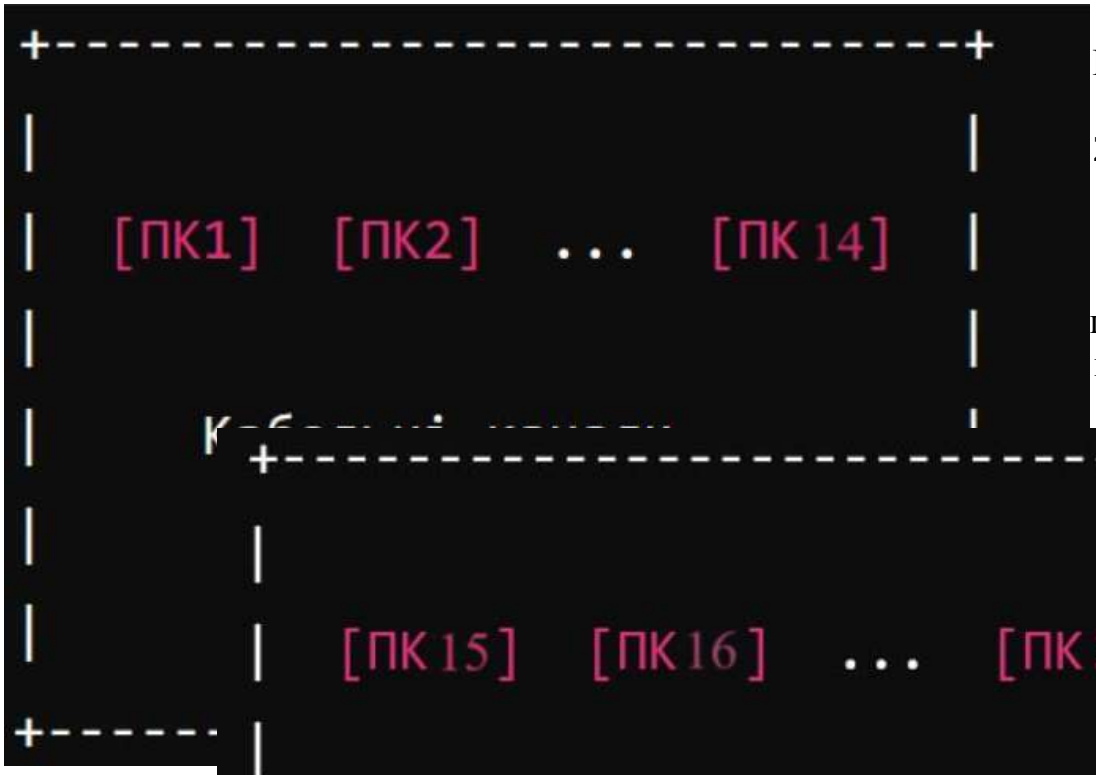

Рисунок 2.2 – План першого поверху

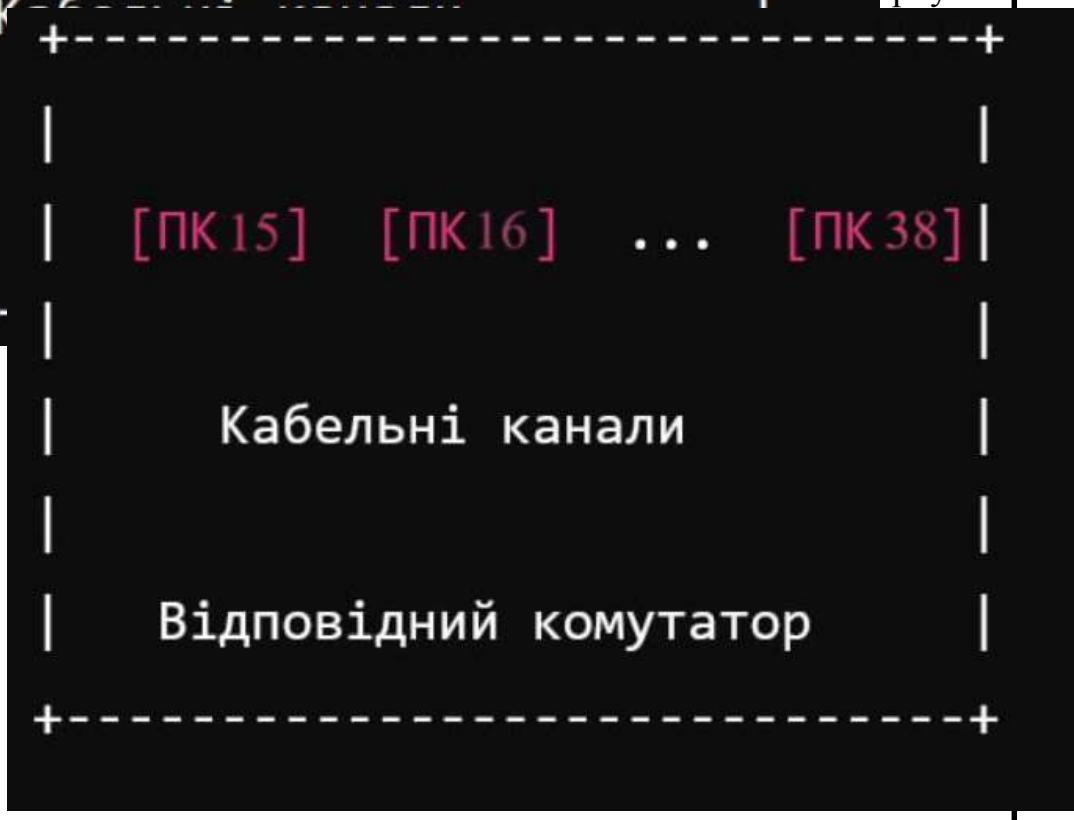

Рисунок 2.3 – План другого поверху

Для детальної інформації про підключення мережі на першому та другому поверхах дивіться рисунок 2.4.

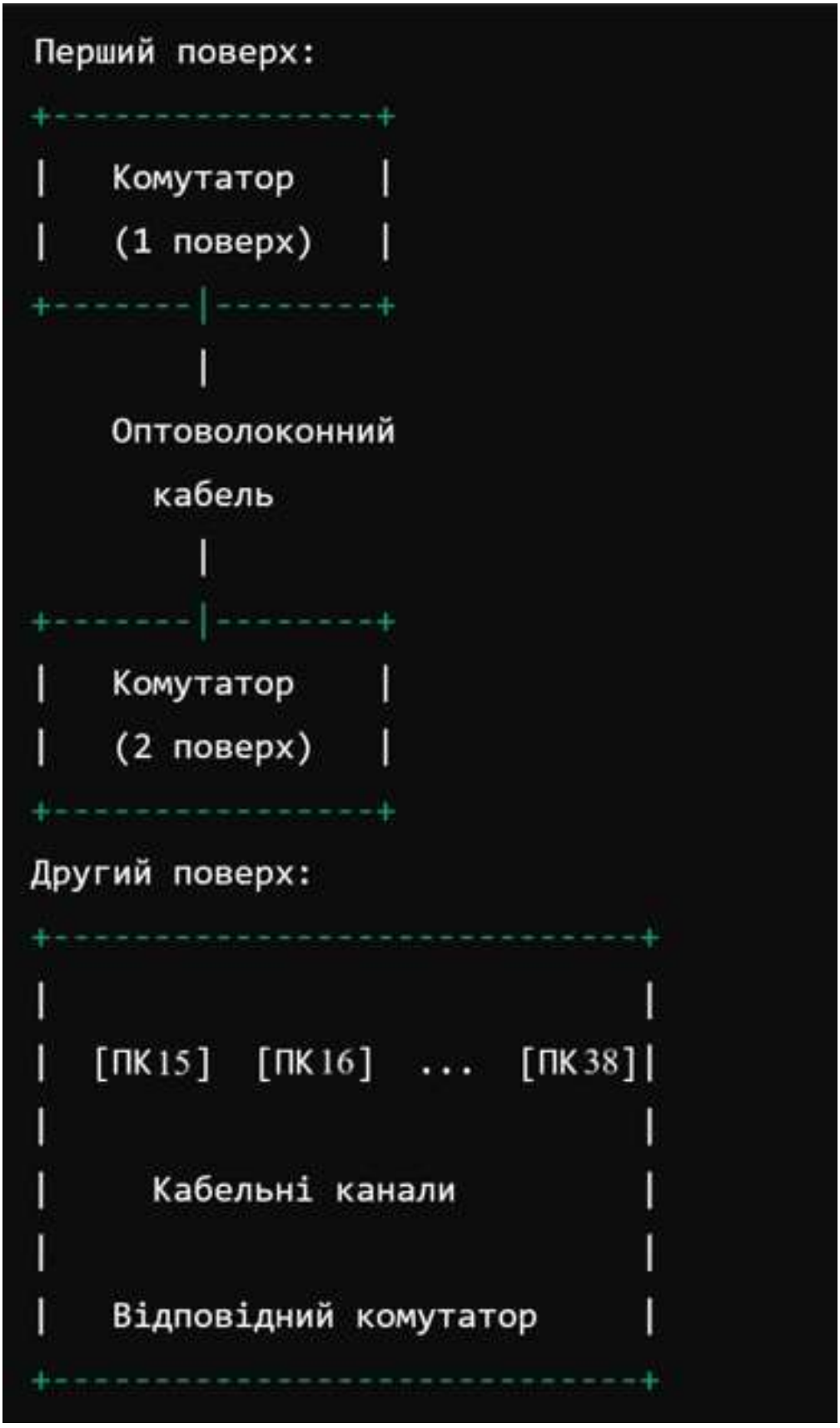

Рисунок 2.4 – Схема вертикальних з'єднань

Математичний розрахунок фізичних розмірів мережі. Для розрахунку фізичних розмірів мережі із врахуванням затримок в обладнанні та прогнозованих можливостей збільшення розмірів використовується наступна формула 2.1:

$$D=\frac{L}{v}+T \qquad (2.1)$$

D - затримка,

L - довжина кабелю,

v - швидкість передачі даних,

Те - затримка в обладнанні.

На основі стандарту проектування СКС (Структурованих Кабельних Систем) і згідно вимог TIA/EIA – 568B, спроектована фізична топологія мережі. Фізична топологія мережі спроектована на основі стандарту проектування СКС (Структурованих Кабельних Систем) і згідно вимог TIA/EIA – 568B. Спочатку спроектована горизонтальна кабельна система, яка забезпечує підключення кінцевих пристроїв, а потім вертикальна кабельна система, яка зв'язує різні поверхи.

Схема фізичного розташування:

– схема фізичного розташування кабелів та вузлів викреслена на плані будівлі та кожного поверху зокрема.

– комутатори розташовані в серверних кімнатах на кожному поверсі, забезпечуючи центральне підключення для всіх пристроїв на поверсі.

– кабелі прокладені в кабель-каналах та підвісних стелях, забезпечуючи захист та легкий доступ для обслуговування.

– схема розташування кабелів та вузлів включає прокладку горизонтальних кабелів Cat 6 від комутаторів до кожного робочого місця та вертикальних оптоволоконних кабелів для з'єднання між поверхами. Така фізична топологія забезпечує високу продуктивність, надійність та легкість у масштабуванні мережі комп'ютерного клубу.(див.рис.2.5)

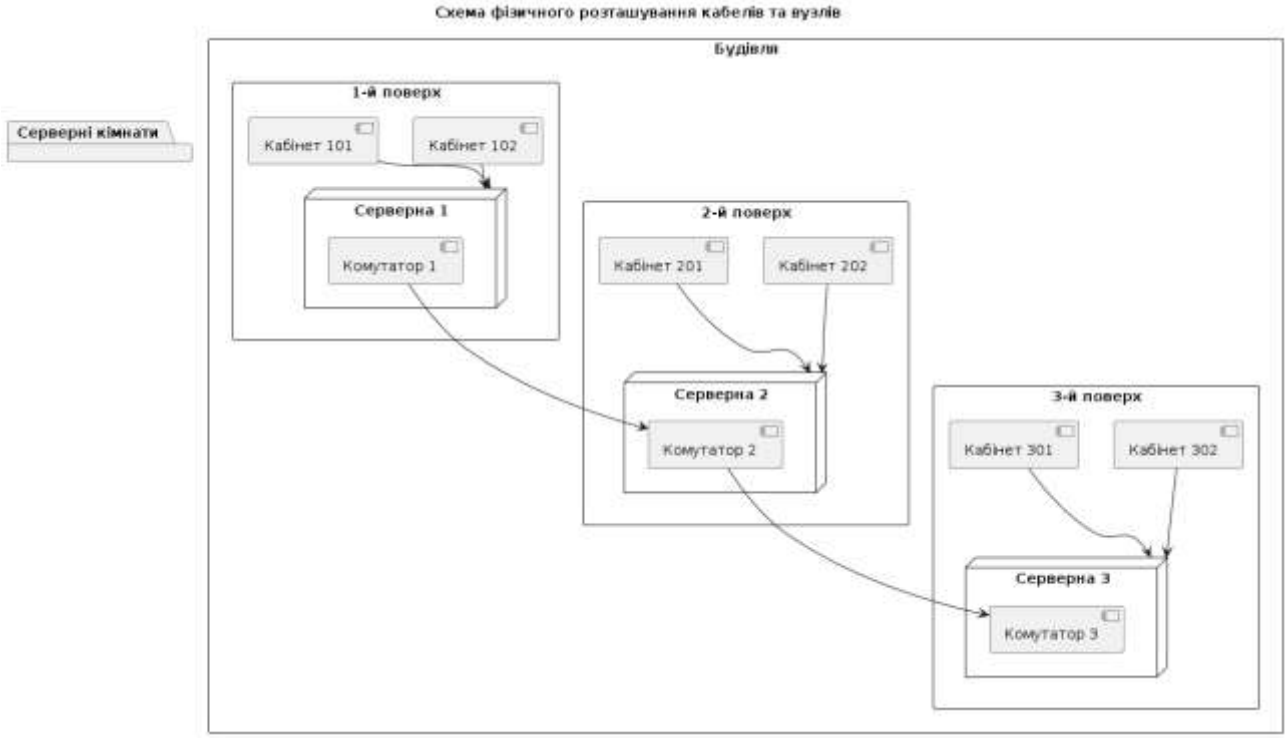

Рисунок 2.5 – Схема фізичного розташування кабелів та вузлів

Таблиця 2.3 – Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мережевого пристрою	Адреса підмережі/ Маска	Номер порту	Тип порту
1	2	3	4	5	6	7	8
1	PC1_1 – PC1_3	1, 2, 3	Access	SW_1	SW_1	1, 2, 3)	Untagged
2	PC1_26 – PC1_28	4, 5, 6	Access	SW_2	SW_2	4, 5, 6	Untagged

Таким чином, фізична топологія мережі розроблена з урахуванням сучасних вимог до продуктивності, надійності та безпеки, як показано в таблиці 2.3.

2.2.1 Типи кабельних з’єднань та їх прокладка

При розробці комп'ютерної мережі для комп'ютерного клубу були розглянуті різні типи кабельних з'єднань, щоб забезпечити максимальну продуктивність, надійність та легкість обслуговування, як показано в таблиці 2.4 та таблиці 2.5

Таблиця 2.4 – Мідні кабелі (UTP/STP)

Назва	Швидкість передачі даних	Переваги	Недоліки
Cat 5e UTP (Unshielded Twisted Pair)	до 1 Гбіт/с.	Низька вартість, легкість у прокладанні та обслуговуванні.	Схильність до електромагнітних завад (EMI).
Cat 6 UTP	до 10 Гбіт/с.	Висока швидкість передачі даних, сумісність з обладнанням Cat 5e.	Трохи вища вартість порівняно з Cat 5e.
Cat 6a STP (Shielded Twisted Pair)	до 10 Гбіт/с.	Висока захищеність від електромагнітних завад, велика швидкість передачі даних.	Вища вартість та складність у прокладанні.

