Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Рабченюка Валентина Руслановича

на здобуття ступеня вищої освіти Бакалавра

Комп'ютерна мережа наукової бібліотеки ХНУ

Галузь знань 12 – Інформаційні технології
Спеціальність 123 – Комп'ютерна інженерія
Освітня програма Програмування та захист комп`ютерних систем і мереж

Шифр КРБКІ. 2101006.21.01.06 ПЗ

Виконав студент 3 курсу група КІ1с-21-1 Валентин РАБЧЕНЮК
Керівник канд. техн. наук, доцент Вікторія ОРЛЕНКО
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

19 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

Освітня програма Програмування та захист комп`ютерних систем і мереж

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рабченюку Валентину Руслановичу

1 Комп'ютерна мережа наукової бібліотеки ХНУ

Керівник роботи к.т.н. доцент Вікторія ОРЛЕНКО

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи Розробити логічну та фізичну топології мережі. В логічній топології передбачити розподіл мережі на підмережі. Вибрати обладнання налаштувати обладнання (пристрої безпеки, комутатори, маршрутизатори, кінцеві пристрої) для забезпечення проходження дозволеного та блокування забороненого трафіку.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Дослідити предметну область, проаналізувати отриману теоретичну інформацію, спроектувати та змоделювати комп'ютерну мережу згідно технічного завдання, розрахувати вартість та характеристики компонентів.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Логічна топологія мережі. Фізична топологія мережі.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Валентин РАБЧЕНЮК

Керівник кваліфікаційної роботи Вікторія ОРЛЕНКО

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Комп'ютерна мережа наукової бібліотеки ХНУ»

Автор роботи: студент групи КІ1с–21–1 Рабченюк В. Р.

Керівник роботи: к.т.н. доц. Орленко В.С.

Пояснювальна записка: 64с., 15 рисунків, 6 таблиць, 50 джерел, 3 креслення.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: комп'ютерна мережа, наукова бібліотека, топологія мережі, безпека, VLAN.

У кваліфікаційній роботі розроблено проект комп'ютерної мережі для наукової бібліотеки ХНУ. Було проведено аналіз потреб та вимог до мережі, зокрема доступності, швидкодії, безпеки та масштабованості. Проаналізовано сучасні мережеві архітектури та обрано оптимальний підхід для впровадження.

Запропоновано структуру мережі, що базується на топології "зірка" з використанням VLAN для розмежування доступу. Розроблено детальні схеми налаштування мережевого обладнання, зокрема маршрутизаторів, комутаторів та точок доступу Wi-Fi. Проведено тестування мережі для забезпечення відповідності функціональним вимогам.

19.06.2024

ABSTRACT

Course project: «Computer Network of the Scientific Library of KhNU»

Author of the work: Rabchenyuk V. R.

Supervisor: Viktoria Orlenko

Amount: 64 p., 15 figures, 6 tables, 50 sources, 3 drawings.

KEYWORDS: computer network, scientific library, network topology, security, VLAN.

The qualification work involves the development of a computer network project for the scientific library of KhNU. An analysis of the needs and requirements for the network was carried out, focusing on accessibility, performance, security, and scalability. Modern network architectures were analyzed, and the optimal approach for implementation was chosen.

The structure of the network based on a star topology with VLAN segmentation for access control is proposed. Detailed configuration schemes for network equipment, including routers, switches, and Wi-Fi access points, were developed. The network was tested to ensure compliance with functional requirements.

19.06.2024

ЗМІСТ

Зм.	Арк.	№докум.	Підпис	Дата	КРБКІ. 2101006.21.01.06 ПЗ		
Виконав		РабченюкВ.Р.			Комп'ютерна мережа наукової бібліотеки ХНУ Пояснювальна записка	Літера	Аркуш 2 / Аркушів 64
Перевір.		Орленко В.С.					
Н.контр.		Мостовий С.В.				ХНУ, КІ1с-21-1	
Затвер.		Кльоц Ю.П.					

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

CISCO OSI – Еталонна модель взаємодії комп’ютерних мереж

Cisco PT- Cisco Packet Tracer

DMZ – демілітаризована зона

HTTP – Протокол передачі гіпертексту

IEEE – Міжнародна організація інженерів електротехніки

IP – Internet Protocol

LAN – локальна мережа

MAC – Media Access Control

NAP – Network Access Point

NAT – перетворення мережевих адрес

SSH – мережевий протокол рівня застосунків

WAN – глобальна мережа

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп`ютер

ВСТУП

На сьогоднішній день важко уявити людську професію, та її діяльність у сфері, яка б не вимагала використання комп'ютерних мереж. Наукові, освітні установи, сфери які займаються торгівлею, та фінансами, усі ці та решта інших підприємств потребують для працездатності своєї діяльності захищеної та швидкої комп'ютерної мережі. В свою чергу, комп'ютерна мережа, є досить складною складовою, незважаючи на те, чи локальна ця мережа, чи приватна. Розробниками мережних пристроїв та програмного забезпечення було прикладено багато зусиль, щоб робота в мережі не викликала труднощів, а налаштування було інтуїтивно зрозумілим навіть для людини, яка не працювала тісно з комп'ютерною мережею, тобто рівень його підготовки вважається низьким. Але, якщо розглянути технічну документацію про роботу комп'ютерної мережі, можна переконатися, що у мережі відбувається безліч досить складних процесів, для того щоб мережа працювала справно, та без збоїв. Звідси слідує висновок, що реалізація та технічна підтримка комп'ютерної мережі вимагає спеціальних технічних знань та практичних навичок у галузі комп'ютерних мереж. Під час виконання бакалаврської роботи було здобуто знання та необхідні навички, які потребувались для бездоганного виконання завданння. Але ситуація ускладнюється через існування дуже широкого асортименту мережевого обладнання та різних мережевих протоколів, внаслідок цього мережеві технології модифікуються та оновлюють надзвичайно швидко. Майже кожного дня можна побачити статтю чи доповідь про те, що з'явились нові мережеві пристрої з кращими характеристиками, аніж були у попередніх їхніх версій, або про розширення здатностей мережевих протоколів. Також від них не відстає і програмне забезпечення, яке направлене на аналіз комп'ютерної мережі, та відслідковування передачі даних та пакетів у локальній мережі, та поза її межами. Декілька комп'ютерів комутують в локальну комп'ютерну мережу для того, щоб була можливість передачі певних ресурсів, до яких відносяться такі як:

-Ресурси(пакети даних);

-Сервіси;

-Певні послуги;

-Програмне забезпечення;

-Тощо;

Локальна мережа, така як домашня, мережа офісів, або шкіл є основною складовою глобальних мереж, наприклад як Інтернет. У ході написання бакалаврської роботи та виконання поставленного завдання було розглянуто архітектуру комп'ютерних мереж. Це дало можливість проаналізувати та дослідити основні принципи реалізації комп'ютерних мереж. Внаслідок цього стало можливим підійти до вирішення проблеми з більш кваліфікованим рівнем проектування та адміністрування комп’ютерної мережі. Далі, у виконанні завдання бакалаврської роботи буде використано еталонну модель відкритих систем Cisco OSI, та стек протоколів TCP/IP, який через свою використовуваність прийнятих як базовий у всіх комп'ютерних мережах. Також при виконанні завдання було отримано глибокі знання у галузі базових принципів технологій збору інформації та управлінням даних, способів їхнього функціонування на аппаратному рівні, що в подальшому виконанні є вкрай необхідним. У розділі №3 було розглянуто адресацію комп'ютерної мережі, було розглянуто зокрема IP, та MAC адресації. При реалізації комп’ютерної мережі організації було реалізовано розбивання мережі на окремі під мережі, які передбачають використання утиліт та програмного забезпечення TCP/IP. Не менш важливим аспектом є адміністрування мережі, яке передбачає реалізацію нового користувацького облікового запису, або створення групп користувачів. Невід'ємною складовою аналізу комп'ютерної мережі та її дослідження стало використання аналізатора трафіку. При виконанні лабораторних робіт було використано таку програму, як WireShark, її ми і будемо використовувати у ході виконання поставленого завдання на бакалаврську роботу. Ця програма аналізує перехоплені кадри, та видає усі інформацію про протоколи, які через неї проходять, та дає можливість розібрати кадр, який був перехоплений. У

реалізації мережі використовувались такі технології як Internet(Ethernet) та Wi-Fi. За основу було взято пакети протоколів IPv4 та IPv6, а також блоки протоколів TCP/UDP.

Актуальність теми роботи. Комп'ютерні мережі є основною складовою для реалізації інформаційних систем. Вони роблять можливим передачу даних та комутацію між хостами підприємства, та управління правом доступу до ресурсів з інформацією. З точки зору збору інформації є проектування інформаційних систем, які б могли втілити надійність та захищеність процесів транспортування даних, як у межах підприємства, так і за її межами, а також для зберігання та керування ними. Отже, комп'ютерні мережі є досить важливою частиною проектування інформаційної системи, оскільки вони уможливлюють підвищення ефективності та швидкодії прийняття рішень за рахунок швидкої обробки даних, даючи при цьому можливість конкурувати бізнес процесами та бізнес системами в цілому. Але при модернізації та проєктуванні комп'ютерних мереж неохідно враховувати певні вимоги, які б допомогли більш ефективно відображати реальні бізнес процеси організації на логічні або віртуальні. Одною з найважливіших характеристик комп'ютерних мереж є її архітектура, фізична та віртуальна топології, тип обладнання, яке було використане, методи захисту та підвищення надійності.

Отже, актуальним завданням є аналіз та дослідження методів забезпечення надійності та захисту комп'ютерної мережі. При реалізації способів підвищення захищенності комп'ютерної мережі слід врахувати вимоги для забезпечення надійної роботи апаратних ПЗ, їх швидкодії, фізичного та логічного захисту обладнання та даних. Але, хоча винайдені методи дають можливість реалізовувати оптимальні варіанти розв'язку задачі забезпечення надійності та захисту комп'ютерних мереж, але вони містять і свої мінуси.

Частково це стосується локальних мереж, які мають свої певні критерії надійності та захисту. З цього випливає, що актуальною задачею реалізації комп'ютерної мережі є задача забезпечення захисту та надійності мережі, а також апаратних та програмної складових.

1 ОСНОВНІ ПОНЯТТЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ЇЇ ХАРАКТЕРИСТИКИ

1.1 Аналіз потреб і вимог до комп'ютерної мережі в науковій бібліотеці

Розробка комп'ютерної мережі для наукової бібліотеки є важливим завданням, що потребує глибокого аналізу функціональних потреб та технічних вимог. Врахування специфіки роботи бібліотеки дозволяє оптимізувати проєктування мережевої інфраструктури, забезпечуючи зручний доступ до інформаційних ресурсів та послуг.

До ключових вимог належать:

- Доступність і надійність мережі. Мережа має функціонувати стабільно протягом усього робочого часу бібліотеки, забезпечуючи безперебійний доступ до електронних ресурсів, каталогів, баз даних та інших цифрових сервісів.

- Швидкість і пропускна здатність. Забезпечення високої швидкості передачі даних є необхідним для роботи з великими обсягами інформації, мультимедійними матеріалами та онлайн-платформами.

- Захист інформації. Безпека мережі повинна охоплювати захист від кібератак, несанкціонованого доступу та збереження конфіденційності даних користувачів і персоналу.

- Відповідність законодавчим нормам. Інфраструктура мережі повинна відповідати вимогам регіонального та національного законодавства, включаючи захист персональних даних, дотримання авторських прав і забезпечення безпечного використання ресурсів.

- Ефективне управління мережею. Мережа має включати інструменти для централізованого управління, моніторингу продуктивності, резервного копіювання даних і вирішення технічних проблем.

- Гнучкість і масштабованість. Інфраструктура повинна підтримувати розширені можливості, такі як організація відеоконференцій, доступ до електронних архівів і інтеграція з іншими інформаційними системами.

- Раціональність витрат. Проєкт мережі повинен відповідати фінансовим можливостям бібліотеки, забезпечуючи оптимальний баланс між вартістю та функціональністю.

При проєктуванні мережі для наукової бібліотеки важливо враховувати:

- Кількість користувачів, включно з персоналом, дослідниками та відвідувачами.

- Структуру доступу, яка може включати групи з різними рівнями прав.

- Обсяги та характер трафіку, а також вимоги до його пріоритезації (наприклад, для роботи з базами даних або мультимедійними матеріалами).

- Типи підключення (стаціонарне чи бездротове).

- Розміщення вузлів мережі та обладнання відповідно до розташування бібліотечних зон і площі покриття.

Застосування комплексного підходу до аналізу та реалізації цих потреб дозволяє створити сучасну, безпечну та ефективну мережеву систему, яка сприяє розвитку інформаційного обслуговування наукової бібліотеки.

1.2 Огляд мережевих архітектур для реалізації мережі наукової бібліотеки

Для побудови мережі наукової біблі можна використати різні архітектури мережі, залежно від вимог та потреб.

Ієрархічна архітектура мережі є підходом до створення комп'ютерної мережі, у якій вузли організовані в ієрархічну структуру з різними рівнями функцій. Такий підхід дозволяє ефективно розподілити навантаження, забезпечити зручне управління мережею та відповідати потребам наукової бібліотеки.

В архітектурі використовуються різні рівні мережі зі строгим розподілом функцій. Наприклад, центральні комутатори на рівні корпусу бібліотеки забезпечують зв’язок між відділами, читальними залами та підсистемами бібліотеки, розподіляючи мережевий трафік до рівнів доступу в кожній зоні бібліотеки.

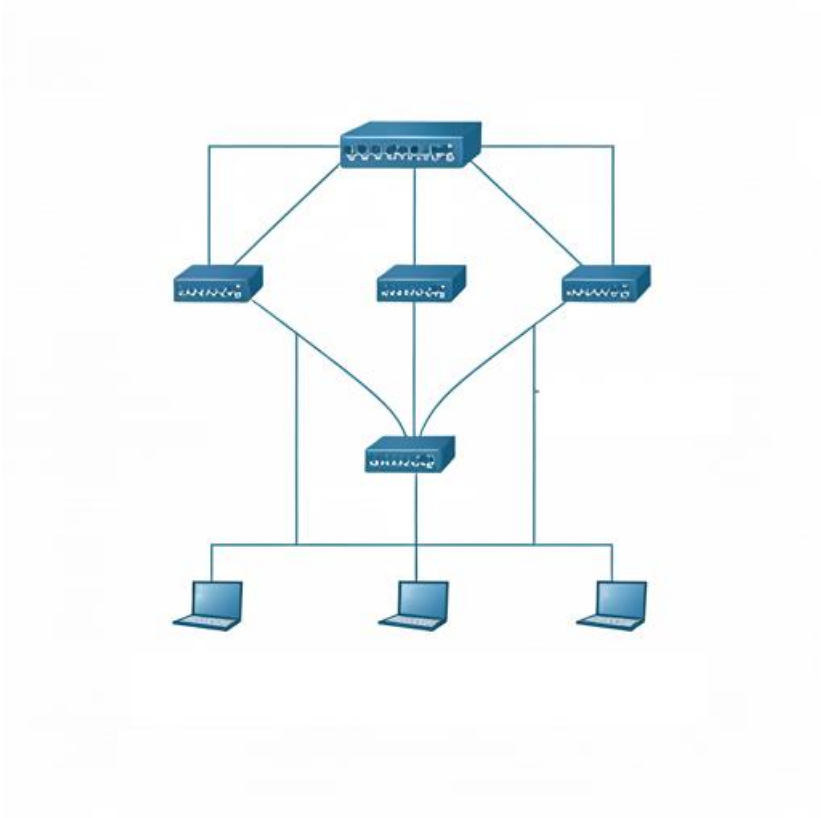


Рисунок 1.1 – Ієрархічна архітектура мережі

Основні рівні ієрархічної архітектури мережі (Рис. 1.1):

Рівень доступу (Access Layer). Найнижчий рівень, що забезпечує підключення кінцевих пристроїв (комп’ютерів, принтерів, сканерів, електронних табло тощо) до мережі. Він використовує комутатори або точки доступу Wi-Fi для організації локального доступу в читальних залах, архівах та інших зонах бібліотеки.

Рівень дистрибуції (Distribution Layer). Цей рівень відповідає за маршрутизацію, розподіл трафіку, політики безпеки та з'єднання між сегментами мережі бібліотеки. Тут використовуються маршрутизатори, комутатори та інші пристрої для ефективного управління трафіком.

Рівень ядра (Core Layer). Центральний рівень мережі, який забезпечує швидкий і надійний обмін даними між усіма сегментами бібліотеки. Він використовується для об'єднання всіх підрозділів у єдину мережу з високою пропускною здатністю.

Додаткові рівні:

Рівень сервісів (Services). Може включати сервери електронних каталогів, баз даних, системи автоматизації бібліотеки, сервіси для обробки запитів користувачів тощо.

Рівень підключення до зовнішніх мереж (WAN Connectivity). Відповідає за доступ до Інтернету, електронних архівів, міжнародних баз даних і взаємодію з іншими бібліотеками.

Ієрархічна архітектура мережі дозволяє легко масштабувати мережу, додаючи нові пристрої або збільшуючи трафік, не перепроектовуючи її ядро. Такий підхід оптимізує роботу мережі, сприяє її надійності, безпеці та продуктивності, що є критично важливим для сучасної наукової бібліотеки.

1.3 Архітектура комп'ютерних мереж

Архітектура комп'ютерної мережі – це правила її проектування та реалізації, яка визначає:

- топологію мережі;
- основні складові мережі;
- фізичну та віртуальну реалізацію взаємодії елементів у мережі.

Розрізняють фізичну та логічну архітектури комп'ютерної мережі.

Фізична архітектура – спосіб представлення комп'ютерної мережі у вигляді апаратних елементів, з якими вона взаємодіє.Приклад фізичною архітектури мережі зображено на рисунку 1.2.

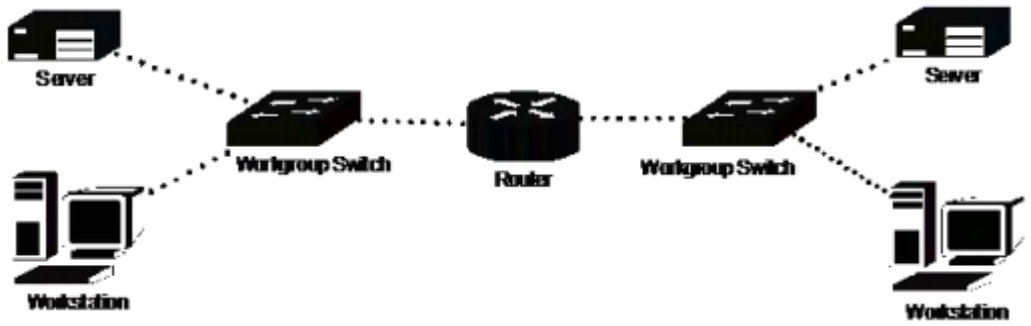


Рисунок 1.2 – Фізична архітектура комп'ютерної мережі

Логічна архітектура – спосіб представлення комп’ютерної мережі у вигляді взаємно зв’язаних між собою хостів.Приклад логічної архітектури зображено на рисунку 1.3. Логічна архітектура відображає технологію комп’ютерної мережі та може бути деталізована за допомогою рівнів фізичної архітектури.

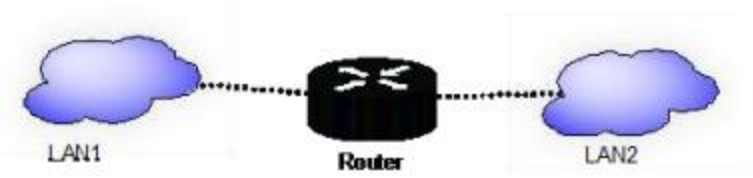


Рисунок 1.3 – Логічна архітектура мережі

1.4 Модель ISO/OSI

Модель Cisco OSI була побудована при створенні глобальних мереж.Модель була побудована так, щоб була можливість розділити стеки протоколів, та забезпечити можливість їхньої розробки незалежними організаціями, отже щоб процес модернізації протоколів став більш доцільним.У моделі Cisco OSI є сім рівнів взаємодії, які має робити кожен рівень.

Система Cisco Osi показана на рисунку 1.4.