Таблиця 2.5 – Оптоволоконні кабелі

Назва	Швидкість передачі даних	Переваги	Недоліки
Многомодовий оптоволоконний кабель (OM3, OM4)	до 100 Гбіт/с на коротких відстанях	Висока швидкість передачі даних, велика пропускна здатність, низька затримка	Висока вартість, складність у встановленні та обслуговуванні
Одномодовий оптоволоконний кабель	до 100 Гбіт/с на довгих відстанях	Відсутність затримок, підходить для довгих відстаней	Дуже висока вартість, складність у встановленні та обслуговуванні

Прокладка кабелів, таблиця 2,6

Таблиця 2.6 – Горизонтальна кабельна система

Назва	Опис	Переваги	Недоліки
1	2	3	4
Прокладка в кабель-каналах	Кабелі прокладаються у пластикових чи металевих каналах для захисту від пошкоджень і легкого доступу.	Легкість у встановленні та обслуговуванні, захист кабелів від зовнішніх впливів	Обмежена гнучкість у зміні траси прокладки

Продовження таблиці 2.6

1	2	3	4
Прокладка під підвісними стелями:	Кабелі прокладаються у просторі між підвісною стелею та основною стелею приміщення	Приховане прокладання, легкий доступ для обслуговування	Необхідність наявності підвісної стелі

Основні методи прокладки кабелів та їхні переваги і недоліки наведено в таблиці 2.7.

Таблиця 2.7 – Вертикальна кабельна система

Назва	Опис	Переваги	Недоліки
Прокладка у вертикальних шахтах	Кабелі прокладаються у спеціальних шахтах або трубопроводах, що проходять через всі поверхи будівлі.	Надійність та захист кабелів, легкий доступ для обслуговування.	Потреба у спеціальних конструкціях для прокладання..
Прокладка в кабель-каналах:	Кабелі прокладаються у вертикальних кабель-каналах, які забезпечують захист кабелів та легкий доступ для обслуговування.	Легкість у встановленні та обслуговуванні, захист кабелів від зовнішніх впливів.	Обмежена гнучкість у зміні траси прокладки.

Для комп'ютерного клубу було обрано наступні типи кабелів та методи їх прокладки:

– горизонтальна кабельна система: кабель Cat 6 UTP (Прокладка в кабель-каналах та підвісних стелях).

– вертикальна кабельна система: многомодовий оптоволоконний кабель (Прокладка у вертикальних шахтах).

Цей вибір забезпечує оптимальну швидкість передачі даних, надійність та легкість обслуговування мережі, що відповідає вимогам сучасного комп'ютерного клубу.

2.2.2 Будова вузлів та необхідність їх застосування

У комп'ютерній мережі комп'ютерного клубу основними вузлами є сервери, комутатори, маршрутизатори та кінцеві пристрої (комп'ютери, принтери тощо). Кожен з цих вузлів має специфічну будову та функції, що забезпечують стабільну роботу всієї мережі.(див.рис.2.8)

Сервери:

– високопродуктивний багатоядерний процесор для обробки великої кількості запитів.

– великий обсяг пам'яті RAM для швидкої обробки даних і забезпечення багатозадачності.

– накопичувачі SSD для швидкого доступу до даних та HDD для зберігання великих обсягів інформації.

– гігабітні або 10-гігабітні мережеві адаптери для високошвидкісного з'єднання.

– блок живлення з резервуванням, система охолодження та управління.

Комутатори:

– комутатори для управління трафіком забезпечують швидке з'єднання між кінцевими пристроями, мінімізуючи затримки та підвищуючи швидкість передачі даних.

– можливість розподілу мережі на VLAN, логічні сегменти для покращення безпеки та управління трафіком.

Маршрутизатори:

– маршрутизатори розподіляють трафік між різними підмережами та забезпечують з'єднання з зовнішніми мережами.

– інтегровані функції безпеки захищають мережу від зовнішніх загроз та забезпечують безпечний доступ до ресурсів.

Кінцеві пристрої:

– комп'ютери забезпечують користувачам доступ до ігор, інтернету та інших мережевих послуг.

– мережеві принтери та інші пристрої забезпечують додаткові послуги, необхідні для повноцінної роботи клубу.

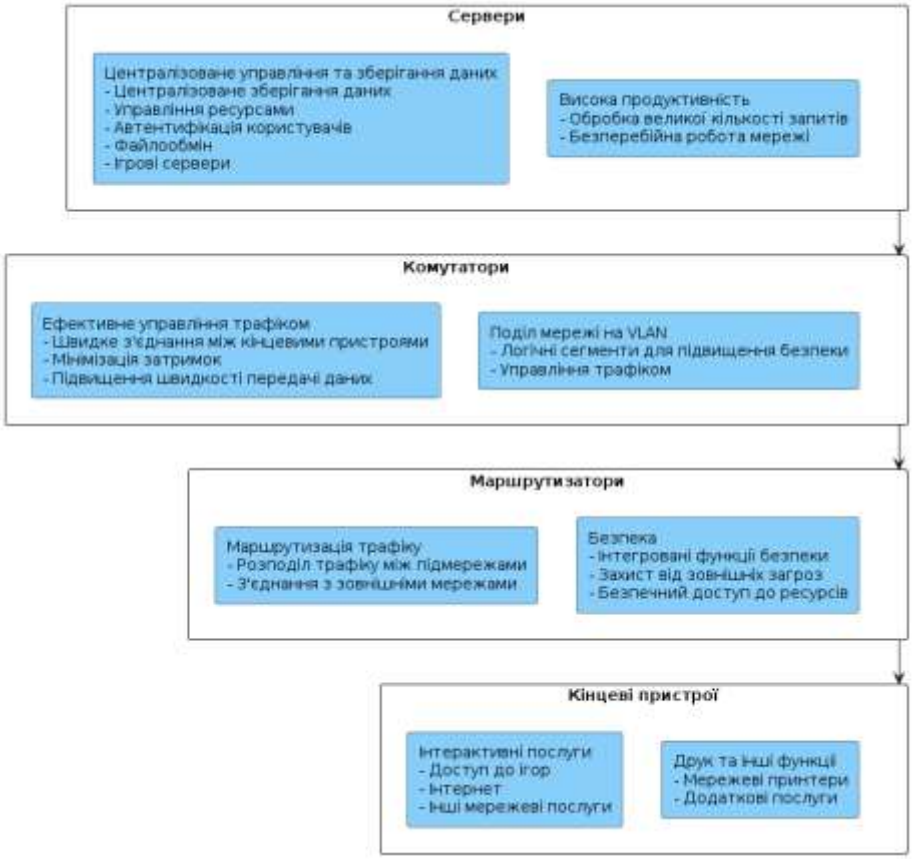

Рисунок 2.8 – Застосування різних вузлів у комп'ютерному клубі

Необхідність застосування вузлів (див.рис.2.9):

- централізоване управління та зберігання даних
- висока продуктивність
- ефективне управління трафіком
- поділ мережі на VLAN
- маршрутизація трафіку
- безпека
- інтерактивні послуги
- друк та інші функції

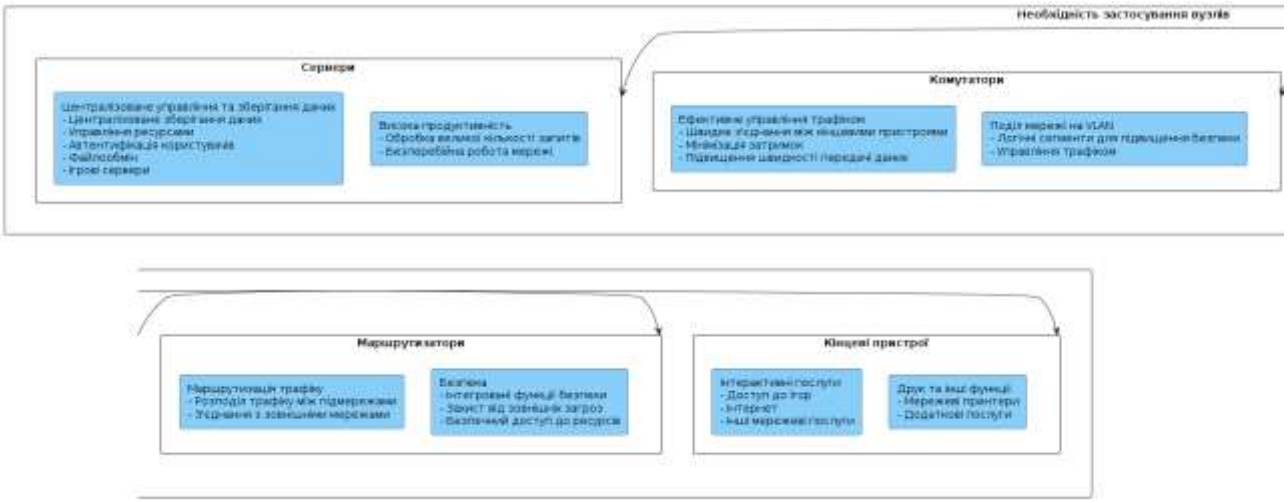

Рисунок 2.9 – Необхідність застосування вузліву комп'ютерному клубі

Використання цих вузлів забезпечує ефективну роботу комп'ютерного клубу, надаючи користувачам високоякісний доступ до мережевих ресурсів та ігор. Вони також дозволяють адміністраторам легко управляти та масштабувати мережу, підвищуючи її надійність та безпеку.

2.3 Обґрунтування вибору обладнання для мережі

Згідно вимог TIA/EIA-568B, для побудови комп'ютерної мережі комп'ютерного клубу необхідно вибрати відповідне комунікаційне обладнання. Це обладнання повинно забезпечувати високу продуктивність, надійність, можливість масштабування та ефективне управління мережею [9].

Вибір проміжного комутаційного вузла (IDF) та головного комутаційного вузла (MDF). IDF розташовуються на кожному поверсі для забезпечення зв'язку між кінцевими пристроями і головним комутаційним вузлом. Основним обладнанням IDF є керовані комутатори з підтримкою VLAN та необхідною пропускною здатністю. MDF є центральним вузлом мережі, де розміщуються основні маршрутизатори, комутатори та сервери. MDF забезпечує зв'язок між підмережами та зовнішніми мережами.

Вибір активного, таблиця 2.10, та пасивного, таблиця 2.11, обладнання:

Таблиця 2.10 – Активне обладнання

Назва	Марка	Кількість портів	Швидкість портів	Пропускна здатність	Швидкість комутації	Ціна (грн)
Комутатори (Switches)	D-Link DGS-1210-28/ME	24 + 4 (SFP)	10/100/1000	41.7 млн. пакетів/с	56 Гбіт/с	5200
	TP-Link T2600G-28TS (TL-SG3424)	24 + 4 (SFP)	10/100/1000	41.67 млн. пакетів/с	56 Гбіт/с	7500
	HP Aruba 2530-24G	24 + 4 (SFP)	10/100/1000	41.6 млн. пакетів/с	56 Гбіт/с	9152

Таблиця 2.11 – Пасивне обладнання

№ п/п	Характеристики обладнання	Модель вибраного пристрою (D-Link DGS-1210-28/ME)	Аналог 1 TP-Link T2600G-28TS (TL-SG3424)	Аналог 2 HP Aruba 2530-24G
1	Кількість портів	24 + 4 (SFP)	24 + 4 (SFP)	24 + 4 (SFP)
2	Швидкість портів	10/100/1000	10/100/1000	10/100/1000
3	Автовизначення швидкості	Так	Так	Так
4	Кількість портів	24 + 4 (SFP)	24 + 4 (SFP)	24 + 4 (SFP)
5	Швидкість портів	10/100/1000	10/100/1000	10/100/1000
6	Автовизначення швидкості	Так	Так	Так
7	Підтримка протоколу IEEE 802.1d	Так	Так	Так
8	Пропускна здатність, млн. пакетів /с	41.7	41.67	41.6
9	Швидкість комутації, Гбіт/с	56	56	56

Продовження таблиці 2.11

№ п/п	Характеристики обладнання	Модель вибраного пристрою (D-Link DGS-1210-28/ME)	Аналог 1 TP-Link T2600G-28TS (TL-SG3424)	Аналог 2 HP Aruba 2530-24G
10	Вартість, грн	5200	7500	9152

Вибір маршрутизаторів та серверів:

- маршрутизатор D-Link DSR-500 з пропускною здатністю 1 Гбіт/с,, підтримка VPN, Firewall, вартыстю близько 5214 грн.

- сервер Patriot Rack 1U E3-1220V3 з процесором Intel Xeon E3-1220V3, ОЗП на 16 ГБ (DDR3), накопичувачем 1 ТБ SSD, вартістю близько 32517 грн.

Таблиця 2.12 – Зведена таблиця розрахунку необхідності телекомунікаційного обладнання

Назва елемента	Позначення	Модель	Ціна, грн	Од. вим.	К-ть
Кабель	-	UTP cat 5e	510	м	500
Роз'єми	-	RJ-45	69	шт	200
Телекомунікаційна розетка	-	Electrum RJ-45	28	шт	49
Керований комутатор	MDF	D-Link DGS-1210-28/ME	5200	шт	3

Продовження таблиці 2.12

Назва елемента	Позначення	Модель	Ціна, грн	Од. вим.	К-ть
Маршрутизатор	-	D-Link DSR-500	5214	шт	1
Сервер	S_1	Patriot Rack 1U E3-1220V3	32517	шт	2

Вибране комунікаційне обладнання, таблиця 2.12 задовольняє всі необхідні технічні вимоги для побудови надійної, високопродуктивної та масштабованої комп'ютерної мережі для комп'ютерного клубу. Обране обладнання забезпечує ефективне управління трафіком, високий рівень безпеки та зручність адміністрування мережі.

2.4 Особливості монтажу мережі

Монтаж комп'ютерної мережі в комп'ютерному клубі потребує врахування кількох важливих аспектів для забезпечення надійної та ефективної роботи мережі [10]. Нижче наведено основні етапи та особливості монтажу мережі. Перед початком монтажу необхідно провести ретельне планування та підготовку:

- підготовчий етап
- прокладка кабелів
- налаштування та тестування
- введення в експлуатацію

Проведення огляду приміщення для визначення оптимальних шляхів прокладки кабелів. Визначення місць розташування серверних кімнат, розподільчих шаф та точок доступу. Розробка детального плану мережі з урахуванням логічної та фізичної топології. Визначення маршруту прокладки кабелів. Вибір необхідного обладнання та матеріалів. Прокладка кабелів від

серверних кімнат до робочих місць через кабель-канали, підвісні стелі або спеціальні труби [11]. Використання UTP кабелів категорії 5e або 6 для забезпечення високої швидкості передачі даних. Прокладка магістральних кабелів між поверхами для з'єднання серверних кімнат. Використання оптоволоконних кабелів для магістральних з'єднань, що забезпечує високу пропускну здатність і мінімальні втрати сигналу. Розміщення серверів, комутаторів, маршрутизаторів і іншого активного обладнання в серверних шафах або стійках. Забезпечення належної вентиляції та охолодження обладнання. Встановлення джерел безперебійного живлення (UPS) для захисту від збоїв у електропостачанні. Встановлення патч-панелей та крос-панелей для зручного підключення та перемикання кабелів. Використання маркування для всіх з'єднань для полегшення обслуговування та управління мережею.

Конфігурація комутаторів, маршрутизаторів, серверів і точок доступу згідно з проектними вимогами. Налаштування VLAN для сегментації мережі та підвищення її безпеки. Перевірка всіх з'єднань на цілісність та відповідність стандартам. Тестування пропускної здатності мережі та її продуктивності. Перевірка роботи всіх мережевих сервісів та обладнання. Складання

повної документації по мережі, включаючи схеми з'єднань, конфігурації обладнання та результати тестувань. Опис процедур обслуговування та оновлення мережі. Проведення навчання для технічного персоналу щодо обслуговування та управління мережею. Надання інструкцій з усунення несправностей та оперативного реагування на інциденти.