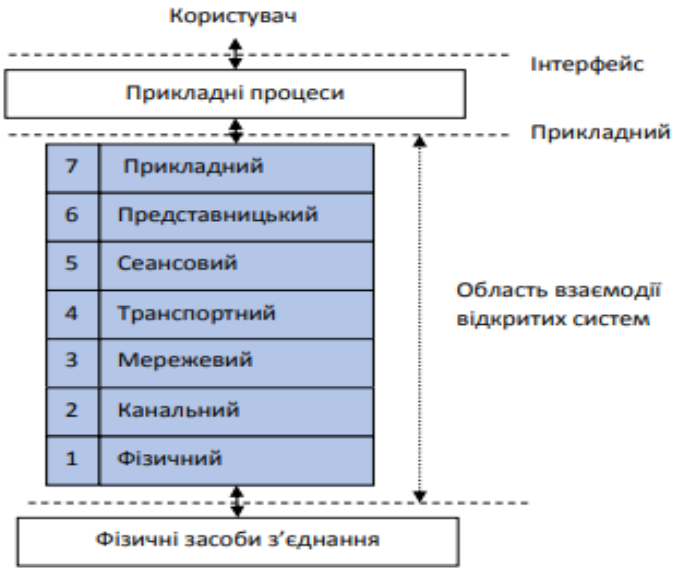


Рисунок 1.4 – Модель Cisco OSI

Модель Cisco OSI не включає в себе методи взаємодії з процесами користувачів прикладного рівня.Свої протоколи взаємодії процеси прикладного рівня реалізовують за допомогою звертання до системних засобів.У таблиці 1.1 показано призначення кожного рівня моделі OSI.

На фізичному рівні реалізовується передача бітів.На мережевому рівні кадри, які ще не сформувались, мають назву дейтаграми(datagrames).

На канальному рівні інформація складається з кадрів, так званих фреймів.

Таблиця 1.1 – Рівні моделі Cisco OSI

№	Рівень	Призначення	Приклади
7	Прикладний (Application)	Забезпечує послуги, що надаються безпосередньо прикладним програмам	SMTP, HTTP, FTP і т.п.
6	Представлення (Presentation)	Забезпечує кодування і перетворення даних. Цей же рівень здійснює шифрування і стиснення даних.	Стандарти кодування (GIF, JEPEG, TIFF MPEG і т.п.)
5	Сеансовий (Session)	Забезпечує проведення сеансів зв'язку (тобто установку, підтримку і переривання зв'язку). Цей же рівень розпізнає логічні імена абонентів, контролює надані їм права доступу.	Remote Procedure Call, Session Control Protocol (SCP)
4	Транспортний (Transport)	Забезпечує доставку даних від одного вузла до іншого без помилок і втрат, а також в необхідній послідовності, через їх розбивку на пакети і нумерування пакетів. Доставка пакетів можлива як з встановленням з'єднання (віртуального каналу), так і без нього.	TCP, UDP
3	Мережевий (Network)	Забезпечує логічну структуризацію мережі і маршрутизацію пакетів між підмережами. Цей же рівень здійснює перетворення мережевих адрес в фізичні (наприклад, IP-адрес в MAC-адреси).	IP
2	Канальний (Data Link)	Забезпечує надійну передачу даних в рамках підмережі з тим чи іншим каналом зв'язку (шляхом формування низькорівневих кадрів для даного виду підмережі)	Ethernet, Token Ring, FDDI, Frame Relay, PPP (Point-to-Point Protocol)
1	Фізичний (Physical)	Забезпечує умови прийому-передачі по фізичному каналу зв'язку шляхом визначення вимого до його фізичних, механічних, електричних та інших характеристик (рівні напруги, частота, опір і т.п.)	LAN категорії 3, LAN категорії 5, V.90

1.5 Стек протоколів TCP/IP

Стек TCP/IP був розроблений за вимогою Міністерства оборони Сполучених Штатів Америки, та на сьогоднішній день вважається одним з найбільш популярних.

Великий внесок було зроблено університетом Берклі, який у своїй операційній системі UNIX реалізував стек протоколів TCP/IP.

Модель стеку TCP/IP зображено на рисунку 1.5. Була розроблена також спеціальна характеристика, яка визначає експлуатацію технології ATM на тому рівні.

Рівні моделі OSI	**Протоколи стеку TCP/IP**				**Рівні моделі TCP/IP**	
7 6	HTTP	FTP	SMTP	Telnet	I	Прикладний
5 4	TCP		UDP		II	Транспортний
3	IP	RIP	OSPF	ICMP	III	Міжмережевої взаємодії
2 1	Ethernet	Token Ring	FDDI	ISDN	IV	Мережевих інтерфейсів

Рисунок 1.5 – Модель стеку протоколів TCP/IP

До складу стеку протоколів TCP/IP входить ряд утилів для пошуку та усунення неполадок в TCP/IP-мережах, які розглянуто на рисунку 1.7.

На рисунку 1.6 розглянуто, як працює утиліта Tracert

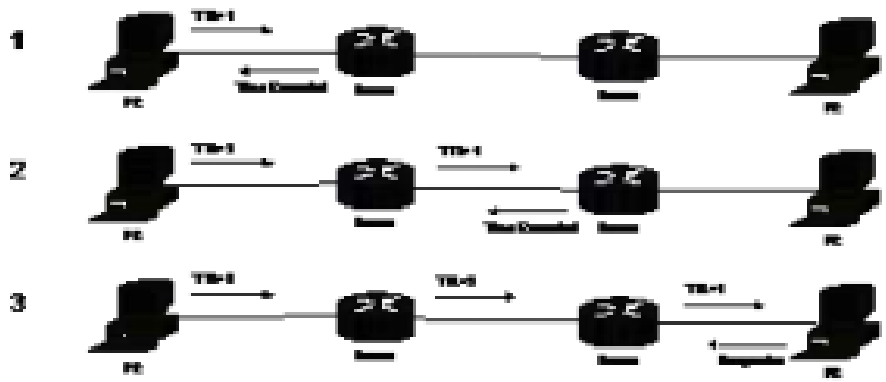


Рисунок 1.6 Приклад роботи Tracert

Утиліта	Опис
Hostname	Виводить хост-ім'я локального комп'ютера (не передбачає будь-яких параметрів і ключів)
Ipconfig	Виводить звіт про конфігурацію IP-інтерфейса.
Ping	Перевіряє доступність віддаленої системи. Утиліта відправляє на IP-адресу одержувача відлуння-запит ICMP. Якщо хост з вказаною адресою відповідає, можна спробувати використати замість IP-адреси хост-ім'я. Утиліта спочатку намагається перетворити хост-ім'я в IP-адресу через DNS-сервер, потім через WINS-сервер і нарешті за допомогою локального широко віщання. Якщо перевірка за адресою закінчилась успішно, а за ім'ям – ні, це свідчить про проблему не в мережевому з'єднанні, а в розпізнаванні імен. Використання ключа –a дозволяє перетворювати IP-адреси в хост-імена.
Tracert	Дозволяє прослідкувати маршрут до віддаленої системи. Утиліта відправляє відлуння-запити ICMP, послідовно збільшуючи значення поля TTL на 1, як показано на рис. 8.3. Обробка запиту маршрутизатором полягає у зменшенні значення поля TTL на 1 і відправки спеціального повідомлення Time Exceeded у випадку коли TTL=0. Після кожної успішної доставки утиліта відправляє пакет на один перехід далі.
Pathping	Дозволяє прослідкувати маршрут до віддаленої системи і оцінити втрати пакетів на кожному маршрутизаторі. Утиліта суміщає в собі функціональність утиліт Ping і Tracert та надає додаткову інформацію про ступінь перевантаженості каналу.
Netstat	Відображає статистику по протоколам і TCP/IP -з'єднанням. Найчастіше використовується з такими ключами: -a – для виведення інформації по всім з'єднанням; -e – для виведення статистики по інтерфейсу; -s – для виведення статистики по TCP, IP, ICMP і UDP для локального хосту.
Arp	Для перегляду кеша ARP і виявлення в ньому некоректних записів. Якщо двом хостам не вдається з'єднатись по команді Ping, слід виконати на кожному з них команду Arp –a, щоб перевірити правильність MAC-адрес в кешах ARP. З'ясувати коректну MAC-адресу можна за допомогою Ipconfig.

Рисунок 1.7 – Утиліти Microsoft TCP/IP

1.6 Адресація в комп'ютерних мережах

При комутації двох або більше хостів у мережі виникає необхідність в тому, щоб ідентифіквати кожен хост.

Адреси можуть бути використані не тільки для ідентифікації хостів, але й їх груп.За допомогою таких адрес дані можуть бути направлені одразу декільком хостам.Також є широкомовна адреса – дані, направлені за її допомогою доставляються усім хостам в мережі.

Існує декілька схем адресації.

Адресний простір це множина усіх адрес, які є у комп'ютерній мережі.

Множина адрес може бути не структурованою, у випадку плоского адресного простору, як показано на рисунку 1.8.

Рисунок 1.8 – Плоский адресний простір

Також адресний простір може складатись із вкладених одна в одну груп, якщо розглядати ієрархічну організація простору. Вона є більш доцільною порівнюючи з лінійною:вона дає змогу на етапі початку транспортування даних використовувати лише старшу складову адреси, а потім інші складові, при кінці – наймолодшою складовою адреси. На рисунку 1.9 розглянуто адресний простір дворівневої ієрархії.

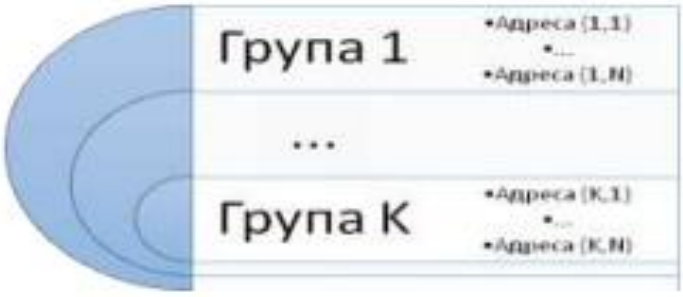


Рисунок 1.9 Адресний простір дворівневої ієрархії

Типовим прикладом адресного простору дворівневої ієрархії є поштова адреса, в якій покроково уточнюється геолокація адресата.

Хост може мати водночас декілька адрес, це залежить від схеми адресації, яка використовується.Для того, щоб перетворити адресу з одного виду в інший використовується спеціальний допоміжний протокол, який має назву протокол розрізнення адрес.