Правильне планування та монтаж мережі комп'ютерного клубу забезпечать її надійну та ефективну роботу. Врахування всіх технічних і організаційних аспектів дозволить створити мережу, яка буде відповідати всім вимогам з точки зору продуктивності, безпеки та масштабованості.

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

При виборі операційних систем (ОС) для робочих станцій та серверів, слід враховувати кілька ключових факторів, включаючи профіль роботи організації, сумісність з апаратним забезпеченням, наявність і сумісність існуючого програмного забезпечення, а також загальні витрати, таблиця 2.13

Таблиця 2.13 – Вибір операційних систем для робочих станцій

ОС	Переваги	Недоліки
1	2	3
Windows 10/11	Широка підтримка програмного забезпечення.	Висока вартість ліцензій.
	Висока сумісність з апаратним забезпеченням.	Регулярні оновлення можуть потребувати значних ресурсів.
	Інтуїтивно зрозумілий інтерфейс для кінцевих користувачів.	
	Потужні можливості для корпоративного управління через Active Directory.	
Linux (Ubuntu, Fedora)	Безкоштовна та відкрита ОС.	Відносно крута крива навчання для користувачів, які не знайомі з Linux.

Продовження таблиці 2.13

1	2	3
	Висока стабільність і безпека.	Можливі проблеми із сумісністю

		програмного забезпечення.
	Відмінна підтримка для розробників та системних адміністраторів.	

Windows 10/11 підходить для організацій, що використовують спеціалізоване ПЗ, яке працює лише на Windows. Забезпечує легкий доступ до оновлень та технічної підтримки. Ubuntu Linux відмінний вибір для розробників та організацій з обмеженим бюджетом, де використовуються відкриті рішення, таблиця 2.14

Таблиця 2.14 – Вибір операційних систем для серверів

ОС	Переваги	Недоліки
1	2	3
Windows Server 2019/2022	Інтеграція з Windows середовищем робочих станцій	Висока вартість ліцензій
	Підтримка широкого спектру серверних ролей та функцій	Більша потреба в апаратних ресурсах порівняно з Linux
	Потужні засоби для віртуалізації та управління мережею	

Продовження таблиці 2.14

1	2	3
Linux Server (Ubuntu Server, CentOS, Red Hat Enterprise Linux)	Безкоштовні або низьковартісні ліцензії	Потреба у високій кваліфікації для адміністрування
	Висока стабільність і	

	безпека	
	Широкі можливості для налаштування та оптимізації	

Для організації мережевих сервісів різного рівня та складності було розглянуто наступне програмне забезпечення, таблиця 2.15:

Таблиця 2.15 – Вибір мережевих сервісів

Вид ПЗ	Назва	
Електронна пошта	Microsoft Exchange	Потужний поштовий сервер з інтеграцією з іншими продуктами Microsoft.
	Postfix/Dovecot	Безкоштовне рішення на базі Linux, висока налаштовуваність та безпека.
Чат	Microsoft Teams	Інтеграція з іншими продуктами Microsoft, зручність використання.
	Slack	Популярне рішення для командної роботи, зручний інтерфейс
Сторінка FAQ та служба розсилки повідомлень	WordPress з плагінами FAQ	Легке в налаштуванні та використанні, підтримка різноманітних плагінів.
	Mailchimp	Потужна служба для розсилки електронних листів, інтеграція з різними платформами.

Продовження таблиці 2.15

Дошки оголошень	phpBB	Безкоштовне та широко використовуване рішення для створення форумів.
	Discourse	Сучасна платформа для обговорень з активною спільнотою підтримки.

Для забезпечення безперебійного доступу до інтернету з внутрішньої мережі передбачено використання веб-сервера. Тип веб-сервера та приклад його конфігурування будуть наведені в розділі 3. Розглянуті такі варіанти, таблиця 2.16:

Таблиця 2.16 – Вибір тип веб-сервера

Назва	Переваги	Недоліки
Apache	Висока стабільність, велика кількість модулів, підтримка різних операційних систем.	Складність налаштування для новачків.
Nginx	Висока продуктивність, низькі вимоги до ресурсів, простота налаштування.	Менша кількість модулів порівняно з Apache.

Таким чином, вибір операційних систем та мережевого програмного забезпечення обґрунтовано з урахуванням специфіки діяльності організації, технічних вимог та фінансових можливостей. Це забезпечить стабільну, безпечну та ефективну роботу мережі, а також дозволить легко масштабувати та модернізувати її в майбутньому.

2.6 Обґрунтування вибору засобів захисту мережі

Для забезпечення безпеки мережі від несанкціонованого доступу необхідно використовувати комплексний підхід, що включає різні засоби та методи захисту. Необхідно розглянути вибір та обґрунтування засобів захисту мережі.

Основні характеристики та обґрунтування вибору мережевого обладнання показано в таблиці 2.17.

Таблиця 2.17 – вибір та обґрунтування брандмауери (Firewall)

Назва	Функції	Обґрунтування вибору
D-Link DFL-1660	Виявлення та запобігання вторгнень (IDS/IPS), фільтрація трафіку, VPN	Високий рівень безпеки, підтримка різних типів підключень, можливість масштабування
Cisco ASA 5506-X	Захист від атак на рівні додатків, захист від DDoS атак, VPN, управління доступом	Надійність, продуктивність, гнучкі налаштування політик безпеки

Ось посилання на таблицю 2.18, яка містить детальну інформацію про Kaspersky Endpoint Security та ESET Endpoint Security, включаючи їхні функції та обґрунтування вибору. У цій таблиці ви знайдете порівняльний аналіз цих двох популярних рішень для захисту кінцевих точок, що допоможе вам визначитися з вибором найбільш підходящого продукту для вашої організації.

Таблиця 2.18 – Вибір та обґрунтування антивірусного програмного забезпечення

Назва	Функції	Обґрунтування вибору
Kaspersky Endpoint Security	Захист від вірусів, шпигунського ПЗ, фішинг-атак, брандмауер, контроль програм	Високий рівень захисту, регулярні оновлення баз даних, зручне управління
ESET Endpoint	Захист від вірусів, антифішинг, захист	Висока ефективність, невелике навантаження на систему,

Security	мережевого трафіку, управління пристроями	гнучкі налаштування

Ось посилання на таблицю 2.19, що містить інформацію про вибір протоколів захисту мережі:

Таблиця 2.19 – Вибір протоколів захисту мережі

Вид	Назва	Обґрунтування вибору
1	2	3
Шифрування даних	SSL/TLS (Secure Sockets Layer/Transport Layer Security):	Захист даних під час передачі, використання для захищеного доступу до веб-сайтів, електронної пошти, VPN.
	IPsec (Internet Protocol Security)	Захист IP-трафіку шляхом шифрування, забезпечення автентифікації та цілісності даних
Автентифікація та авторизація	RADIUS (Remote Authentication Dial-In User Service)	Централізована автентифікація, контроль доступу, управління правами користувачів

Продовження таблиці 2.19

1	2	3
	LDAP (Lightweight Directory Access Protocol)	Централізоване управління обліковими записами користувачів, інтеграція з різними сервісами, зручний доступ до каталогів

Контроль доступу	протокол EAP - Extensible Authentication Protocol	Встановлення механізмів для контролю доступу до радіомережі

Загальною метою вибору засобів захисту мережі є забезпечення конфіденційності, цілісності та доступності даних, а також мінімізація ризику виникнення інцидентів та атак.

2.7 Тестування та налагодження мережі

Під час введення мережі в експлуатацію важливо було провести процедуру тестування для переконання у правильності її налаштування та функціонування. Нижче представлено процедуру тестування мережі та на рисунку 2.17 показано бланк результатів тестування.

Процедура тестування мережі:

– використання кабельних тестерів для перевірки кабелів на відповідність стандартам і виявлення можливих дефектів або переривань.

– перевірка правильності підключення пристроїв до комутаторів або інших мережевих вузлів.

– виконання пінг-тестування для перевірки доступності мережевих пристроїв між собою.

– перевірка функціональності мережевих сервісів, таких як DHCP, DNS, електронна пошта тощо.

– тестування доступу до Інтернету та інших зовнішніх мережевих ресурсів.

– виконання сканування портів для виявлення вразливостей мережевих пристроїв.

– перевірка конфігурації файерволів та систем аутентифікації.

Ось посилання на таблицю 2.20, що містить інформацію про характеристики Fluke Networks CableIQ Qualification Tester та Fluke Networks DSX-5000 CableAnalyzer:

Таблиця 2.20 – Кабельні тестери та їх характеристики

Назва	Характеристики
Fluke Networks CableIQ Qualification Tester	Підтримує категорії кабелів від Cat 3 до Cat 6a
	Вимірює довжину кабелю та виявляє можливі дефекти (переривання, замикання)
	Перевіряє передачу даних на великі відстані
Fluke Networks DSX-5000 CableAnalyzer	Підтримує категорії кабелів від Cat 5 до Cat 8
	Вимірює довжину кабелю, рівень сигналу, затухання та кількість замикань
	Автоматично генерує звіт з результатами тестування

Ось посилання на таблицю 2.21, що містить параметри тесту, вимоги до мережі та фактичні результати:

Таблиця 2.21 – Бланк результатів тестування мережі

Параметр тесту	Вимоги до мережі	Фактичні результати
1	2	3
Фізичне з'єднання	Кабелі категорії 6a	Виявлено 1 переривання на кабелі в зоні №3

Продовження таблиці 2.21

1	2	3
Пінг-тестування	Всі пристрої мають бути доступними між собою	Успішно пройдено. Всі пристрої відповідають на запити
DHCP сервіс	DHCP сервер повинен надавати IP	DHCP сервер працює коректно. Всі пристрої

	адреси пристроям	отримали IP адреси
Доступ до Інтернету	Пристрої мають мати доступ до Інтернету.	Успішно пройдено. Всі пристрої можуть виходити в Інтернет.

Вищевказаний бланк результатів тестування допомагає систематизувати результати тестування та швидко виявити будь-які недоліки у мережі.

3. СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

Налаштування операційних систем:

– встановити ОС Windows Server 2019 з диска або USB-накопичувача за допомогою інсталяційного медіа.

– налаштування мережевих параметрів: присвойте серверу статичну IP-адресу, встановіть правильні DNS-сервери.

– активація ОС, ввести ліцензійний ключ та активувати операційну систему.

– завантажити та встановити оновлення безпеки та пакети оновлень для операційної системи.

Налаштування служб локальної мережі:

– створити папки та ресурси, які будуть доступні для спільного використання.

– налаштувати права доступу до файлів та папок для користувачів.

– додати принтери та налаштувати їх для мережевого друку.

– налаштувати дозволи доступу до принтерів для користувачів.

– встановити та налаштувати Active Directory для централізованого керування користувачами та групами.

– встановити та налаштувати базу даних (наприклад, Microsoft SQL Server або MySQL).

– створити базу даних та користувачів з правами доступу до них.

Налаштування служб локальної мережі:

- створити папки та ресурси, які будуть доступні для спільного використання.

- створіть та налаштуйте електронні скриньки для користувачів.

- встановіть та налаштуйте веб-сервер (наприклад, Apache або Microsoft IIS).

- розмістіть веб-сайти та налаштуйте їх доступність ззовні.

- встановіть та налаштуйте FTP-сервер (наприклад, FileZilla Server або Microsoft FTP Server).

- створіть облікові записи користувачів та налаштуйте права доступу до FTP-ресурсів.

- встановіть та налаштуйте VPN-сервер (наприклад, OpenVPN або Microsoft RRAS).

- налаштуйте правила доступу та обмеження для користувачів, що підключаються через VPN.

Ці інструкції забезпечують належне налаштування серверів та їх служб для повноцінного функціонування в мережі. Важливо виконати всі кроки з урахуванням потреб та вимог проекту ЛОМ.

3.2 Інструкції з налаштування активного комутаційного обладнання

Підключення до комутатора:

– за допомогою консольного кабелю підключіться до комутатора через консольний порт (RS-232 або USB).

– використовувати терміналний програмне забезпечення (наприклад, PuTTY) для доступу до комутатора через консоль.

– увійти в веб-інтерфейс комутатора, використовуючи його IP-адресу та облікові дані адміністратора.

– при вході до режиму конфігурації, ввести логін та пароль для входу до комутатора. Перейти до режиму конфігурації комутатора, ввести команду Enable.

– створити та налаштувати VLAN, перейти до розділу «VLAN» і додати нові VLAN. Призначте порти VLAN та налаштуйте Trunk-порти.

– налаштувати статичну маршрутизацію: перейти до розділу «IP Routing» і додати статичні маршрути для кожної підмережі.

Конфігурування комутаторів та маршрутизаторів:

– виконати вхід до консольного інтерфейсу комутатора або маршрутизатора за допомогою програми терміналу (наприклад, PuTTY).

– створити таблицю маршрутизації за допомогою команди ip route. Визначте маршрути до інших підмереж та зовнішніх мереж.

– виконати вхід до консольного інтерфейсу комутатора або маршрутизатора. Створити листи доступу за допомогою команди access-list. Визначити правила доступу для фільтрації трафіку згідно з потребами мережі.

Налаштування VLAN:

– виконати вхід до консольного або веб-інтерфейсу комутатора.

– створити та налаштуйте VLAN за допомогою команди vlan.

– призначити порти комутатора до відповідних VLAN за допомогою команди SwitchPort access VLAN.

Статична маршрутизація між підмережами:

– виконати вхід до консольного інтерфейсу маршрутизатора.

– створити статичні маршрути до кожної підмережі за допомогою команди ip route.

– перевірити правильність налаштувань маршрутизації за допомогою команди Show IP Route.

Приклад конфігураційних файлів. Конфігурування комутаторів та маршрутизаторів:

– створення VLAN. Комутатор Cisco Catalyst 2960.

Виконати вхід до консольного або веб-інтерфейсу комутатора. Створіть VLAN за допомогою команди vlan <VLAN_ID> і надати йому ім'я за допомогою команди name <VLAN_NAME>. Призначити порти комутатора до відповідних VLAN за допомогою команди switchport access vlan <VLAN_ID>.

– статична маршрутизація між підмережами. Маршрутизатор Cisco ISR 4000. Виконати вхід до консольного інтерфейсу маршрутизатора. Створити статичні маршрути до кожної підмережі за допомогою команди ip route <DESTINATION_NETWORK> <MASK> <NEXT_HOP>. Наприклад: ip route 192.168.2.0 255.255.255.0 192.168.1.2 для маршрутизації до підмережі 192.168.2.0 через IP-адресу 192.168.1.2.