Стек протоколів TCP/IP використовує три типи адрес:

-мережеві адреси(IP)-використовуються на мережевому рівні для обміну даними між мережами;

- локальні адреси(апаратні)- застосовуються на канальному рівні, для передачі даних в мережі за заданим способом;

-символьні адреси – застосовуються в основному на прикладному рівні , щоб забезпечити комфортну роботу з мережевими ресурсами, та даними.

Локальна адреса (апаратна адреса)– називається адреса канального рівня, яка застосовується для базової мережевої технології при доставці даних в межах комп'ютерної мережі .

Якщо підмережею є локальна мережа, тоді роль локальної адреси буде відігравати MAC-адреса.Але до складу інтрамережі може входити також підмережа, яка використовує технологію глобальних мереж.

MAC-адреса – це особистий номер мережевого інтерфейсу в комп'ютерній мережі, який зафіксовано в його программному забезпеченні.

MAC-адреса це двійкове число , довжина якого становить 48 біт, та яке для легкості його сприйняття записується у вигляді 12 цифр в шістнадцятковій системі числення, та розділені тире, наприклад, 21-D3-JK-19-49-12-F2.Тут перші шість символів вказують виробника пристрою, а решта – сам пристрій.

Інтерфейс мережі приймає та обробляє тільки кадри, MAC-адреса яких співпадає з власною.Решта кадрів відкидається.Для того, щоб розрізняти адреси у мережі було створено протокол визначення адреси – ARP(Address Resolution Protocol).

Адреса мережі – це логічна адреса мережного рівня, яка застосовується в якості номера вузла інтрамережі.

Інтернет-протокол IPv4 відиляє двійкове число довжиною 32 біти для IP-адреси.Відповідним чином, протокол IPv6 виділяє 128 бітів, і це основна різниця між протоколами IPv4 та IPv6.

Запис IP-адреси у двійковому вигляді не зручний для використання.Тому, IP-адреса нотується в десятковій , або шістнадцяткових системах числення.

У таблиці 1.2 показано переведення двійкової нотації IP-адреси в десяткову систему числення

Таблиця 1.2 Переведення IP-адреси з двійкової системи числення в десяткову

Двійкова нотація IP-адреси:	10000000000010100000001000011110			
Виділені октети в двійковій системі числення	10000000	00001010	00000010	00011110
Десяткові значення октетів	128	10	2	30
Десяткова нотація IP-адреси:	128.10.2.30			

В адресації , де за основу взято класи, ідентифікатор мережі можна знайти за допомогою значень перших бітів адреси. На основі цього виділяється 5 класів, які показано у таблиці 1.3.

Таблиця 1.3 Класи адрес, які відповідають протоколу адрес IPv4

	Перший октет	Другий октет	Третій октет	Четвертий октет
Клас А	0 Номер мережі	Номер хоста		
Клас В	10 номер мережі		Номер хоста	

Клас C	110 Номер мережі	Номер хоста
Клас D	1110 Широкомовна адреса	
Клас E	11110 Зарезервована адреса	

Якщо адреса починається не з 1, а 0, тоді вона входить у класс A , та під номер комп'ютерної мережі виділяється перший октет.

Якщо адреса починається з 10, тоді вона входить в класс B та під номер комп'ютерної мережі виділяєтьсяя два перших октети.

Серед адрес класів A, B та C існує набір адрес, які були спеціально зарезервовані , та які не можуть бути використані для ідентифікації хостів:

- в номері комп'ютерної мережі, або хоста, не можна встановити усі біти в 1.
- в номері комп'ютерної мережі, або хоста, не можна встановити усі біти в 0.
- номер комп'ютерної мережі не може починатися з 127.

Ці адреси зарезервовані для діагностування программного забезпечення та взаємодії процесів комп'ютерної мережі в рамках окремого хоста.

Наприклад, пакет з IPv4-адресою 127.0.0.1 не буде транслюватись в комп'ютерну мережу, а буде відправлений для верхніх рівнів протоколів.

Характеристики адреси класів A, B та C, якими можна користатися задля ідентифікації хостів було розглянуто нижче у таблиці 1.4.

Таблиця 1.4 Характеристика адрес відповідно IPv4 протоколу

Клас	Діапазон значень першого октета	Максимальна к-сть комп'ютерних мереж	Максимальна к-сть хостів у мережі
A	1-126	126	16 777 214
B	128-191	16 382	65 534
C	192-223	2 097 150	254

1.6.1 Маски адрес у комп'ютерній мережі

Адресація вважається нераціональною, якщо вона базується на основі класів, адже при її експлуатації ініціалізується фіксована к-сть хостів у комп’ютерній мережі.Тому, зараз все частіше починає використовуватись більш гнучкий спосіб для визначення обмежень між ідентифікатором мережі та хоста – за основу береться маска комп’ютерної під мережі.

Число, яке містить в соті 32 біта, та використовується для розпізнавання номера комп’ютерної мережі та номера хоста у IP-адресі називається маскою під мережі. Або ще маску підмережі часто називають двійковим числом, яке використовується з IP-адресою, та має таку ж саму довжину.Маски адрес у комп’ютерній мережі розглянуто в Таблиці 1.5

Таблиця 1.5 Маски адрес для класів у мережі

	Біти маски	Маска в десятковій системі числення	Маска в шістнадцятко вій системі числення	Маска у вигляді префіксу
A	11111111 00000000 00000000 00000000	255.0.0.0	FF.00.00.00	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	FF.FF.00.00	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	FF.FF.FF.00	/24

1.6.2 Публічні та приватні адреси

Для мережі Інтернет використовується два вида IP-адрес : приватні та публічні.

Публічні адреси призначає комітет InterNIC , вони містяться в собі ідентифікатор мережі, які є унікальними в мережі Інтернет.Маршрутизатори InterNIC гарантують доставку трафіка, який направлений на ці адреси, за їхнім призначенням.Доступ до цього трафіка можливий через Інтернет.

В приватних комп'ютерних мережах, які не планують бути під'єднані до мережі Інтернет, можна використовувати які завгодно адреси, навіть ті, що можуть бути зарезервовані InterNIC.Але, якщо через певний час ця мережа буде підключена до Інтернет, може виявитись, що у ній були використані адреси, які були зарезервовані InterNIC для інших організацій.Такі адреси мають назву «недоступні».Отримати доступ в мережу Інтернет з цих адрес неможливо. В основному, не всі вузли вимагають з'єднання з мережею Інтернет напряму.Більшості підприємства потрібні не великі діапазони IP-адрес, які будуть зарезервованими для хостів, напряму підключених до мережі Інтернет – проксі-серверів, брендмауерів, маршрутизаторів.

У Таблиці 1.6 розглянуто приклад розбиття адрес комп'ютерної мережі на підмережі, використовуючи маску.

Таблиця 1.6 Використання маски мережі для розбиття її на підмережі

Необхідна к-сть підмереж	Число бітів для ідентифікації підмережі	Маска підмережі	К-сть хостів у підмережі
1-2	1	255.255.255.128	126
3-4	2	255.255.255.192	62
5-8	3	255.255.255.224	30
9-16	4	255.255.255.240	14
17-32	5	255.255.255.248	6
33-64	6	255.255.255.252	2

Адресний простір приватних мереж можна визначити трьома блоками адрес:

- 10.0.0.0/8 – Мережа класу A, яка включає в себе адреси від 10.0.0.1 до 10.255.255.254.
- 172.16.0.0/12 – Мережа класу B, яка включає в себе адреси від 172.16.0.1 до 172.31.255.254.
- 192.168.0.0/16 – Мережа класу C, яка включає в себе адреси від 192.168.0.1 до 192.168.255.254

Трафік від хоста з приватною адресою повинен надходити до проксі сервера, який перед відправленням інтернет-трафіку в мережу Інтернет транслює приватні адреси в допустимі публічні адреси.

1.7 Постановка задачі

Аналіз можливих рішень для впровадження мережі наукової бібліотеки показав, що архітектура SOHO є неприйнятною, оскільки вона не забезпечує необхідного рівня безпеки для мережі та її користувачів.

На основі цього необхідно спроєктувати мережу, яка відповідатиме таким вимогам:

- Топологія мережі: структура "зірка".
- Кабельна інфраструктура: між основними вузлами використовується одномодове оптоволокно, а від вузлів до кінцевих пристроїв – мідний кабель UTP категорії 5E.
- Відеоспостереження: фізично відокремлений сегмент.
- Ядро мережі: маршрутизатор і файрвол.
- Рівень дистрибуції: керовані комутатори L3 з оптичними портами.
- Розподіл мережі: поділ на VLAN для ізоляції різних сегментів.
- Управління доступом: використання ролей для розмежування доступу до ресурсів мережі.

- Wi-Fi: точки доступу з підтримкою multiSSID.
- Розміщення обладнання: маршрутизатори, сервери та файрволи повинні бути встановлені в серверній кімнаті з обмеженим доступом.
- Аутентифікація: впровадження сервера LDAP для зберігання облікових записів користувачів, їхніх ролей і забезпечення авторизації доступу до ресурсів.
- Проєктування мережі: розробка логічної та фізичної топологій.

2 ПРОЕКТУВАННЯ МЕРЕЖІ НАУКОВОЇ БІБЛІОТЕКИ

2.1 Політики безпеки та правила розмежування доступу

Політика безпеки визначає загальні принципи та цілі, які встановлюються організацією для забезпечення конфіденційності, цілісності та доступності інформації. Вона визначає припустимі та недопустимі види діяльності, а також встановлює відповідальність за порушення правил.

Правила розмежування доступу регламентують, які користувачі або групи користувачів мають доступ до певних ресурсів інформаційної системи. Вони обмежують доступ лише до необхідних для роботи ресурсів, враховуючи ролі користувачів, рівні довіри чи контекст автентифікації.

Основні методи реалізації політики безпеки в бібліотеці:

- Автентифікація і авторизація. Використання паролів, сертифікатів або біометричних даних для ідентифікації читачів і надання їм прав доступу.

- Ролева модель доступу. Розподіл прав на основі ролей, таких як бібліотекарі, читачі чи адміністрація бібліотеки.

- Модель "найменшого привілею". Користувачі мають лише ті дозволи, які необхідні для виконання їхніх завдань.

- Аудит і моніторинг. Збір та аналіз журналів дій користувачів для виявлення потенційних загроз.