Конфігурація комутатора Cisco Catalyst 2960:

```
hostname Switch
interface GigabitEthernet0/1
switchport mode access
switchport access vlan 10
interface GigabitEthernet0/2
switchport mode access
switchport access vlan 20
ip default-gateway 192.168.1.1
```

Конфігурація маршрутизатора Cisco ISR 4000:

```
hostname Router
interface GigabitEthernet0/0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet0/0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
ip route 192.168.3.0 255.255.255.0 192.168.2.2
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Ці інструкції забезпечують належне конфігурування активного комутаційного обладнання для оптимального функціонування в мережі.

На рисунку 3.1 показується веб-інтерфейс налаштування Cisco Catalyst 2960-X Series, де ви можете встановити мережеві параметри, налаштування Ethernet-порту управління та додаткові параметри, такі як ім'я хоста, дата системи та часовий пояс.

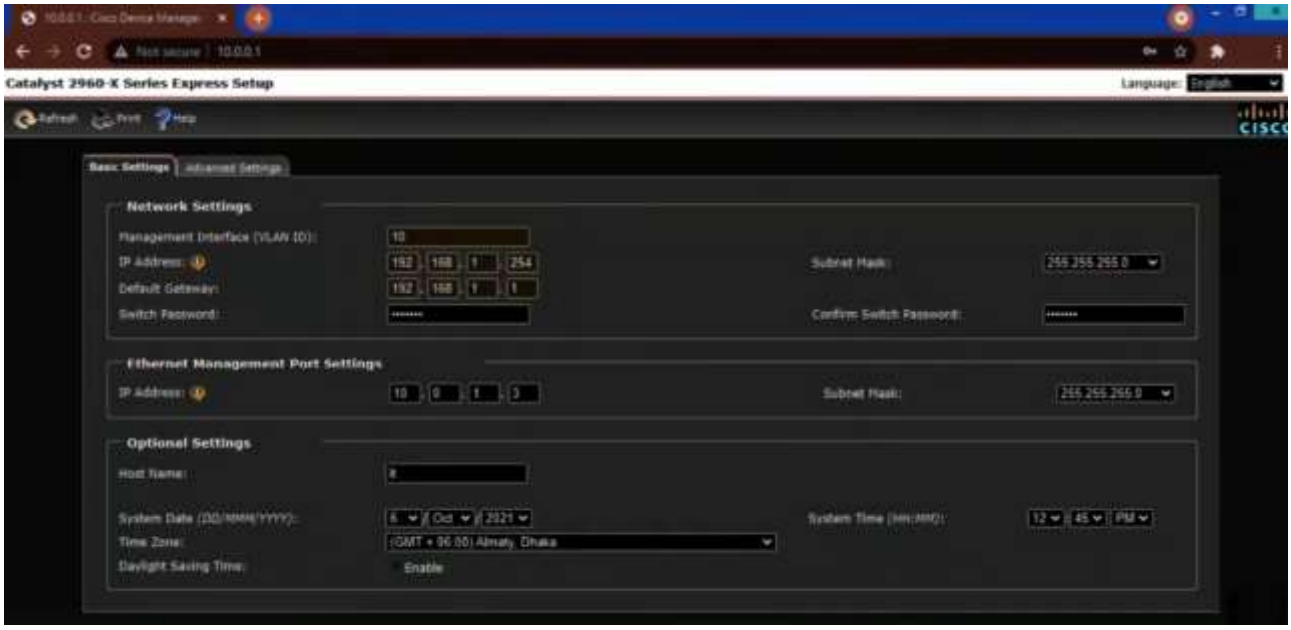

Рисунок 3.1 – Скріншот конфігурації комутатора Cisco Catalyst 2960

Цей рисунок містить наступну інформацію:

- **Версія Cisco IOS-XE:** Повідомлення про версію програмного забезпечення, яке використовується на маршрутизаторі.
- **Час роботи маршрутизатора:** Час, протягом якого маршрутизатор був активний з моменту останнього перезапуску.
- **Інформація про процесор:** Час роботи процесора та інші характеристики.
- **Файл образу системи:** Назва та версія образу системи, який використовується.
- **Криптографічні функції:** Відомості про криптографічні можливості та відповідність законодавству США щодо експорту, імпорту та використання криптографії.
- **Ліцензійні умови:** Інформація про ліцензії, що надаються з продуктом, включаючи технологічні пакети, типи ліцензій та умови їх використання.
- **Технологічні пакети:** Деталі про встановлені технологічні пакети, їх поточний статус та умови наступного перезапуску.
- **Пам'ять маршрутизатора:** Інформація про доступну та використану пам'ять маршрутизатора.
- **Реєстр конфігурації:** Значення реєстру конфігурації, що визначає режим завантаження маршрутизатора.

Ця інформація є важливою для адміністраторів мереж, які мають знати про програмне забезпечення, ліцензії та апаратні характеристики своїх пристроїв Cisco.

Рисунок 3.2 – Скріншот конфігурації маршрутизатора Cisco ISR 4000

3.3 Інструкції з використання тестових наборів та тестових програм

Ping:

Використовується для перевірки доступності пристроїв у мережі та вимірювання часу відправки та отримання пакетів. Спосіб використання. Виконайте команду ping <IP_адреса_пристрою> у командному рядку операційної системи. Якщо відповідь на ping запити успішна (зазвичай підтверджена відповіддю «Reply from <IP_адреса>: bytes=32 time=<час_відповіді>ms»), це означає, що пристрій доступний у мережі. Якщо отримано повідомлення про неуспішну відповідь (наприклад, «Request

timed out»), це може вказувати на проблеми з доступністю пристрою або маршрутизацією до нього.

Це показується на рисунку 3.3, результати ping-тестування до локальної IP-адреси 192.168.1.5 та зовнішньої IP-адреси google.com (216.58.196.110). Включає інформацію про відправлені і отримані пакети, час затримки (round trip time) та статистику втрат пакетів для обох тестів.

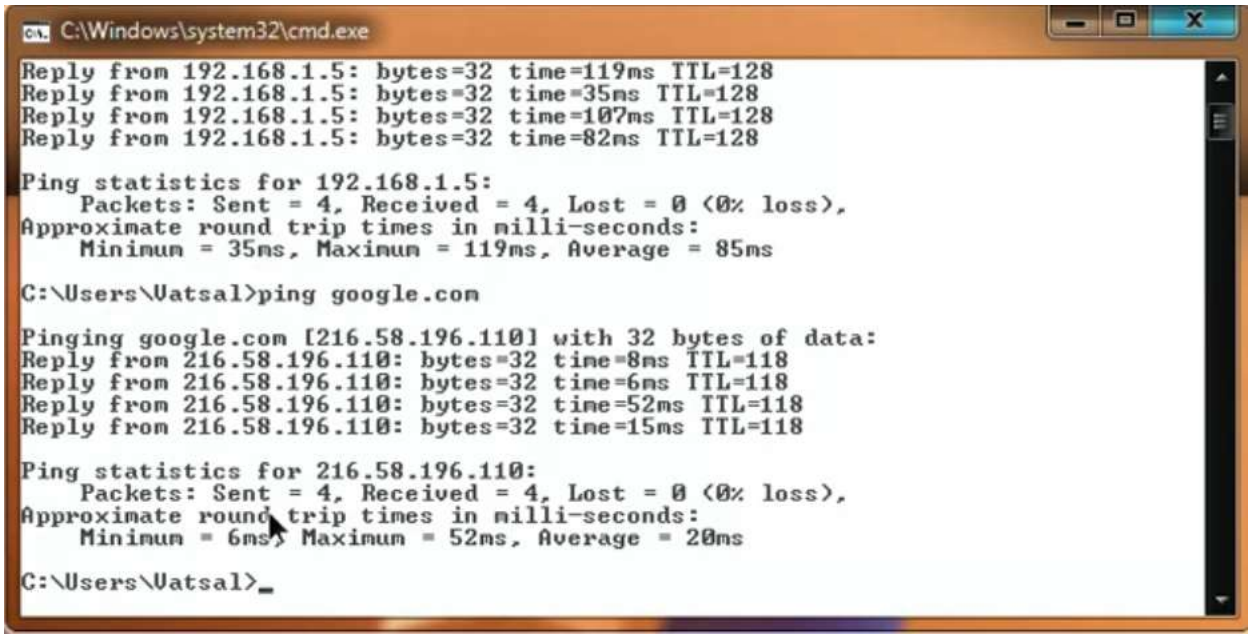

Рисунок 3.3 – Скріншот використання тестових програм

Traceroute:

Допомагає визначити шлях, який пакети дійшли від одного пристрою до іншого, а також час, який зайняло це подорож. Спосіб використання: Виконайте команду traceroute <IP_адреса_пристрою> у командному рядку операційної системи. Результати Traceroute показують шлях, який пакети проходять від відправника до отримувача. Це допомагає виявити проблеми маршрутизації або затримки на маршруті. Кожен рядок виводу представляє маршрутизатор або пристрій у мережі, через який пройшов пакет, а також час затримки до цього вузла.

На рисуноку 3.4 показується результати команд ping та tracert для IP-адреси 192.168.50.1. Команда ping показує, що всі запити до цієї IP-адреси

завершилися тайм-аутом (100% втрата пакетів). Команда tracert показує маршрут до IP-адреси 192.168.50.1, включаючи проміжні вузли, на яких були виявлені тайм-аути.

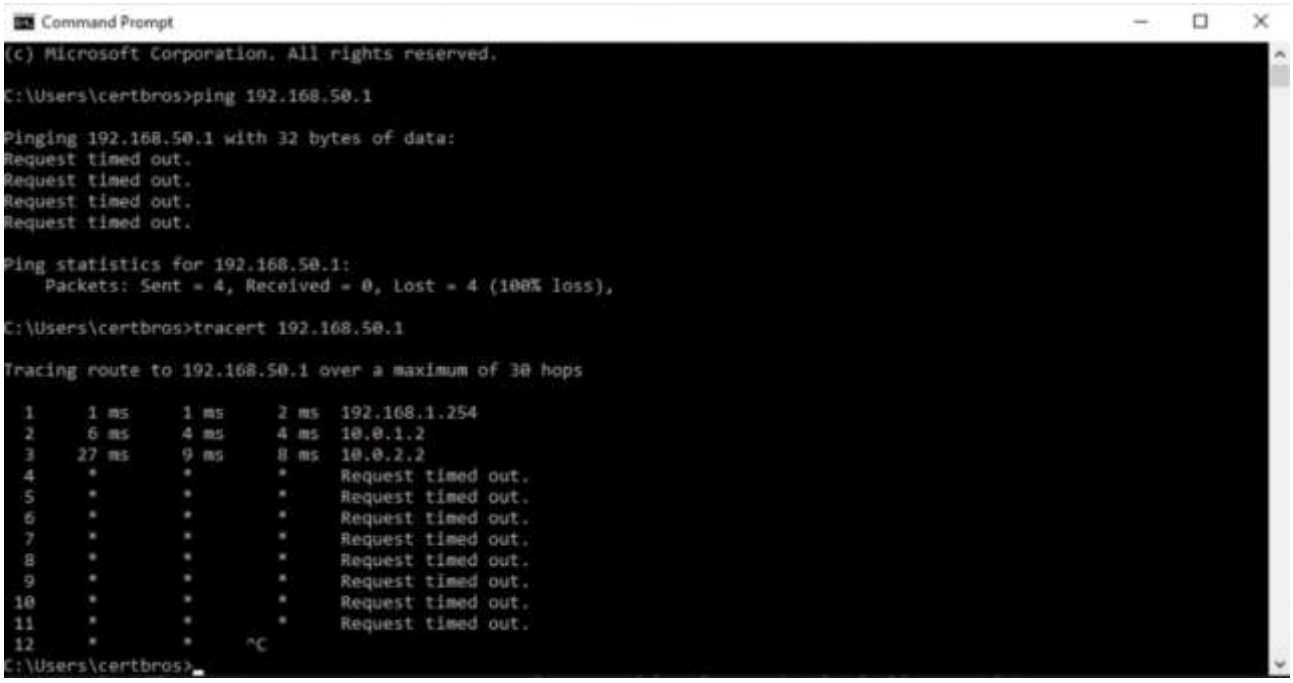

Рисунок 3.4 – Скріншот використання тестових програм

Wireshark:

Використовується для аналізу мережевого трафіку, перехоплення та відображення пакетів даних. Спосіб використання: Запустіть програму Wireshark, оберіть мережевий інтерфейс та почніть перехоплення пакетів. Результати виведені в Wireshark можуть включати перехоплені пакети даних, які можна аналізувати для виявлення аномалій у мережевому трафіку, таких як втрати пакетів, дублювання або атаки зломщиків.

Цей рисунок 3.5 демонструє результати аналізу мережевого трафіку за допомогою Wireshark, популярного інструменту для моніторингу та аналізу мереж. Інтерфейс Wireshark показує різноманітні пакети даних, що передаються через мережу, включаючи ICMP-запити та відповіді. Використовуючи Wireshark, можна детально переглядати та аналізувати інформацію про пакети, що дозволяє ідентифікувати проблеми з маршрутизацією, затримки, втрати пакетів та інші мережеві аномалії. Цей

інструмент є незамінним для адміністраторів мереж та фахівців з кібербезпеки, оскільки дозволяє виявляти і вирішувати різні мережеві проблеми.

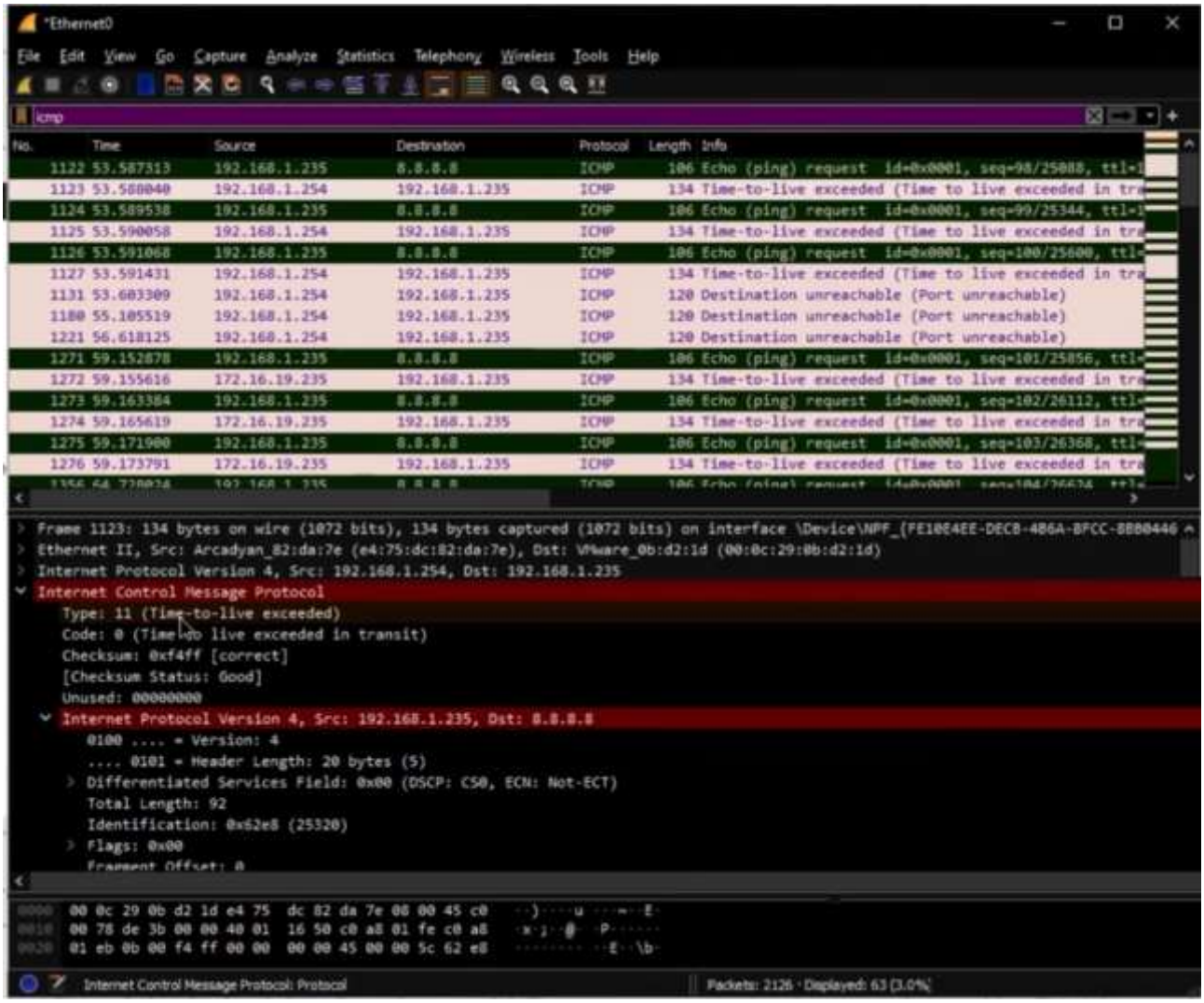

Рисунок 3.5 – Скріншот використання тестових програм

Netcat:

Утиліта для зчитування та запису даних через TCP та UDP протоколи.(див.рис3.6) Спосіб використання. Виконайте команду nc -l -p <порт> для прослуховування порту або nc <IP_адреса> <порт> для встановлення з'єднання з вказаним пристроєм та портом. При успішному встановленні з'єднання можна передавати дані між пристроями. Відсутність

помилок або повідомлення про успішне з'єднання свідчить про правильну роботу програми.

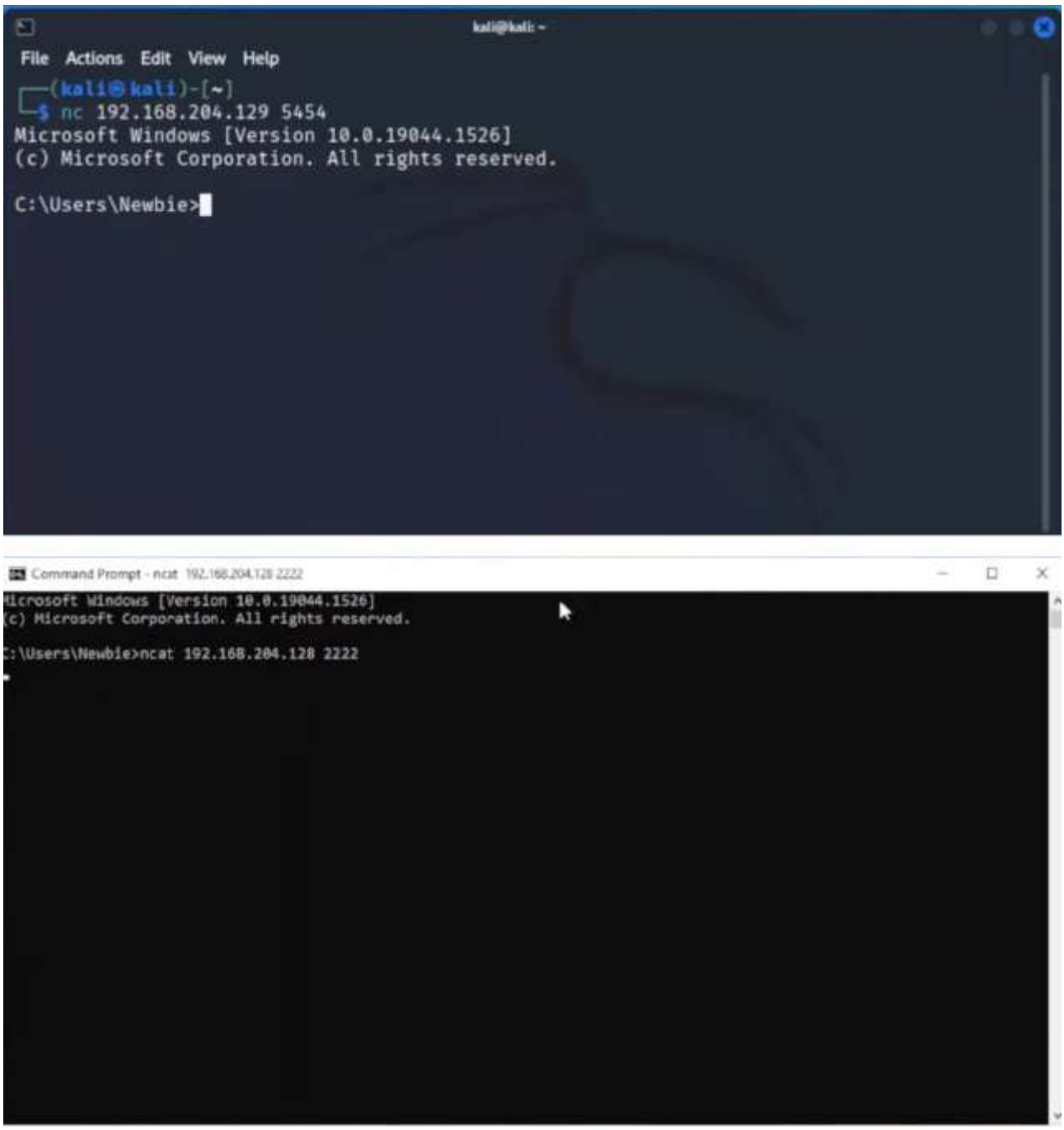

Рисунок 3.6 – Скріншот використання тестових програм

iperf:

Використовується для вимірювання пропускної здатності мережі шляхом передачі даних між пристроями. Спосіб використання. Запустіть

сервер iperf на одному пристрої командою iperf -s, а потім запустіть клієнтський iperf на іншому пристрої командою iperf -c <IP_адреса_сервера>. Вимірює пропускну здатність мережі та швидкість передачі даних. Високі значення швидкості передачі та мала задержка свідчать про ефективну роботу мережі, показано на рисунку 3.7.

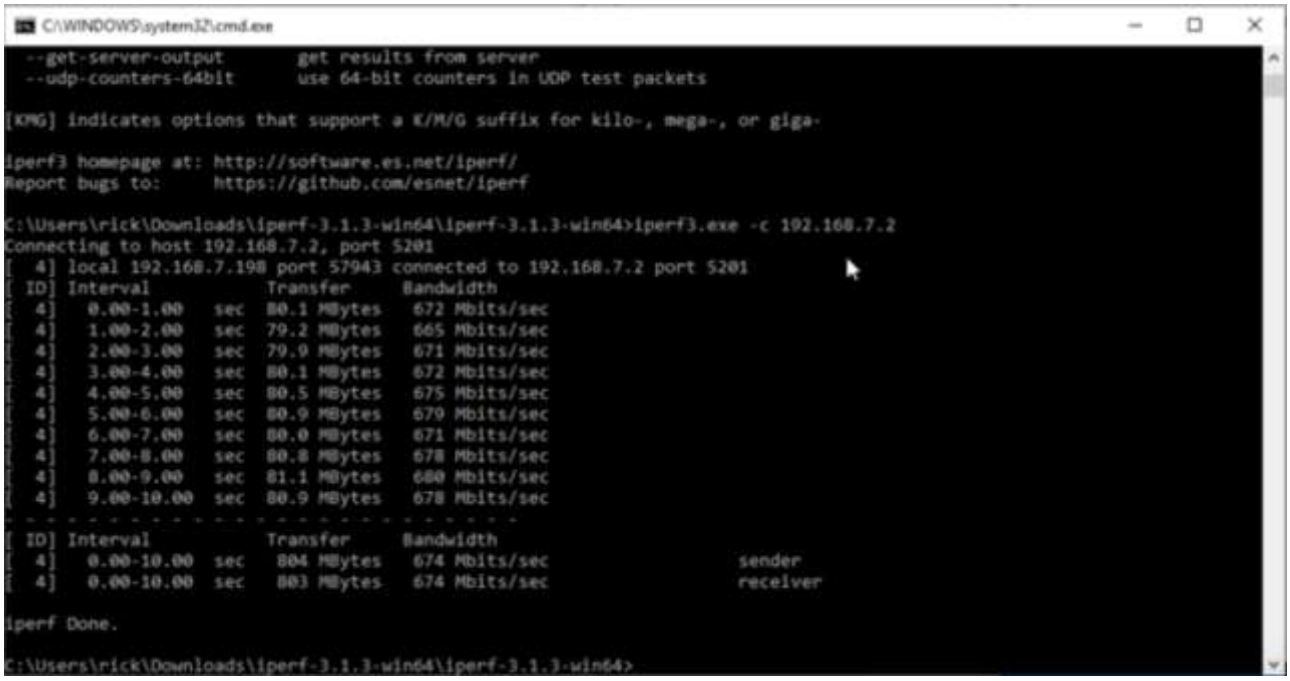

Рисунок 3.7 – Скріншот використання тестових програм

Ці програми та тестові набори можуть бути використані для аналізу, тестування та налагодження мережі, щоб переконатися в її належному функціонуванні та виявити можливі проблеми.

3.4 Інструкції по налаштуванню засобів захисту мережі

У даному розділі описується процес налаштування засобів захисту мережі, включаючи апаратні та програмні засоби, для захисту ЛОМ, операційних систем серверів та служб локальної та глобальної мереж.

Firewall Configuration:

Налаштування правил файрволу для блокування небажаних підключень і трафіку. Створення правил для дозволу доступу лише з визначених IP-адрес

або підмереж. Блокування вразливостей та захист мережі від атак на різних рівнях OSI моделі.

Firewall Configuration Script (iptables for Linux):

```
# Очистка всіх правил та ланцюжків
iptables -F
iptables -X

# Заборона всього трафіку за винятком вихідного та вже встановлених з'єднань
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Дозвіл SSH з певної IP-адреси
iptables -A INPUT -p tcp -s 192.168.1.100 --dport 22 -j ACCEPT

# Дозвіл HTTP та HTTPS
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# Логування неприйнятих пакетів
iptables -A INPUT -j LOG --log-prefix "Firewall: "

# Збереження правил
iptables-save > /etc/iptables/rules.v4
```

Access Control Lists (ACLs):

Налаштування списків доступу на мережевому обладнанні (комутаторах, маршрутизаторах) для контролю доступу до ресурсів мережі.

Визначення прав доступу до певних портів або сервісів залежно від IP-адреси, підмережі, або інших параметрів.

Access Control Lists (ACLs) Configuration Script (Cisco IOS):

```
# Створення стандартного списку доступу
access-list 101 permit tcp any host 192.168.1.100 eq 22
access-list 101 permit tcp any host 192.168.1.100 eq 80
access-list 101 permit tcp any host 192.168.1.100 eq 443
access-list 101 deny ip any any log

# Налаштування списку доступу на інтерфейсі
interface FastEthernet0/0
 ip access-group 101 in
```

Intrusion Detection and Prevention Systems (IDS/IPS):

Налаштування систем виявлення та запобігання вторгнень для виявлення та блокування шкідливого трафіку в реальному часі.

Конфігурування правил для виявлення аномального або підозрілого трафіку та автоматичної реакції на нього.

Intrusion Detection and Prevention Systems (IDS/IPS) Configuration Script (Snort):

```
# Створення правил для виявлення підозрілого трафіку
alert tcp any any -> $HOME_NET any (msg:"Potential SQL Injection";
content:"SELECT"; sid:100001;)
alert udp any any -> $HOME_NET 53 (msg:"Potential DNS Spoofing"; content:"|00 01
00 00 00 01|"; sid:100002;)
# інші правила...

# Запуск Snort з налаштуваннями
snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
```

Encryption and VPN Configuration:

Налаштування віртуальної приватної мережі (VPN) для захищеного тунелювання трафіку через неприватні мережі.

Використання шифрування для захисту конфіденційної інформації під час передачі по мережі.

OpenVPN Configuration Script:

```
# Install OpenVPN
sudo apt-get install openvpn

# Generate the certificate authority (CA)
mkdir -p ~/openvpn-ca && cd ~/openvpn-ca
cp /usr/share/easy-rsa/* .
source vars
./clean-all
./build-ca

# Generate server key and certificate
./build-key-server server

# Generate Diffie-Hellman parameters
./build-dh

# Generate client key and certificate
```

```
./build-key client1

# Copy files to OpenVPN configuration directory
cd keys
sudo cp ca.crt server.crt server.key dh2048.pem /etc/openvpn

# Configure OpenVPN server
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
/etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
sudo nano /etc/openvpn/server.conf
# Edit the configuration file according to your network settings

# Start OpenVPN service
sudo systemctl start openvpn@server
sudo systemctl enable openvpn@server
```

User Authentication and Authorization:

Налаштування систем аутентифікації та авторизації для обмеження доступу користувачів до різних рівнів ресурсів мережі.

Встановлення паролів, ідентифікаційних токенів, аутентифікації за допомогою LDAP або інших методів.

RADIUS Configuration Script:

```
# Install FreeRADIUS
sudo apt-get install freeradius

# Configure RADIUS server
sudo nano /etc/freeradius/3.0/users
# Add user authentication details

# Configure RADIUS clients
sudo nano /etc/freeradius/3.0/clients.conf
# Add client IP and shared secret

# Start FreeRADIUS service
sudo systemctl start freeradius
sudo systemctl enable freeradius
```

Security Auditing and Logging:

Включення журналювання подій для відстеження та аналізу активності користувачів та подій у мережі.

Налаштування моніторингу та сповіщення про підозрілу або аномальну активність.

Example Logrotate Configuration:

```
# Install rsyslog
sudo apt-get update
sudo apt-get install rsyslog

# Configure rsyslog to accept logs from remote systems
sudo nano /etc/rsyslog.conf
# Uncomment the following lines:
# module(load="imudp")
# input(type="imudp" port="514")
# module(load="imtcp")
# input(type="imtcp" port="514")

# Restart rsyslog service
sudo systemctl restart rsyslog

# Configure clients to send logs to the Syslog server
sudo nano /etc/rsyslog.d/50-default.conf
# Add the following line at the end of the file:
*.* @<Syslog_Server_IP>:514

# Restart rsyslog on the client
sudo systemctl restart rsyslog
```

Повний код показано в додатку 5

Реалізуючи наведені вище конфігурації, ви можете налаштувати надійні механізми аудиту безпеки та журналювання. Ці налаштування допомагають контролювати діяльність, виявляти аномалії та ефективно реагувати на потенційні інциденти безпеки. Переконайтеся, що всі механізми реєстрації належним чином захищені для запобігання втручанню та несанкціонованому доступу.

3.5 Інструкції з експлуатації та моніторингу в мережі

Для ефективної експлуатації та моніторингу мережі необхідно мати чітко визначену документацію, процедури моніторингу працездатності, а також алгоритми пошуку та локалізації несправностей [13]. Нижче наведено необхідні елементи, які слід включити в дану інструкцію.

Документація для експлуатації та супроводу мережі

1. Опис мережевої топології:

Документація повинна містити детальні схеми мережі, включаючи всі з'єднання між пристроями. Всі мережеві пристрої повинні бути позначені, включаючи комутатори, маршрутизатори, сервери, точки доступу тощо.

2. Конфігураційні файли:

Копії конфігураційних файлів для всіх мережевих пристроїв. Версії конфігураційних файлів з позначенням дат та змін.

3. Інструкції з налаштування:

Детальні інструкції з налаштування мережевого обладнання та програмного забезпечення. Опис процедур оновлення та резервного копіювання конфігурацій.

4. Контактна інформація:

Контактні дані підтримки виробників обладнання. Контактні дані внутрішньої технічної підтримки.

Процедури відслідковування працездатності мережі та контролю за основними функціональними параметрами:

1. Моніторинг мережі:

Використання спеціалізованого програмного забезпечення для моніторингу, наприклад, Zabbix, Nagios, або PRTG Network Monitor. Налаштування сповіщень про помилки та аномалії в мережі.

Приклад налаштування Zabbix для моніторингу мережі:

```
# Встановлення Zabbix Server
sudo apt-get update
sudo apt-get install zabbix-server-mysql zabbix-frontend-php zabbix-agent

# Налаштування бази даних для Zabbix
sudo mysql -u root -p
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by
'password';
mysql> quit;

# Імпорт початкової бази даних
zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -u zabbix -p zabbix
```

```
# Налаштування Zabbix server
sudo nano /etc/zabbix/zabbix_server.conf
# Зміна параметра DBPassword на 'password'

# Перезапуск Zabbix сервера
sudo systemctl restart zabbix-server zabbix-agent
sudo systemctl enable zabbix-server zabbix-agent
```

2. Контроль за пропускною здатністю та трафіком:

Використання програмного забезпечення для аналізу трафіку, наприклад, Wireshark або SolarWinds.

Регулярне збирання та аналіз статистики трафіку для виявлення потенційних проблем.

3. Резервне копіювання конфігурацій:

Автоматизовані скрипти для регулярного резервного копіювання конфігурацій мережевих пристроїв.

Приклад скрипту резервного копіювання конфігурацій:

```
#!/bin/bash
# Список пристроїв
devices=("router1" "switch1" "switch2")
# Папка для збереження конфігурацій
backup_dir="/backup/network_configs"