Оскільки мережею бібліотеки користуються читачі, бібліотекарі, адміністрація, а також відвідувачі, потрібно провести аналіз їхніх потреб та визначити права доступу до ресурсів.

Права читачів:

- Доступ до особистого кабінету веб-системи (пошук літератури, резервування книг).

- Доступ до цифрових ресурсів (електронних книг, баз даних).

- Доступ до локальної мережі бібліотеки для роботи з каталогами.

Права бібліотекарів:

- Адміністрування облікових записів читачів.

- Контроль та оновлення інформації про фонди бібліотеки.

- Доступ до локальних ресурсів та хмарних сховищ для роботи.

Права адміністрації:

- Формування звітів про відвідуваність та використання ресурсів.

- Управління політиками доступу до мережі.

Аналіз прав користувачів мережі вказує, що користувачі постійно працюють з мережею з однією роллю.

Відповідно до цього прийняте рішення забезпечити рольовий доступ для користувачів, авторизацію та автентифікацію користувачів.

З огляду на це визначено такі ролі в системі:

- Адміністратор мережі. Має права на зміну налаштувань мережевого обладнання, адміністрування серверів, резервне копіювання та відновлення даних, реєстрацію та зміну ролей користувачів, зміну політик доступу, адміністрування та користування корпоративною поштою.

- Адміністратор бібліотеки. Має права на оновлення інформації про бібліотечний фонд, формування звітів щодо використання ресурсів, контроль доступу до мережевих і цифрових ресурсів, користування корпоративною поштою.

- Бібліотекар. Має права на обробку заявок читачів, адміністрування облікових записів, редагування та оновлення даних про літературу, доступ до локальних і хмарних ресурсів бібліотеки, користування корпоративною поштою.

- Читач. Має права на доступ до особистого кабінету, перегляд бібліотечного каталогу, резервування літератури, доступ до електронних ресурсів і користування локальною мережею бібліотеки.

- Технічний персонал. Має права на доступ до розкладу роботи відділів та службових інструкцій.

- Відвідувачі. Мають обмежені права – доступ до публічного Wi-Fi та відкритих веб-ресурсів через мережу бібліотеки.

Такий розподіл ролей забезпечує раціональне використання ресурсів бібліотеки та гарантує безпеку інформаційної інфраструктури.

2.2 Компоненти комп'ютерної мережі бібліотеки

Для того,щоб забезпечити можливість зв'язку персонального комп'ютера з рештою пристроїв у мережі , використовується мережевий NIC(Network Interface Card).

NIC-це периферійний пристрій, який взаємодіє з середовищем транспортування даних.

Network Interface Card виконує задачі канального та фізичного рівнів моделі Cisco OSI, які розглядались у розділі №1.

До основних функцій NIC відносяться такі як:

- кодування та декодування інформації,
- розпізнавання даних,які приймаються,
- метод доступу до середовища передачі даних,
- буферизація даних.

Nic поділяються на адаптери Token Ring, FDDI ,в залежності від технології побудови.NIC виготовляються у вигляді окремої плати ,яка під'єднується у слоти розширення комп'ютера.

Мережевий адаптер зазвичай розрахований на один тип передачі даних,наприклад вита пара,але він може підтримувати кілька середовищ(товстий/тонкий коаксіальний кабель).Спеціально для цього,на платі встановлюють відповідні входи.Найбільш розповсюдженими є адаптери Combo, в склад яких входять усі види роз'ємів ,такі як:

- BNC,
- AUI,
- RJ-45.

Основною задачею NIC є отримання,та передача інформації.

На рисунку 2.1 розглядається топологія комп'ютерної мережі,яка містить в собі три персональних комп'ютери з NIC через комутатор,робота якого буде розглянута нижче.Стандарт підключення NIC до коммутатора виглядає таким чином:усі мережеві адаптери NIC ПК мають по два виходи для транспортування сигналу та прийому,за допомогою кабелю,наприклад – коаксіального.Транслятор сигналу від персонального комп’ютера ,який розташований на NIC,має назву трансмітер,і позначається Tx,а приймача сигналу називають ресивер,та позначається Rx.Також не слід забувати,що швидкість передачі даних у комп’ютерній мережі залежить не тільки від NIC,але і інших чинників,такі як швидкодія диску,процесора,об’єм оперативної пам’яті,завантаженість комп’ютерної мережі,ПЗ тощо.

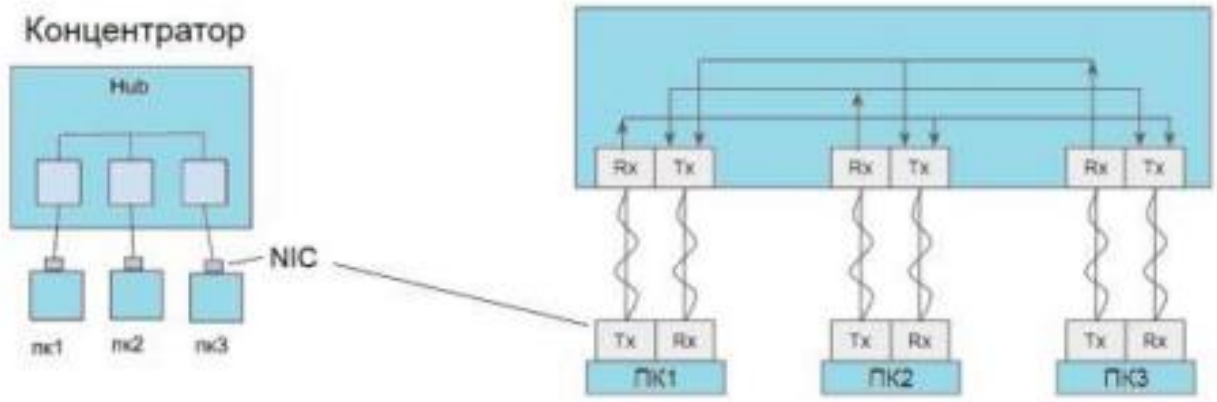


Рисунок 2.1. – Візуальна модель коммутатора(Hub’a)

Отже,вибір швидкого NIC не завжди може вплинути на швидкість передачі даних у комп’ютерній мережі. Для того,щоб підвищити швидкість передачі даних у комп’ютерній мережі необхідно проводити тестування продуктивності мережі за допомогою програм,які створені для тестування мереж,такі як : nGrinder,WireShark,Netbrench,та порівнювати їх результати.

2.3 Мости

Коли досягається граничне значення хостів у комп’ютерній мережі,тривалість затримок збільшується у арифметичній прогресії,і також пропускна здатність комп’ютерної мережі починає знижуватись.Щоб цього не було,мережу слід розбивати на декілька під мереж,які комутуються за допомогою мостів.Міст-мережевий пристрій,який застосовується для об’єднання комп’ютерних мереж.Міст передає кадри з однієї комп’ютерної мережі у іншу.Також за допомогою мостів комп'ютерна мережа поділяється на декілька підмереж,які розподіляють мережевий трафік,через що зменшується навантаження на середовище передачі даних.На рисунку 2.2 розглянуто приклад логічної моделі на базі моста.

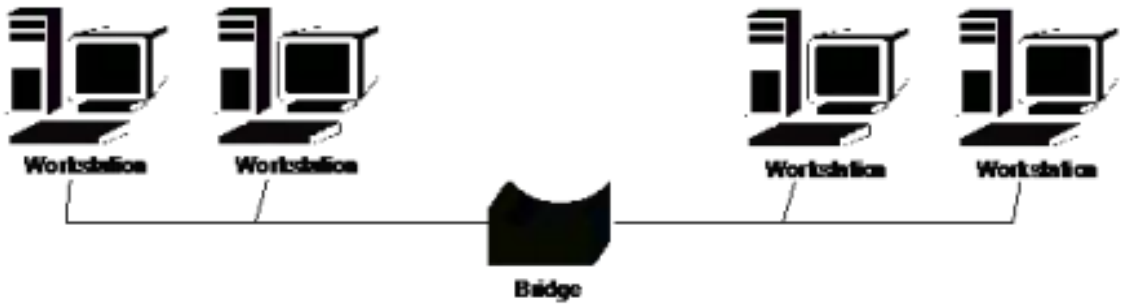


Рисунок 2.2 – Логічна модель мережі на базі моста

2.4 Комутатори(Switch)

Комутатор це мережевий пристрій,який дає можливість комутувати декілька сегментів у одну комп'ютерну мережу,задовільняючи її високу ефективність та пропусну здатність.

Комутатор також можна розглядати як швидкий міст.Він дає змогу розподіляти комп'ютерну мережу на декілька підмереж,щоб збільшити радіус мережі,та зменшити завантаження комп'ютерної мережі вцілому.

Основна відмінність коммутатора від моста,це те,що коммутатор виконує паралельну обробка кадрів,а мост послідовну.

Логічна структура комутатора розглянута на рисунку 2.3.В її склад входить перехресна матриця,у критичних точках якої можуть відбуватись комутація на час передачі даних.В результаті ,дані які приходять від якогось хоста,можуть бути передані в будь-який інакший.

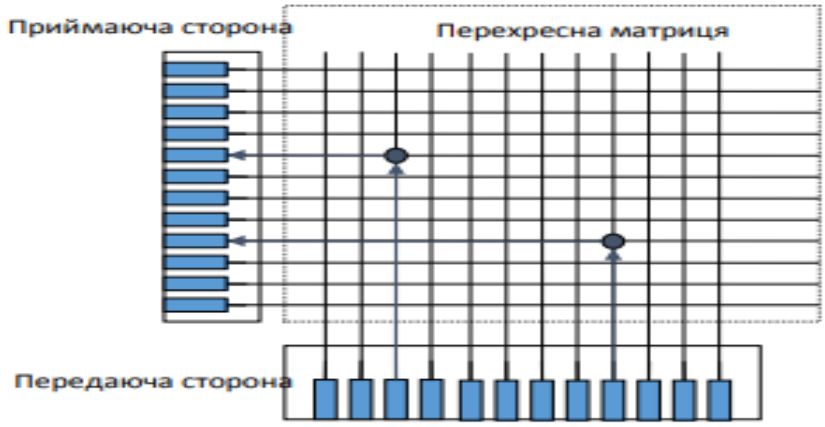


Рисунок 2.3 – Логічна модель свіча

В основному свічі виготовляються з 12,16, та 24 портами.При розділені на підмережі,не слід нехтувати правилом 80:20.Для того,щоб комутатор працював ефективно – треба щоб приблизно 80% усіх транспортувань відбувались у межах однієї частини мережі,а 20% усіх транспортувань має відбуватись між різними сегментами.