# Поточна дата
date=$(date +%Y%m%d)

# Резервне копіювання конфігурацій
for device in "${devices[@]}"
do
    scp admin@$device:/config/running-config $backup_dir/$device-config-$date.cfg
done
```

Алгоритми пошуку та локалізації несправностей:

1. Алгоритм пошуку несправностей.

Визначення проблеми:

- отримання детального опису проблеми від користувача.
- перевірка наявності аналогічних проблем в системі моніторингу.

Перевірка фізичних з'єднань:

- огляд кабелів та роз'ємів.

– перевірка світлодіодних індикаторів на мережевих пристроях.

Перевірка конфігурацій:

– перевірка конфігураційних файлів на наявність помилок.

– відновлення з резервних копій у разі потреби.

Аналіз мережевого трафіку:

– використання інструментів для аналізу трафіку (Wireshark, tcpdump).

– виявлення аномалій та підозрілої активності.

Локалізація проблеми:

– використання команд ping, traceroute для визначення місцезнаходження проблеми.

– перевірка таблиць маршрутизації та ARP-кешу.

2. Документування вирішення проблеми:

– збереження змін конфігурацій та результатів тестів.

– запис всіх дій, що були виконані для вирішення проблеми.

Веб-сторінка з відповідями на запитання. Приклад FAQ-сторінки:

Запитання 1: Як підключитися до мережі?

Відповідь: Підключіть мережевий кабель до вашого комп'ютера та використайте надані облікові дані для входу в систему.

Запитання 2: Що робити, якщо немає підключення до Інтернету?

Відповідь: Перевірте фізичне підключення, перезавантажте маршрутизатор, якщо проблема не зникає – зверніться до технічної підтримки.

Інструкції з використання спеціалізованого програмного забезпечення для моніторингу. Приклад використання PRTG Network Monitor:

Встановлення PRTG:

Завантажте та встановіть PRTG з офіційного сайту.

Налаштування PRTG:

Додайте нові сенсори для моніторингу мережевих пристроїв.

Налаштуйте сповіщення для різних типів подій.

Моніторинг та звітність:

Переглядайте реальні дані про стан мережі через веб-інтерфейс.

Генеруйте звіти для аналізу продуктивності та виявлення проблем.

Ці інструкції забезпечують надійне та ефективне управління мережею, сприяючи стабільній та безпечній роботі мережевої інфраструктури. Правильна документація та належний моніторинг дозволяють швидко реагувати на будь-які несправності та підтримувати високу продуктивність мережі, як показано на рисунку 3.8, рисунку 3.9 та рисунку 3.10.

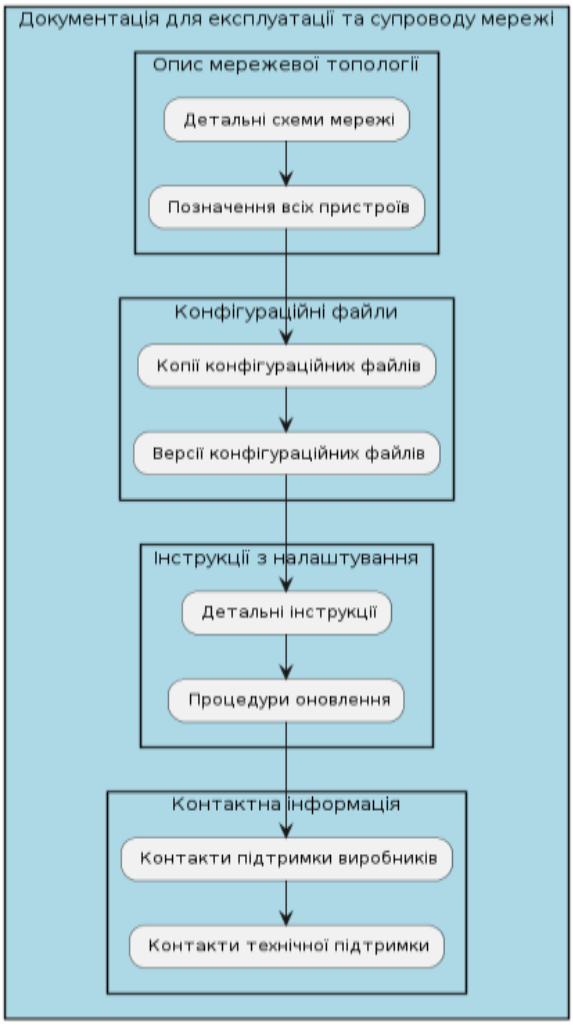

Рисунок 3.8 – Схема процедур відслідковування працездатності мережі

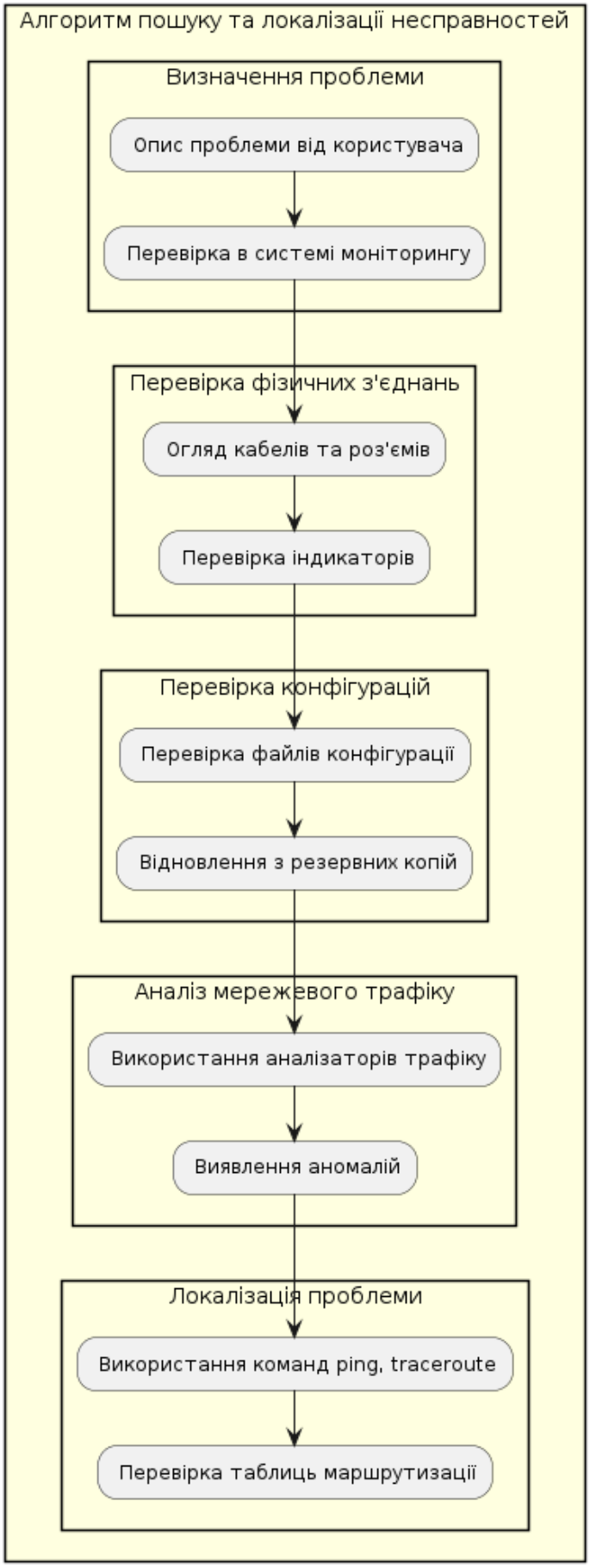

Рисунок 3.9 – Схема алгоритму пошуку та локалізації несправностей

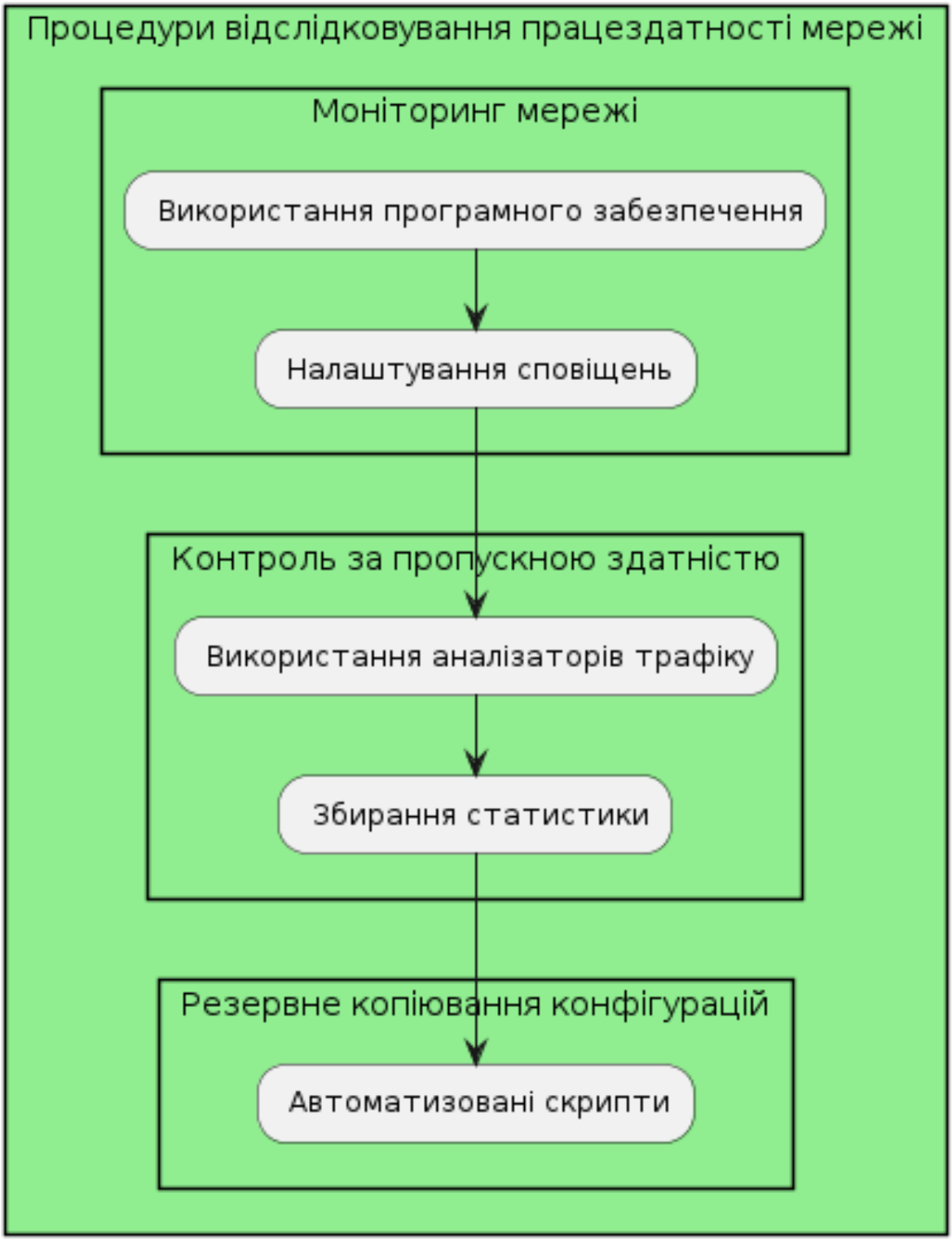

Рисунок 3.10 – Схема процедур відслідковування працездатності мережі

Процес моніторингу мережі зображено на рисунку 3.11

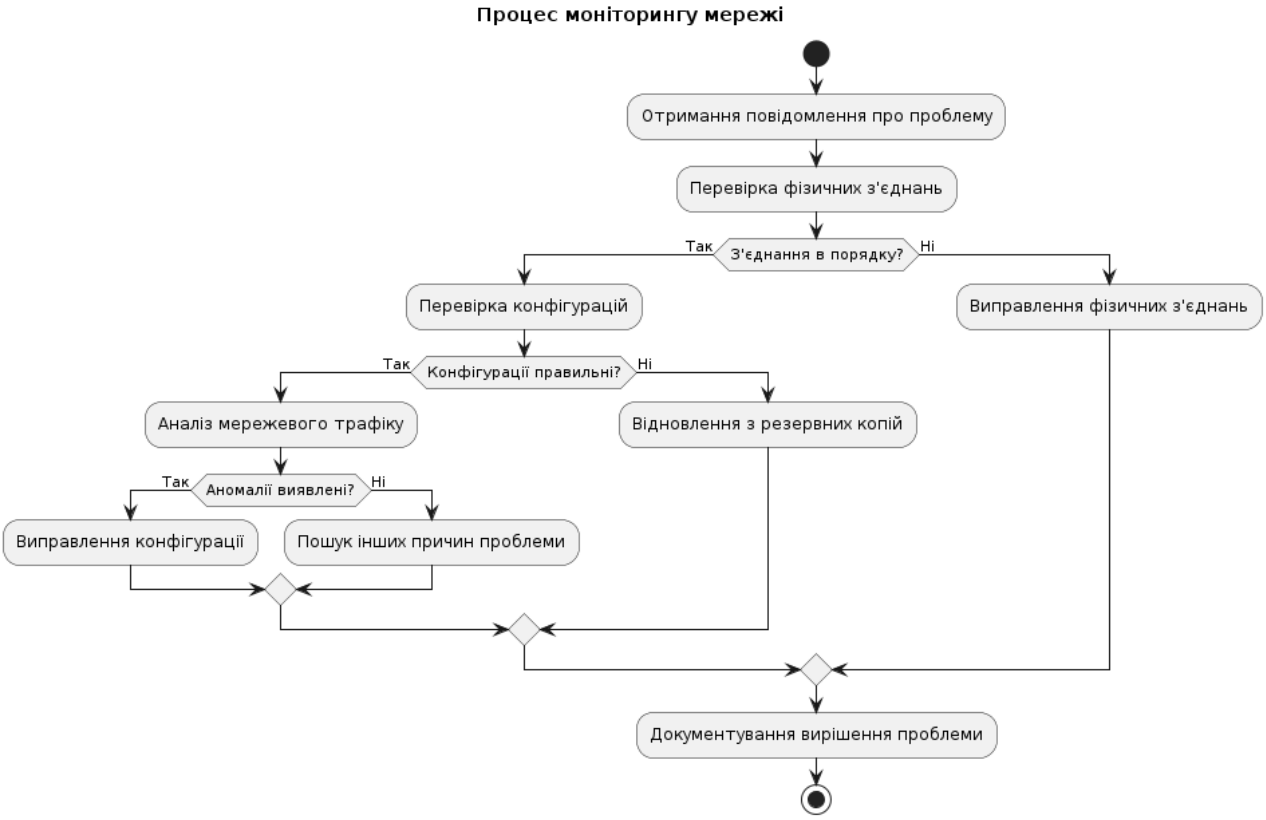

Рисунок 3.11 – Діаграма процесу моніторингу мережі

На рисунку 3.12 зображена діаграма діяльності для резервного копіювання

Рисунок 3.12 – Діаграма діяльності для резервного копіювання конфігурацій

3.6 Моделювання мережі

Розгялається моделювання мережі з використанням емулятора Packet Tracer від фірми Cisco. Основною метою моделювання є створення і тестування моделі локальної обчислювальної мережі (ЛОМ), яка відповідає вимогам проекту та забезпечує надійну роботу мережевих служб і сервісів. Основне завдання для моделювання повинно бути сформульоване таким чином, щоб охоплювати ключові аспекти проектованої мережі. Це може включати:

Налаштування комутаторів та маршрутизаторів.

- конфігурацію VLAN.
- реалізацію статичної та динамічної маршрутизації.
- забезпечення мережевої безпеки за допомогою ACL (списків контролю доступу) і файрволів.
- організацію VPN для захищеного віддаленого доступу.
- моделювання навантаження на мережу та аналіз її продуктивності.

Завдання для моделювання може виглядати так, як показано на рисунку 3.13:

Рисунок 3.13 – Схема моделювання мережі

– створити топологію мережі з двома сегментами LAN, підключеними через центральний маршрутизатор.

– налаштувати VLAN на комутаторах у кожному сегменті LAN для сегментації трафіку.

– реалізувати статичну маршрутизацію між сегментами LAN.

– налаштувати VPN на маршрутизаторі для захищеного віддаленого доступу до мережі.

– забезпечити безпеку мережі, використовуючи ACL на маршрутизаторі для обмеження доступу до критичних ресурсів.

– перевірити працездатність мережі за допомогою інструментів тестування, таких як ping та traceroute, і проаналізувати продуктивність за допомогою спеціалізованого програмного забезпечення для моніторингу. Це завдання охоплює основні аспекти проектованої мережі та дозволяє продемонструвати всі етапи її створення і налаштування.

Для моделювання мережі ми використовуємо Cisco Packet Tracer. Це безкоштовний інструмент, який дозволяє створювати віртуальні мережеві топології і На першому етапі визначається структура мережі, включаючи розміщення всіх комутаційних і маршрутизуючих пристроїв, серверів і кінцевих пристроїв (наприклад, робочих станцій).тестувати їх роботу без використання реального обладнання. Встановлюємо всі необхідні з'єднання між пристроями, враховуючи як фізичні, так і логічні аспекти мережі. Після визначення структури мережі у Cisco Packet Tracer треба приступати до налаштування параметрів кожного пристрою. Це включає встановлення IP-адрес, налаштування VLAN, статичних та динамічних маршрутів, налаштування безпеки (наприклад, списків доступу), а також конфігурування служб та сервісів, таких як DHCP, DNS, FTP, HTTP тощо. Після завершення налаштувань ми проводимо тестування мережі для перевірки її працездатності та ефективності. Ми можемо використовувати вбудовані інструменти для відлагодження мережі, такі як інструменти діагностики,

ping, traceroute тощо, а також можемо створити симуляцію робочого процесу та перевірити, як вона взаємодіє з мережею,як показано на рисунку 3.14.

Завершальним етапом є аналіз результатів тестування та виправлення будь-яких виявлених проблем. Ми можемо змінювати налаштування мережі та перевіряти їх вплив на її продуктивність та надійність. Після завершення цих кроків ми можемо зберегти нашу модель мережі для подальшого використання або представлення на захисті.

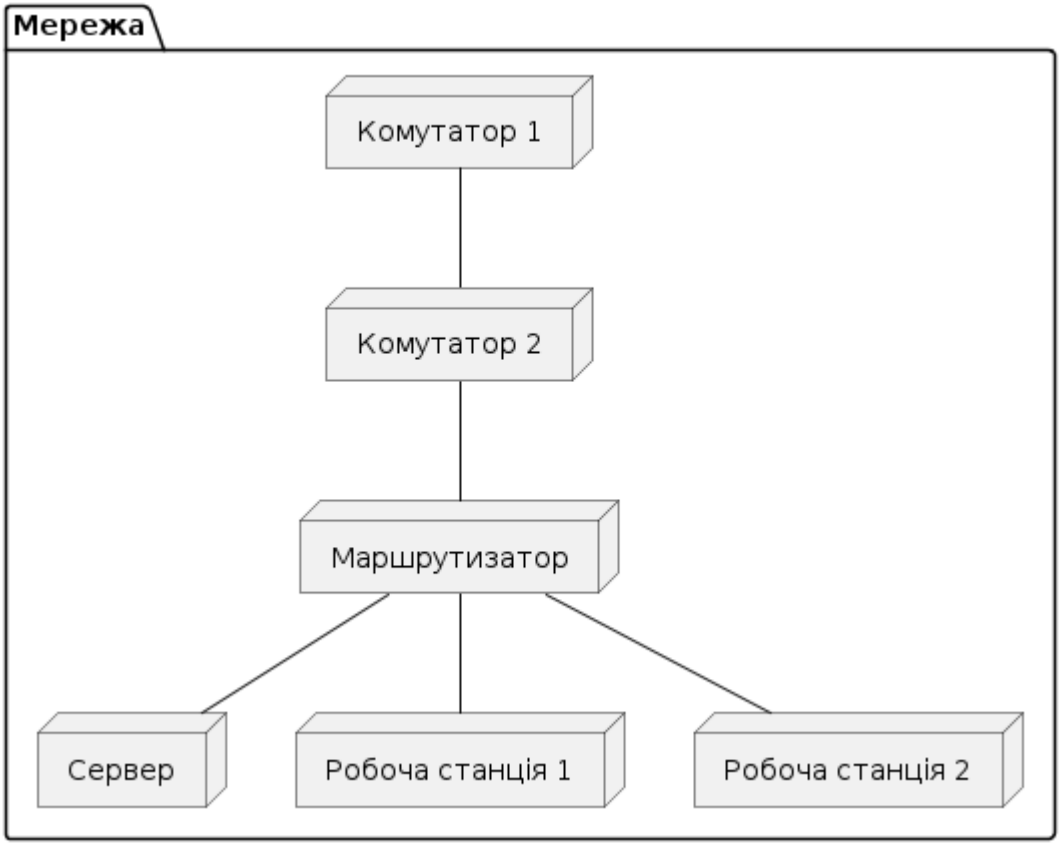

Рисунок 3.14 – Створена модель в Cisco Packet Tracer

У цьому прикладі представлені комутатори, маршрутизатор, сервер і дві робочі станції, а зв'язки між ними показані стрілками. Ви можете змінити цей код, додавши або видаляючи вузли та зв'язки, відповідно до вашої мережевої топології.

4 ЕКОНОМІЧНА ЧАСТИНА

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

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

Для розрахунку вартості НДР необхідно виконати наступні етапи:

– описати технологічний процес розробки із зазначенням трудомісткості кожної операції;

– визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;

– визначити суму матеріальних затрат;

– обчислити витрати на електроенергію для науково–виробничих цілей;

– розрахувати транспортні витрати;

– нарахувати суму амортизаційних відрахувань;

– визначити суму накладних витрат;

– скласти кошторис та визначити собівартість НДР;

– розрахувати ціну НДР;

– визначити економічну ефективність та термін окупності продукту.

4.1 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

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

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

4.2 Визначення витрат на оплату праці та відрахування на соціальні заходи

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

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

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

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

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

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 80 грн./год., лаборант – 60 грн./год.

$$З_{осн.}=80*12+50*26=2260 \text{ грн.}$$

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

$$З_{дод.}= З_{осн.}\cdot К_{допл.}, \quad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам.

$$З_{дод.}= 2260*0,15=339 \text{ грн.}$$

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

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

$$В_{о.п.}= 2260+339=2599 \text{ грн.}$$

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

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{з.п.}=ФОП \cdot 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.}= 2599*0,22=571,78 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

No п/п	Категорія прац.	Основна заробітна плата, грн			Додаткова зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрат на оплату праці, грн.
		Тариф. ставка, грн.	К–сть від–пр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	80	12	960	144	–	–
2	Лаборант	50	26	1300	195	–	–
Разом				2260	339	571,78	3170,78

Отже, загальні витрати на оплату праці становлять 9512,34грн.

4.3 Розрахунок матеріальних витрат

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

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

де q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.}=\sum M_{Bi}, \quad (4.6)$$

$З_{м.в.}$= 43144,44 грн.

Проведені розрахунки занесемо у таблиці 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1–ці, грн	Загальна сума витрат, грн.
1	Сервери	шт.	2 шт.	25000	50000
2	Комутатори	шт.	4 шт.	5000	20000
3	Маршрутизатори	шт.	1 шт.	15000	15000
4	Робочі станції	шт.	20 шт.	10000	200000
5	Кабелі та з’єднання	шт.	1 шт.	5000	5000
6	Операційні системи	шт.	22 шт.	3000	66000
7	Антивірусне ПЗ	шт.	22 шт.	1000	22000
8	Програмне забезпечення	шт.	1 шт.	10000	10000
9	Імпульсний DC-DC підвищуючи перетворювач	шт.	1 шт.	300	300
Разом			74 шт.	74300	388300

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат–години електроенергії.

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

$З_е$=0,50*22*4,32=47,52 грн.

4.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

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

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

$НА$ – норма амортизації, %.

Для проектування даної комп'ютерної системи використовується один комп'ютер (вартість якого становить 20000 грн.), який працює 22 години.

Тоді:

$$А=20000*0,04*22/150=117,33 \text{грн.}$$

4.6 Обчислення накладних витрат

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

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

$$Н_в = В_{о.п.} \cdot 0,2 \ldots 0,6 , \quad (4.9)$$

де $НВ$ – накладні витрати.

$$Н_В=2599*0,4=1039,6 \text{ грн.}$$

4.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	2599	0,66
Відрахування на соціальні виплати	571,78	0,14
Матеріальні витрати	388300	98,88
Витрати на електроенергію	47,52	0,012
Амортизаційні відрахування	117,33	0,029
Накладні витрати	1039,6	0,029
Собівартість	392675,23	100

Собівартість ($С_в$) НДР розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_е + А + Н_в \,, \quad (4.10)$$

Св=2599+571,78+388300+47,52+117,33+1039,6=392675,23 грн.

4.8 Розрахунок ціни НДР

Ціну *НДР* можна визначити за формулою:

$$Ц = \frac{С_в(1+Р_{рвн})\cdot К + В_{н.і}}{К} \cdot (1+ПДВ) \,, \quad (4.11)$$

де $Р_{рен.}$ – рівень рентабельності;
$К$ – кількість замовлень, од.;

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

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

$Ц$=392675,23*1,3*1,2=612573,35 грн.

4.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

$$П = 612573,35 - 392675,23 = 219898,12 \text{ грн.}$$

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

$$Е_р = П / С_в, \quad (4.14)$$

де П – прибуток;

$С_в$ – собівартість.

$$Е_р = 219898,12 / 392675,23 = 0,56$$

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

$$Т_р = 1 / Е_р \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

$$Т_р=1/0,56=1,78$$

Таблиця 4.5 - Економічні показники НДР

№	Показник	Значення
1.	Собівартість, грн.	392675,23
2.	Плановий прибуток, грн.	219898,12
3.	Ціна, грн.	612573,35
4.	Термін окупності, рік	1,78

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

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Навчання з питань пожежної безпеки

З метою запобігання виникненню пожеж, їх поширенню та для боротьби з ними працівники проходять інструктажі й навчання за спеціальними програмами. Організація своєчасного і якісного проведення навчання, інструктажів та перевірки знань із питань пожежної безпеки в організаціях покладається на їх керівників, а в структурних підрозділах – на керівника відповідного підрозділу. Навчання з питань пожежної безпеки є обов'язковим і здійснюється в робочий час за програмами з питань пожежної безпеки, які погоджуються з центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту, а також під час проведення спеціальних об'єктових навчань і тренувань з питань цивільного захисту.

З урахуванням пожежної небезпеки наказом керівника (інструкцією) встановлюється відповідний порядок проходження посадовими особами навчання й перевірки знань із питань пожежної безпеки, а також проведення з працівниками протипожежних інструктажів та занять із пожежно-технічного мінімуму з призначенням відповідальних за їхнє проведення.

Кодексом цивільного захисту України передбачено такі види протипожежних інструктажів: вступний; первинний та повторний на робочому місці, а також може бути позаплановий та цільовий інструктаж. За призначенням та часом проведення протипожежні інструктажі поділяють на вступний, первинний.

Вступний протипожежний інструктаж проводиться з усіма працівниками, які щойно прийняті на роботу (постійну або тимчасову), а також з особами, які прибули на підприємство у відрядження і мають брати безпосередню участь у трудовому процесі. При проведенні цього

інструктажу працівників знайомлять з основними вимогами Кодексу цивільного захисту України, з установленим на підприємстві протипожежним режимом, з найбільш пожежонебезпечними ділянками, де забороняється палити, використовувати відкритий вогонь, з практичними діями на випадок виникнення пожежі, з можливими причинами виникнення пожеж і вибухів та заходами щодо їх запобігання. Він проводиться, як правило, у спеціально обладнаному для цього приміщенні фахівцем, на якого наказом покладені ці обов'язки. Вступний інструктаж може поєднуватися зі вступним інструктажем з охорони праці. Програма для проведення вступного протипожежного інструктажу затверджується керівником або його заступником.

Первинний протипожежний інструктаж новоприйнятий працівник проходить на робочому місці перед початком роботи, а також при переміщенні з одного підрозділу до іншого, на іншу посаду. Цей інструктаж також проходять особи, які прибули на підприємство у відрядження і мають брати безпосередню участь у трудовому процесі. Під час первинного інструктажу: знайомлять з пожежною безпекою приміщення, з правилами та інструкціями з пожежної безпеки; показують запасні виходи, пожежну сигналізацію, вогнегасники, засоби пожежогасіння; перевіряють практичні дії особи, що інструктується на випадок пожежі.

Повторний протипожежний інструктаж проводиться на робочому місці з усіма працівниками не менш як один раз на рік за визначеним переліком питань, з якими необхідно ознайомити працівників під час проведення вступного та первинного протипожежних інструктажів.

Позаплановий протипожежний інструктаж повинен проводитися на робочому місці або у спеціально відведеному для цього приміщенні у разі введення в дію нових нормативних актів з питань пожежної безпеки (норм, правил, інструкцій, положень тощо) чи змін та доповнень до них або ж на вимогу державних інспекторів з пожежного нагляду, якщо виявлено незадовільне знання працівниками правил пожежної безпеки на робочому

місці, невміння діяти у випадку пожежі та користуватися первинними засобами пожежогасіння.

Обсяг та зміст інструктажу визначаються в кожному випадку окремо залежно від причин, що спричинили необхідність його проведення.

Первинний, повторний, позаплановий та цільовий протипожежні інструктажі проводяться безпосередньо керівниками робіт, які пройшли навчання і перевірку знань із питань пожежної безпеки.

Цільовий протипожежний інструктаж проводиться із працівниками у разі ліквідації аварії, стихійного лиха; при проведенні робіт, на які відповідно до законодавства оформлюються наряд-допуск, наказ або розпорядження.

Цільовий інструктаж проводиться індивідуально з окремим працівником або з групою працівників. Обсяг і зміст цільового інструктажу визначаються залежно від виду робіт, що виконуватимуться.

Особи, яких приймають на роботу, пов’язану з підвищеною пожежною небезпекою, повинні попередньо пройти спеціальне навчання (пожежно-технічний мінімум). Вони один раз на рік проходять перевірку знань відповідних нормативних актів з пожежної безпеки, а посадові особи до початку виконання своїх обов’язків і періодично (один раз на три роки) проходять навчання і перевірку знань з питань пожежної безпеки.

Про проведення всіх видів протипожежних інструктажів, крім цільового, у спеціальних журналах робляться записи (окремо від інструктажів з питань охорони праці) з підписами осіб, з якими проводився інструктаж, і тих, хто його проводив.

Первинний, повторний та позаплановий інструктажі завершуються перевіркою знань. Перевірку здійснює особа, яка проводила інструктаж.

Допуск до роботи осіб, які не пройшли навчання, інструктаж і перевірку знань з питань пожежної безпеки, забороняється.

Навчання та перевірку знань з питань пожежної безпеки до початку виконання своїх обов'язків і періодично (один раз на три роки) проходять посадові особи. Відповідно до переліку посад, при призначенні на які особи

зобов'язані проходити навчання і перевірку знань з питань пожежної безпеки, у міністерствах, інших центральних органах виконавчої влади, концернах, корпораціях, об'єднаннях підприємств, на підприємствах, в установах та організаціях складаються і затверджуються керівництвом конкретні переліки посад, під час призначення на які особи зобов'язані проходити навчання і перевірку знань з пожежної безпеки, із зазначенням відповідних термінів. Навчання і перевірку знань з питань пожежної безпеки можуть проводити тільки фахівці, що мають спеціальну (пожежнотехнічну) освіту та стаж роботи за фахом не менше 5 років.

Після закінчення навчання особам, які успішно склали залік, видається посвідчення. Особи, які показали незадовільні знання, повинні протягом одного місяця пройти повторну перевірку знань із пожежної безпеки.

Позачергова перевірка знань посадових осіб із питань пожежної безпеки за рішенням керівника підприємства проводиться: при введенні в дію нових нормативних актів з пожежної безпеки; при переміщенні посадової особи на іншу посаду, яка потребує додаткових знань із пожежної безпеки; на вимогу органів державного пожежного нагляду, якщо встановлено факти необізнаності посадової особи з нормативними актами з питань пожежної безпеки [7, с. 213-216].

5.2 Розрахунок системи штучного освітлення інформаційно-технічного відділу

Розрахунок освітлення робочих місць проведемо для інформаційно-технічного відділу. Розрахунок виконаємо згідно методики [8].

Штучне освітлення приміщення з робочими місцями, обладнаними відеотерміналами ЕОМ загального та персонального користування, мас бути обладнане системою загального рівномірного освітлення. У виробничих та адміністративно-громадських приміщеннях, де переважають роботи з документами, допускається вживати систему комбінованого освітлення

(додатково до загального освітлення встановлюються світильники місцевого освітлення).

Загальне освітлення має бути виконане у вигляді суцільних або переривчастих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників.

Як джерело світла при штучному освітленні повинні застосовуватися, як правило, люмінесцентні лампи типу ЛБ. При обладнанні відбивного освітлення у виробничих та адміністративно-громадських приміщеннях можуть застосовуватися металогалогенові лампи потужністю до 250 Вт. Допускається у світильниках місцевого освітлення застосовувати лампи розжарювання.

Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 град до 90 град відносно вертикалі в подовжній і поперечній площинах повинна складати не більше 200 кд/м^2, а захисний кут світильників повинен бути не більшим за 40 град.

Розраховуємо систему загального рівномірного освітлення люмінесцентними лампами для виробничого приміщення, в якому виконуються зорові роботи високої точності ($II_В$), мінімальне освітлення якого становить Е = 300лм. Як світлові пристрої приймаємо світильники типу ЛПО01 (з двома лампами).