Це правило все частіше обумовлюється тим,що сервер та станції,які з ним працюють мають розсташовуватись в одному сегменті комп'ютерної мережі.

2.5 Маршрутизатор

Роутер – пристрій,який пересилає пакети даних у комп'ютерних мережах. Роутери також мають можливість керувати трафіком в мережі Інтернет.Зазвичай,пакет даних транспортується з одного роутера на інший через

комп'ютерні мережі,які утворюю глобальну мережу Інтернет,поки він не дійде до свого кінцевого хоста.Логічне зображення роутера зображено на рисунку 2.4.

Роутер може підключатись до двох,та більше ліній зв'язку у різних мережах.Він зчитує інформацію про IPv4 адресу пакета,коли дані приходять на маршрутизатор,щоб визначитись з кінцевим пунктом призначення.Внаслідок цього,записується адреса у таблицю маршрутизації,та використовуючи цю інформацію направляє пакет у наступну мережу.

Рисунок 2.4 – Логічна модель роутера

Найбільш розповсюджений вид роутерів це домашній або невеликий офісний маршрутизатор,який передає IP-пакети між комп’ютерами та глобальною мережею Інтернет.Прикладом роутера може виступати власний кабель,або DSL розтер,який під’єднується до глобальної мережі Інтернет,через постачальника послуг Інтернет(ISP).Наприклад,більш професійні роутери,до яких відносяться корпоративні,які підключають величезні комп’ютерні мережі,або комп’ютерні мережі глобальної мережі Інтернет до більш потужніших роутерів ,які здійснюють передачу даних на більш високій швидкості за допомогою опто-волоконного кабелю.Зазвичай роутери застосовуються лише апаратними пристроями,але також існують роутери на базі ПЗ.

2.6 Канали зв’язку та види кабелів у комп’ютерній мережі

Каналом зв’язку називається сполучення ліній зв’язку та мережевих пристроїв,які здійснюють транспортування сигналів від транслятора до

кінцевого хоста.Лінія зв'язку це фізичний простір трансліції інформації,через який відбувається передача сигналу.Пристрої зв’язку налічують:

- Апаратура передачі інформації – гарантує передачу та прийом сигналу;
- проміжні обладнання – виконують дві задачі: посилюють сигнал та гарантують постійний зв’язок між абонентами

Отже,канали зв’язку створюють:

- лінії зв’язку;
- пристрої передачі інформації(NIC,роутери,тощо);
- проміжне обладнання (концентратор,репітер,та інші).

На рисунку 2.5 розглянуто приклад простого каналу,та на рисунку 2.6 також.

Рисунок 2.5 – Структура каналу зв'язку

В мережах зазвичай використовують :

- провідні канали зв’язку – вони побудовані на базі провідних та кабельних магістралей зв’язку (коаксіальний кабель,вита пара,опто-волоконний кабель),
- безпровідні канали зв’язку – побудовані на базі радіо ліній зв’язку,супутникового зв’язку,мікрохвильового зв’язку ,або радіозв’язку надвисокої частоти.

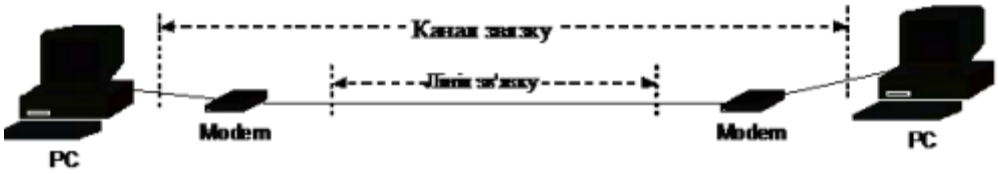


Рисунок 2.6 – Приклад каналу зв'язку

2.6.1 Типи ліній зв'язку

Для того,щоб інформація передавалась по мережі застосовують такі типии ліній зв'язку ,як показано на рисунку 2.7.

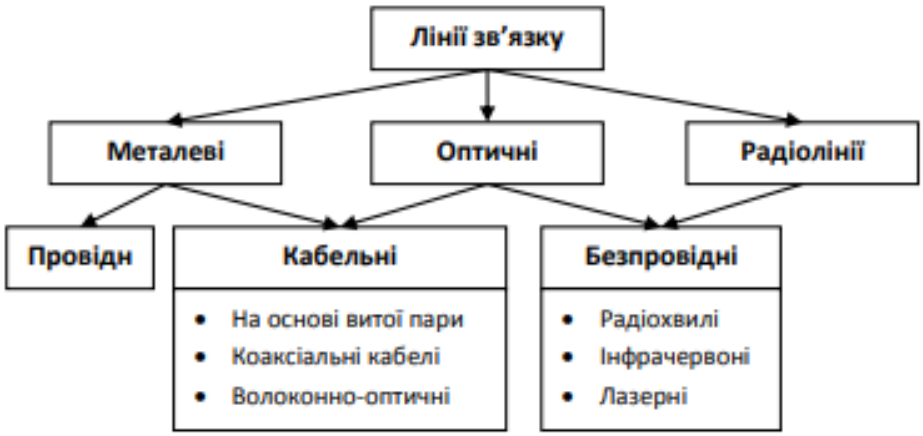


Рисунок 2.7 – Типи ліній зв’язку

Провідні лінії створюють магістралі без ізоляційних обгорток,що підвішуються до стовпців.Зазвичай такі лінії використовують телефонні сигнали,або коли відсутні інші можливості,можуть також застосовуватись для транспортування інформації.Також на сьогоднішній день широко розповсюджена технологія,яка дає змогу користуватись лінією електропостачання для передачі інформації та даних.

Кабельні магістралі – містять в собі мідний провідник,який захищається декількома шарами ізоляції.В комп’ютерних мережах існує три типи кабельних ліній:

- вита пара з мідним провідником;

- опто-волоконний кабель;
- коаксіальний кабель.

Усі ці види кабелів ми розглянемо пізніше.

Також існують бездротові лініх,які для передачі інформації використовують радіхвилі.Пропускна здатність таких ліній може досягати декілька десятків Гбіт/с.

Основним недоліком цих ліній є їхня висока вартість пристроїв,надійність зв'язку,низький рівень захисту,та вразливість до нападу.Бездротові лінії використовуються якщо треба підтримувати контакт з об'єктом,який рухається,тобто не є статичним,або для того,щоб не витрачати гроші на прокладання кабельної магістралі.

Інфрачервоний канал зв'язку використовується для трансляції інформації в інфра-червоному діапазоні.Швидкість передачі інформації через інфрачервоний канал обмежена 5-10 Мбіт/с.Аналогічно,як і з бездротовим каналом зв'язку для його робоити використовуються дорогі приймачі та передавачі,захист при цьому не забезпечується.Основною перевагою щодо бездротових ліній є те,що не потрібно отримувати дозвіл на експлуатацію та встановлення,через те ,що інфрачервоний канал зв'язку має малу потужність випромінювання,приблизно до 50 Мегават.Але основним їхнім недоліком є те,що вони працюють в умовах сильної запиленості повітря не дуже ефективно.

Найрідкішими рахуються лазерні канали,через те що вони мають високу вартість,та за рахунок цього використовуються тільки у особливих випадках:коли неможливо забезпечити з'єднання за допомогою кабельної магістралі(наприклад через річку),або для того,щоб створити запасний канал зв'язку тощо.

2.6.2 Види кабелю

Основними видами кабелів,які використовують при проектуванні комп'ютерних мереж ,є :

- опто-волоконні кабелі,
- вита пара,
- коаксіальні кабелі.

Вита пара – кабель,який складається з двох проводів,скручених між собою та за ізольованими,як показано на рисунку 2.8.

Рисунок 2.8 – Вита пара

Сенс витої пари полягає у тому,щоб зовнішні шуми були рівномірно розподілені.Якщо провідними буде скручено,як вита пара,то джерело шуму може послідовно генерувати в них напругу,це практично не вплине на напругу,як показано на рисунку 2.9.

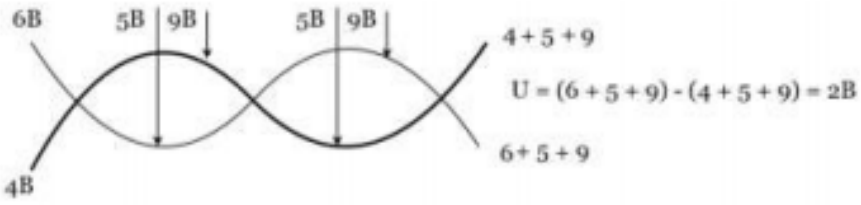


Рисунок 2.9 – Перешкоди витої пари

Існує два типи витих пар:

- екранована вита пара-провода скручуються,та поміщаються в оплітку з екраном;

- неекранована вита пара- провода скручуються без екранування.

На рисунку 2.10 розглянуто основні категорії кабелів.

Категорія	Призначення і характеристики	Швидкість передачі
1	Звичайний телефонний кабель, в якому пари проводів не витi.	20 Кбіт/с
2	Кабель з витих пар для передачі даних у полосі частот до 1 МГц. Зараз використовується рідко.	4 Мбіт/с
3	Широко використовується для передачі даних і голосу в полосі частот до 16 Мгц. Містить 9 витків на метр. Зараз найбільш поширений.	10 Мбіт/с
4	Використовується для передачі даних в полосі частот до 20 МГц. Призначався для роботи в мережах по стандарту IEEE 802.5 (Token Ring Lan). Зараз використовується рідко.	16 Мбіт/с
5	Розрахований на передачу даних в полосі частот до 100 МГц. Містить не менше 27 витків на метр. На сьогодні найбільш досконалий кабель, що рекомендується для використання в сучасних високошвидкісних мережах (типу Fast Ethernet).	100 Мбіт/с
5e	Найбільш поширений в комп'ютерних мережах. Переваги – в меншій собівартості та товщині.	100 Мбіт/с (2 пари) 1000 Мбіт/с (4 пари)
6	Неекранований кабель (UTP) складається з 4 пар провідників, здатний передавати дані на відстань до 55 м	10 Гбіт/с
6A	Складається з 4 пар провідників передає дані на відстань до 100 метрів. Кабель має або спільний екран (F / UTP), або екрани навколо кожної пари (U / FTP).	10 Гбіт/с
7	Кабель цієї категорії має загальний екран і екрани навколо кожної пари (F / FTP, або S / FTP).	10 Гбіт/с
7A	Кабель цієї категорії має загальний екран і екрани навколо кожної пари (F / FTP, або S / FTP). Полоса частот – до 1000 МГц	10 Гбіт/с
8/8.1	Повністю сумісний з кабелем кат. 6A. Швидкість передачі даних до 40 Гбіт/с при використанні стандартних конекторів 8P8C. Кабель цієї категорії має або загальний екран, або екрани навколо кожної пари (F / UTP або U / FTP). Полоса частот – 1600….2000 МГц	40 Гбіт/с
8.2	Сумісний з кабелем кат. 7A. Швидкість передачі даних до 40 Гбіт/с при використанні стандартних конекторів 8P8C або GG45 / ARJ45 і TERA. Кабель має загальний екран і екрани навколо кожної пари (F / FTP або S / FTP). Полоса частот – 1600….2000 МГц	40 Гбіт/с

Рисунок 2.10 – Основні категорії кабелів

Усі кабелі виду неекранована вита пара,випускаються в 4-парному вигляді,незалежно від їхньої категорії,як зображено на рисунку 2.11.

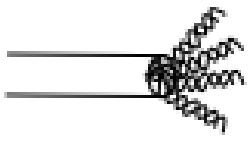


Рисунок 2.11 – Неекранована вита пара

Для комутації цього типу кабелю використовуються роз'єми RJ-45.

Як випливає з Рисунка 2.10,кабелі категорії 7 та 8.2 мають полосу частот 1000 та до 2000МГц.Кабелі у 6 категорії можуть бути як неекрановані,так і екрановані.Кабелі у 7 категорії мають бути обов'язково екранованими.

Такий вид кабелю вважається значно дорожчим,та за вартістю майже такий самий,як волоконно-оптичний кабель.

Волоконно-оптичний кабель складається із світловодів,які розміщуються у захисній оболонці.Кожен світлодіод складається з серцевини,яка має дуже високий рівень перелому світла .

Освновними видами оптоволоконного кабелю є,як зображено на рисунку 2.12.:

- багатомодовий кабель;
- одномодовий кабель.

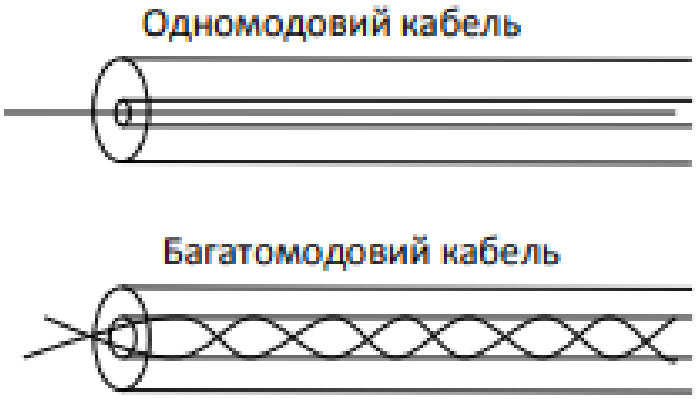


Рисунок 2.12. – Види оптоволоконного кабелю

В одномодовому кабелі використовується серцевина з дуже малим діаметром,

приблизно 9 мкм.Виготовлення світлодіодів такого мізерного діаметру є дуже важким процессом,і тому вартість одномодового кабелю є доволі високою.Але основною перевагою цього типу кабелю є передача інформації на доволі великі відстані з високими швидкостями .(Декілька сотень кілометрів з швидкістю декілька десятків Гбіт/с).

У багатомодовому кабелі використовують ширшу серцевину,через що цей кабель дешевший,ніж одномодовий.Багатомодовий кабель використовується в основному при передачі інформації на малі відстані(приблизно 2000м) з невеликими швидкостями (до 1000Мбіт/с).

Основними перевагами волоконно-оптичного кабелю є:

- невисоке затухання сигналів,
- висока захищеність від перешкод,
- висока швидкість передачі сигнула.

До основних недоліків волоконно-оптичного кабелю є:

- чутливість до випромінювань,
- чутливість до температури,що призводить до створення тріщин,
- складність монтажу та демонтажу.

Коксіальний кабель зображає з себе електричний кабель,який складається з центрального провідника з міді,та металевого екрану,які розділені шаром діелектрика,та поміщені у зовнішню оболонку,яка їх ізолює.

Конструкцію коаксіального кабелю розглянуто на рисунку 2.13.

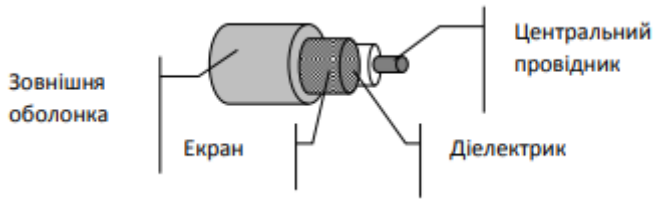


Рисунок 2.13 – Конструкція коаксіального кабелю

Металева оплітка служить для передачі інформації,та захищає основний провід від перешкод.

Для реалізації комп'ютерної мережі використовують:

- тонкий коаксіальний кабель – діаметр центрального провідника становить 0,89 мм та зовнішній діаметр приблизно 50 мм.
- товстий коаксіальний кабель – діаметр центрального провідника становить 2,17 мм та зовнішній діаметр приблизно 100мм.

Опір обох кабелів має однакове значення,та складає приблизно 50 Ом.

Коаксіальний кабель раніше був досить широко розповсюдженим,але на сьогоднішній день їх витіснили волоконно-оптичні кабелі,та вита пара.

2.7 Висновки

В розділі було проаналізовано наявні та доступні засоби для ямоделювання та дослідження мереж. Із запропонованоих варіантів було обрано продукт Packet Tracer від компанії Cisco Systems, оскільки він дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори та комутатори, взаємодіяти між кількома користувачами (через хмару).

У симуляторі реалізовані серії маршрутизаторів Cisco 2900 і комутаторів Cisco Catalyst 2950, а також міжмережевий екран ASA 5505, що будуть використовуватись фізично при побудові мережі. Крім того є імітації серверів DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP та EMAIL, робочі станції, різні модулі до комп'ютерів та маршрутизаторів, IP-фони, смартфони, хаби, а також хмара, що емулює WAN.

Це дає змогу успішно створювати складні макети мереж, перевіряти на працездатність топологію мережі та переносити готові конфігураційні файли на реальні пристрої.

3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ НАУКОВОЇ БІБЛІОТЕКИ

3.1 Налаштування мережевого обладнання наукової бібліотеки

Підібране і розміщене обладнання з розділів 1 та 2 необхідно налаштувати і підготувати до роботи.

Першим етапом налаштування мережевого обладнання є налаштування файєрвола ASA 5506.

Рисунок 3.1 – початкове налаштування ASA

Створення VLAN:

```
ASA (config)# vlan 10
ASA (config-vlan)# name 10
ASA (config-vlan)# exit
```

Налаштування портів ASA:

```
ASA (config)# interface 1
ASA (config-if)# switchport mode access
ASA (config-if)# switchport access vlan 10
ASA (config-if)# exit
```

Налаштування підінтерфейсу ASA для кожної VLAN:

```
ASA(config)# interface GigabitEthernet0/0
ASA(config-if)# nameif 10
ASA(config-if)# security-level 100
ASA(config-if)# ip address 192.168.0.1 24
ASA(config-if)# no shutdown
ASA(config-if)# exit
```

Додавання маршруту за замовчуванням:

ASA(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1

Налаштування ACL:

ASA(config)# access-list indns extended permit tcp 0.0.0.0 192.168.0.1

Налаштування NAT:

ASA(config)# object network object_1

ASA(config-network-object)# subnet 192.168.0.1 24

ASA(config)# nat (inside,outside) dynamic interface

Застосування ACL до інтерфейсу:

ASA(config)# access-group indns in interface GigabitEthernet0/0

Збереження налаштувань:

ASA(config)# write memory

Налаштування вхідного маршрутизатора.

Першим етапом потрібно створити VLAN на маршрутизаторі, для чого потрібно додати їх до бази даних.

vlan database

vlan 20

vlan 21

vlan 22

vlan 23

vlan 24

vlan 25

vlan 26

vlan 30

vlan 40

exit

Потрібно провести налаштування інтерфейсів VLAN.

interface GigabitEthernet0/1

switchport mode access

switchport access vlan 20

exit

interface GigabitEthernet0/2

switchport mode access

switchport access vlan 21

exit

Відповідні налаштування потрібно провести для усіх VLAN.

Проводиться налаштування підінтерфейсів для VLAN на порту маршрутизатора:

interface GigabitEthernet0/0

no shutdown

interface GigabitEthernet0/0.10

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 21

ip address 192.168.21.1 255.255.255.0

exit

exit

Налаштування NAT:

ip nat inside source list 1 interface GigabitEthernet0/1 overload

ip nat inside source static tcp 192.168.20.1 80 interface GigabitEthernet0/1 80

ip nat inside source static tcp 192.168.21.1 80 interface GigabitEthernet0/1 80

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.21.0 0.0.0.255

interface GigabitEthernet0/1

ip nat outside

exit

Аналогічні налаштування необхідно провести на решті маршрутизаторів, що створюють ядро мережі.

enable

configure terminal

hostname Switch1

Цей набір команд дозволяє змінювати налаштування комутатора та задає його ім’я.

Аналогічно до вхідного маршрутизатора в базу даних комутатора вносяться номери VLAN.

vlan database

vlan 20

vlan 21

…

Далі, так само як і на маршрутизаторі прив’язуються VLAN до відповідних портів.

Наступним етапом є налаштування тегованого порту для зв’язку з маршрутизатором.

interface GigabitEthernet0/24

switchport mode trunk

switchport trunk allowed vlan all

exit

налаштування завершується встановленням IP адреси комутатора та збереженням налаштувань.

interface Vlan1

ip address 192.168.0.5 255.255.255.0

exit

end

write memory

виконання цих команд забезпечує налаштування комутатора.