Розміри приміщення інформаційно-технічного відділу, де встановлено серверну шафу з мережевим обладнанням і серверами: довжина а = 5,5м. (прийнята усереднено для спрощення розрахунків), ширина b = 5 м, висота Н = 3 м. Приміщення має такі показники: коефіцієнт відбиття $\rho_{стелі}$= 70 %, $\rho_{стін}$= 50%.

Висота робочих поверхонь (столів) $h_р$ = 0,7 м. Оскільки світильники кріпляться до стелі, то їх висота над підлогою майже рівна висоті приміщення h_0 = 3 м, що не суперечить вимогам СНиП 11-4-79, відповідно до яких $h_{0\,min}$ = 2,6 - 4 м.

Визначимо висоту світильника над робочою поверхнею:

$$h = h_0 - h = 3 - 0,7 = 2,3\ м \tag{5.1}$$

Показник приміщення *i* становить:

$$i = \frac{ab}{h(a+b)} = \frac{5,5 \cdot 5}{2,3(5,5+5)} = 1.14 \tag{5.4}$$

При *i* = 1,10 (*i* =1,14 немає), $\rho_{стелі}$= 70 %, $\rho_{стін}$= 50% для світильника ЛПО01 коефіцієнт використання дорівнює η =48%. Ці дані отримано з таблиці 5.2. [8]

Визначимо необхідну кількість світильників, для забезпечення необхідної нормованої освітленості робочих поверхонь, якщо відомо, що в кожному світильнику встановлено по дві лампи ЛБ-40, а світловий потік однієї такої лампи становить $Ф_Л$ = 3200 лм:

$$N = \frac{ESKZ}{2Ф_Л\eta} = \frac{300 \cdot 27,5 \cdot 1,5 \cdot 1,14}{2 \cdot 3200 \cdot 0,48} = 4.6 \tag{5.5}$$

Приймаємо 6 світильників, які для забезпечення рівномірності освітлення розташовуємо в 2 ряди, симетрично до стін. Оскільки довжина світильника становить 1м., то між ним будуть рівномірні проміжки. Розміщення світильників наведено на рисунку 5.1

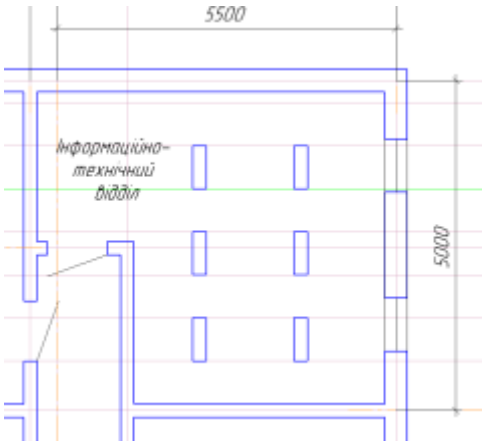

Рисунок 5.1 - Схема розміщення світильників в інформаційно-технічному відділі

ВИСНОВОК

Дана кваліфікаційна робота бакалавра успішно виконана згідно поставлених завдань.

Проектування та впровадження локальної обчислювальної мережі на підприємстві дозволило створити надійну та ефективну інфраструктуру для підтримки різноманітних бізнес-процесів. Вибрані апаратні та програмні засоби забезпечують високу продуктивність, безпеку та масштабованість мережі. Проведені економічні розрахунки підтвердили доцільність впровадження проекту з точки зору витрат та очікуваної користі. Ретельний підхід до налаштування та захисту мережі гарантує її стабільну роботу та захист від несанкціонованого доступу. Виконані тестування підтвердили відповідність мережі технічним та функціональним вимогам. В цілому, дипломний проект успішно реалізував поставлені задачі, створивши надійну та ефективну мережеву інфраструктуру, яка відповідає потребам підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Мащакевич О. М., Шикова О. М. Інформатика та комп’ютерна техніка: посібник для молодших спеціалістів. Київ: МАУП, 2007, 356 с.
2. Cisco Systems, Inc. "Cisco Packet Tracer." [Online]. Available: https://www.netacad.com/courses/packet-tracer. [Accessed: June 1, 2024].
3. Stallings, W. "Data and Computer Communications." 10th Edition. - Pearson, 2013. - 888 p.
4. Microsoft Corporation. "Windows Server Documentation." [Online]. Available: https://docs.microsoft.com/en-us/windows-server/. [Accessed: June 3, 2024].
5. Stevens, W. R. "TCP/IP Illustrated, Volume 1: The Protocols." - Addison-Wesley, 1994. - 675 p.
6. RFC 4301. "Security Architecture for the Internet Protocol." [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4301. [Accessed: June 4, 2024].
7. ISO/IEC 27001:2013. "Information technology — Security techniques — Information security management systems — Requirements." [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed: June 5, 2024].
8. Comer, D. "Internetworking with TCP/IP Volume One." - Prentice Hall, 2006. - 864 p.
9. RFC 791. "Internet Protocol." [Online]. Available: https://datatracker.ietf.org/doc/html/rfc791. [Accessed: June 6, 2024].
10. Cisco Systems, Inc. "Cisco IOS Security Configuration Guide." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-4/security-configuration-guide-15-4.html. [Accessed: June 7, 2024].
11. ISO/IEC 11801:2017. "Information technology — Generic cabling for customer premises." [Online]. Available: https://www.iso.org/standard/66182.html. [Accessed: June 8, 2024].
12. Pfleeger, C. P., Pfleeger, S. L., and Margulies, J. "Security in Computing." 5th Edition. - Prentice Hall, 2015. - 944 p.
13. RFC 5246. "The Transport Layer Security (TLS) Protocol Version 1.2." [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5246. [Accessed: June 9, 2024].

14. ISO/IEC 20000-1:2018. "Information technology — Service management — Part 1: Service management system requirements." [Online]. Available: https://www.iso.org/standard/70636.html. [Accessed: June 10, 2024].
15. Pfleeger, C. P. "Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach." - Pearson, 2012. - 800 p.
16. Tanenbaum, A. S., and Wetherall, D. "Computer Networks." 5th Edition. - Pearson, 2011. - 960 p.
17. Oracle Corporation. "Oracle Database Documentation." [Online]. Available: https://docs.oracle.com/en/database/. [Accessed: June 13, 2024].
18. RFC 2865. "Remote Authentication Dial In User Service (RADIUS)." [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2865. [Accessed: June 12, 2024].
19. Forouzan, B. A. "Data Communications and Networking." 5th Edition. - McGraw-Hill, 2012. - 1264 p.
20. Fortinet, Inc. "FortiGate Security Documentation." [Online]. Available: https://docs.fortinet.com/. [Accessed: June 14, 2024].

ДОДАТКИ

Додаток А. План розташування обладнання в головному комутаційному вузлі

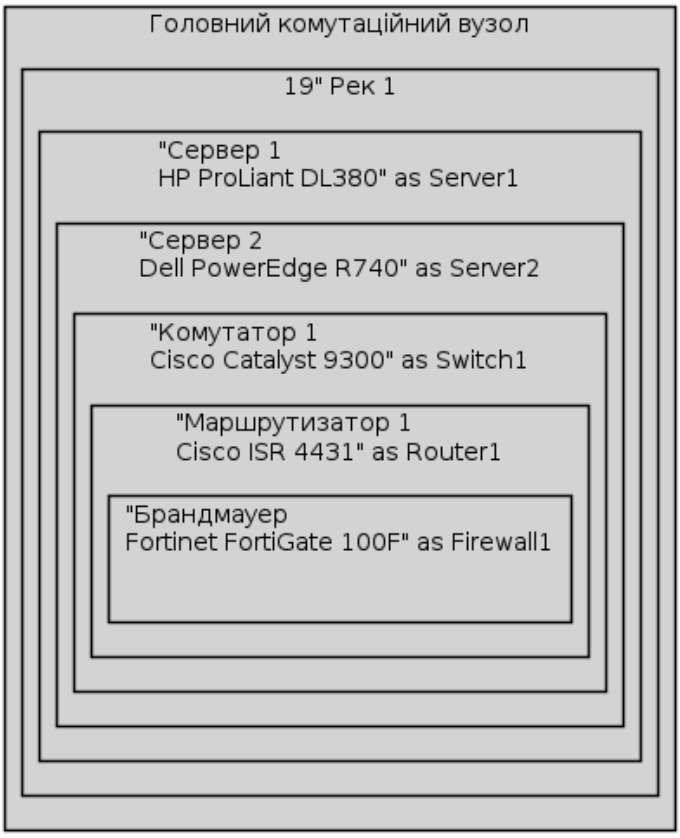

Рисунок 6.1 – План розташування обладнання

Опис компонентів:

- Сервери:
  - HP ProLiant DL380. Основний сервер для обробки даних.
  - Dell PowerEdge R740. Сервер для резервного копіювання і відновлення.
  - Lenovo ThinkSystem SR650. Сервер для баз даних.
  - IBM System x3650 M5. Сервер для додатків.
- Комутатори:
  - Cisco Catalyst 9300. Використовується для внутрішньої комутації між пристроями.
- Маршрутизатори:
  - Cisco ISR 4431. Забезпечують маршрутизацію трафіку між мережами.
- Брандмауери:
  - Fortinet FortiGate 100F. Захищають мережу від несанкціонованого доступу.
- Шафа для кабелів:

- Патч-панелі. Організація кабельних з'єднань між обладнанням.
-

Додаток Б. Характеристики активного комутаційного обладнання мережі

Маршрутизатори

Cisco ISR 4431

Процесор: 4-ядерний процесор з тактовою частотою 2.5 ГГц

Оперативна пам'ять: 8 ГБ DDR4

Порти: 3 Gigabit Ethernet (RJ-45), 2 SFP (Small Form-factor Pluggable)

Пропускна здатність: 1 Гбіт/с

Безпека: Підтримка IPsec VPN, інспекція пакетів, шифрування AES

Мережеві протоколи: OSPF, BGP, EIGRP, RIP

Інтерфейси управління: CLI, GUI (Cisco ASDM), SNMP

Комутатори

Cisco Catalyst 9300

Процесор: UADP 2.0 ASIC

Оперативна пам'ять: 8 ГБ DRAM

Флеш-пам'ять: 16 ГБ

Порти: 24/48 портів Gigabit Ethernet (RJ-45), 4 порти 10 Gigabit Ethernet (SFP+)

Пропускна здатність: До 480 Гбіт/с

VLAN: Підтримка до 1024 VLAN

Безпека: 802.1X, порт-базований контроль доступу, захист від DoS-атак

Мережеві функції: Stacking, QoS, LACP, VRF, MSTP

Інтерфейси управління: CLI, WebUI, SNMP, NetFlow

Брандмауери

Fortinet FortiGate 100F

Процесор: 2-ядерний процесор з підтримкою Content Processor (CP9)

Оперативна пам'ять: 4 ГБ

Флеш-пам'ять: 64 ГБ

Порти: 10 портів Gigabit Ethernet (RJ-45), 2 порти 10 Gigabit Ethernet (SFP+)

Пропускна здатність: Firewall throughput до 20 Гбіт/с, VPN throughput до 1.4 Гбіт/с

Безпека: Application Control, IPS, Antivirus, SSL Inspection

Віртуалізація: Підтримка VDOMs

Мережеві протоколи: Static, RIP, OSPF, BGP

Інтерфейси управління: CLI, WebUI, FortiManager

Додаток В. Характеристики серверів

HP ProLiant DL380
Процесор: 2 x Intel Xeon Scalable
Оперативна пам'ять: 32 ГБ DDR4 (розширюється до 3 ТБ)
Сховище: 8 x 2.5" SAS/SATA, підтримка до 12 NVMe SSD
Мережеві інтерфейси: 4 x 1GBASE-T, підтримка 10GbE через PCIe
Інтерфейси управління: iLO (Integrated Lights-Out), CLI, GUI

Dell PowerEdge R740
Процесор: 2 x Intel Xeon Scalable
Оперативна пам'ять: 64 ГБ DDR4 (розширюється до 3 ТБ)
Сховище: 8 x 2.5" SAS/SATA, підтримка до 12 NVMe SSD
Мережеві інтерфейси: 4 x 1GBASE-T, підтримка 10GbE через PCIe
Інтерфейси управління: iDRAC9, CLI, GUI

Lenovo ThinkSystem SR650

Процесор: 2 x Intel Xeon Scalable
Оперативна пам'ять: 64 ГБ DDR4 (розширюється до 3 ТБ)
Сховище: 8 x 2.5" SAS/SATA, підтримка до 16 NVMe SSD
Мережеві інтерфейси: 4 x 1GBASE-T, підтримка 10GbE через PCIe
Інтерфейси управління: XClarity Controller, CLI, GUI

IBM System x3650 M5
Процесор: 2 x Intel Xeon E5-2600 v4
Оперативна пам'ять: 64 ГБ DDR4 (розширюється до 1.5 ТБ)
Сховище: 8 x 2.5" SAS/SATA, підтримка до 12 NVMe SSD
Мережеві інтерфейси: 4 x 1GBASE-T, підтримка 10GbE через PCIe
Інтерфейси управління: IMM2 (Integrated Management Module), CLI, GUI

Додаток Г. Тексти для програмування активного комутаційного обладнання, серверні скріпти

Аудит безпеки та журналювання

```
Example Logrotate Configuration:
# Create a custom logrotate configuration file
sudo nano /etc/logrotate.d/custom_logs

# Add the following content:
/var/log/syslog {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 0640 syslog adm
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}

/var/log/auth.log {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 0640 syslog adm
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
```

```
    endscript
}

Example Auditd Configuration:
# Install auditd
sudo apt-get install auditd

# Edit the audit rules file
sudo nano /etc/audit/rules.d/audit.rules

# Add the following rules to monitor system calls and files:
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /var/log/auth.log -p wa -k auth_log
-a always,exit -F arch=b64 -S execve -k exec

# Restart auditd to apply the rules
sudo systemctl restart auditd



Example OSSEC Installation:
# Download and install OSSEC
wget https://github.com/ossec/ossec-hids/archive/refs/tags/3.6.0.tar.gz
tar -xvzf 3.6.0.tar.gz
cd ossec-hids-3.6.0
sudo ./install.sh

# Follow the on-screen instructions to complete the installation

# Start OSSEC service
sudo /var/ossec/bin/ossec-control start
```