3.2 Вимірювання продуктивності мережі

Вимірювання продуктивності мережі передбачає використання метрик.

До таких метрик можна віднести:

- швидкість передачі даних. Вимірювання пропускної здатності мережі шляхом передачі файлів різного розміру та запису часу, необхідного для завершення передачі. Використання такої метрики передбачає тестування готової мережі та дозволяє оцінити якість вибору та налаштування мережевого обладнання та пропускну здатність каналів зв’язку.
- Затримка передачі пакету. Вимірювання часу затримки між двома вузлами мережі. Це можна зробити за допомогою утиліти ping, яка надає інформацію про час, необхідний для відправки пакету даних від одного вузла до іншого та повернення його. Оцінку затримок в мережі можна провести як на реальній мережі так і на її моделі.
- Втрата пакетів. Вимірювання кількості втрачених пакетів під час передачі даних. Це можна зробити за допомогою утиліти ping або спеціальних інструментів, таких як traceroute, які дають змогу відстежувати маршрут пакетів і визначати місце втрати. Можна провести на реальній мережі, є інформативним у випадку неналежного конфігурування мережі. За мови відсутності критичних помилок може бути інформативним лише за умови значного завантаження каналів передачі даних. Зазвичай для працездатних мереж не застосовується.
- Пропускна здатність. Вимірювання фактичної швидкості передачі даних через мережу. Це можна здійснити за допомогою інструментів, таких як iPerf або вбудованих засобів моніторингу мережевого обладнання. Може бути реалізовано виключно на реальній мережі.

- Вимірювання навантаження. Застосування спеціальних інструментів, таких як Apache JMeter або Gatling, для створення імітованого трафіку на мережевому обладнанні та вимірювання продуктивності під навантаженням. Вимірювання за цією метрикою може бути реалізоване на реальній мережі.

З метою перевірки продуктивності мережі використаємо метрику «Затримка передачі пакету». Результати тестування представлено в таблиці 3.1.

Таблиця 3.1 – Перевірка продуктивності мережі метрикою «Затримка передачі пакету»

Джерело / Отримувач	Система відеоспостереження	Серверна (DMZ)	Читальний зал №1	Читальний зал №2	Адміністрації	Бібліотекарі	Закритий Wi-Fi	Публічний Wi-Fi	Зовнішня мережа
Система відеоспостереження	*	3мс	-	-	+	-	-	-	-
Серверна (DMZ)	-	*	4мс	4мс	3мс	3мс	24мс	26мс	10мс
Читальний зал №1	-	-	*	-	-	4мс	-	-	11мс
Читальний зал №2	-	-	-	*	-	4мс	-	-	-
Адміністрація	-	-	-	-	*	-	25мс	-	-
Бібліотекарі	-	-	-	-	4мс	*	26мс	-	-

Отримані результати тестування показують прийнятні значення метрики, які зазвичай, є типовими для комп’ютерних мереж такого класу.

3.3 Тестування розмежування доступу в мережі

Тестування розмежування доступу в мережі зазвичай включає перевірку правильності налаштування правил файєрвола, контролю доступу до ресурсів та рівня безпеки мережевих сегментів.

Зазвичай таке тестування проводиться в декілька етапів:

- перевірка правил файєрвола;
- перевірка контролю доступу;
- перевірка безпеки мережевих сегментів, а саме обмежень доступів між VLAN.

Виконання сканування відкритих портів на вхідному інтерфейсі файєрвола командою nmap -p 0-65535 10.10.90.1 показало, що відкритими є лише порти, які перенаправляються до серверів в демілітаризовану зону. Файєрвол та вхідний маршрутизатор не мають відкритих вхідних портів та адмініструються виключно з внутрішньої мережі.

Перевірка контролю доступу передбачає запуск утиліти ping з кожного vlan, включаючи зовнішній, до ресурсів мережі. Результати виконання утиліти ping представлені в таблиці 3.2.

В результаті проведеного тестування можна зробити висновок, що правила фільтрації трафіку між VLAN збудовані правильно, та забезпечують виконання поставлених на завдань. Такий набір правил мінімізує ймовірність проведення хакерських атак на інфраструктуру бібліотеки, оскільки як внутрішні так і зовнішні користувачі мають доступ до серверів виключно через дозволені для веб-доступу порти.

Таблиця 3.2 – Тестування доступності між VLAN в мережі бібліотеки

З мережі / Доступний ресурс	Система відеоспостереження	Серверна (DMZ)	Читальний зал №1	Читальний зал №2	Адміністрація	Бібліотекарі	Закритий Wi-Fi	Публічний Wi-Fi	Зовнішня мережа
1	2	3	4	5	6	7	8	9	10
Система відеоспостереження	*	+	-	-	+	-	-	-	-
Веб-сервер	-	*	+	+	+	+	+	+	+
DNS-сервер	-	*	+	+	+	+	+	-	-
DHCP-сервер	-	*	+	+	+	+	+	+	-
FTP-сервер	-	*	+	+	+	+	+	-	-
Читальний зал №1	-	-	*	-	-	+	-	-	-
Читальний зал №2	-	-	-	*	-	+	-	-	-
Адміністрація	-	-	-	-	*	-	+	-	-
Бібліотекарі	-	-	-	-	+	*	+	-	-

Таблиця 3.2 (Закінчення) – Тестування доступності між VLAN в мережі бібліотеки

1	2	3	4	5	6	7	8	9	10
Закритий Wi-Fi	-	-	-	-	+	+	*	-	-
Публічний Wi-Fi	-	-	-	-	-	-	-	*	+
Зовнішня мережа	-	-	+	+	+	+	+	+	*

Користувачі мережі мають доступи до внутрішніх ресурсів мережі, обґрунтовані виключно потребою навчання або виконання посадових обов'язків.

3.4 Адресація у мережі та фінансова частина

У таблиці 3.3 представлено схему адресації для пристроїв, що входять до складу розроблюваної мережі.

Таблиця 3.3 – Таблиця адрес у мережі

PC	IP-адреса	SWITCH	IP-адреса
PC-0	192.168.1.8	SWITCH-1	192.168.1.1
PC-1	192.168.1.10	SWITCH-2	192.168.2.2
PC-2	192.168.1.15	SWITCH-3	192.168.1.3

Підрахунок вартості спроектованої мережі відбувався за цінами, взятими з «Rozetka.ua». Інсталяцію програмного забезпечення, збірку та налаштування устаткування, прокладання мережі виконується спеціалістами та фірмою потстачальником, тому вартість цих послуг не враховується.

Таблиця 3.4 – Перелік комплектуючих для робочих комп’ютерів.

Пристрій	Марка і модель	Ціна грн.
Процесор	Intel Core i3-4130 (BX80646I34130) LGA1150, 2 ядра, 3.4GHz	8800
Материнська плата	EliteGroup (ECS) H81H3- M4(HDMI)	1300
Оперативна пам'ять	TEAM 4 GB DDR3 1600 MHz	900
Вінчестер	500 Gb Toshiba DT01ACA050 SATA rev. 3.0	1618
Монітор	21,5" Lenovo LI2221sw	3156
Клавіатура	Maxxtro KB-107U, USB	150
Мишка	Defender Dacota MS-155 бездротова USB	250
Корпус	Linkworld M06 400W	440
Всього: 19092 грн		

Вартість 8 робочих комп’ютерів складає: 8 * 19092грн = 152 736 грн.

Таблиця 3.5 – Перелік активного мережевого обладнання

Пристрій	Марка	Ціна грн.
Комутатор	TP-LINK TL-SG1024DE	2999
Роутер	Oltec AHD-KIT; TP-Link TL-WR940N,	7600, 1650
Мережевий принтер	Epson Expression Home XP-3100	2499
Камери відеонагляду	Oltec AHD-KIT-311	1569

Вартість 6 камер відеонагляду 8*1569грн=12552грн

Вартість 3 роутерів 1650грн*3+7600=12550 грн

Вартість за 3 комутатори 2999грн*3=9000грн

Загальна вартість активного мережевого обладнання – 36 749 грн

Таблиця 3.6 – Вартість пасивного мережевого обладнання

Назва	Ціна	Кількість	Вартість
Прямий кабель	8 грн	300 м	2400 грн
Коаксіальний кабель	20 грн	3м	60 грн

Загальна вартість пасивного мережевого обладнання – 2460 грн

Вимоги до обладнання :

- 14 комутаторів (комутатор Cisco 2950);
- 1 маршрутизатор (Cisco 12811router);
- IP-телефон;
- бездротовий маршрутизатор.

3.5 Висновки

У розділі було розроблено логічну та фізичну тополгії мережі бібліотеки, розроблено схему адресації та сегментації мережі, виконано конфігурування мережних пристроїв відповідно до обраної схеми адресації. Виконано тестування та перевірку проходження трафіку мережею. Виконано вибір та розраховано вартість впровадження даної мережі.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було проаналізовано і досліджено предметну область, теоретичну інформацію про проєктування комп'ютерних мереж. Автором дослідження була спроєктована, розроблена та реалізована комп'ютерна мережа бібліотеки з ціллю налаштування пристроїв захисту інформації бібліотеки від небажаного злому.

Було проведено огляд наявних засобів для моделювання та дослідження мереж та обрано в якості такого пакет Packet Tracer від компанії Cisco. За допомогою нього було розроблено фізичну та логічну схеми мережі, виконано налаштування пристроїв безпеки, налаштування комутаторів, маршрутизаторів, кінцевих пристроїв, для забезпечення проходження дозволеного та блокованого трафіку.

Результати тестування мережного трафіку показали коректність та правильність налаштування пристроїв для забезпечення параметрів безпеки мережі.

Вимоги до мережі виконано у повному обсягу. Розроблена мережа має широкий простір для удосконалення, доповнення, розширення та модернізації згідно з побажаннями замовника.

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ

1 Стасєв Ю.В. Комп’ютерні мережі. Технології, протоколи та моделювання: навчал. посібн. / І.В. Рубан, С.В. Дуденко, О.І. Тимочко. – Х.: ХУПС, 2019. – 359 с

2 Корпоративна мережа. URL: http://wikipedia.ua.nina.az/wiki/%D0%9A%D0 (дата звернення 01.06.2023)

3 Трояновська Т. І. Корпоративна мережа, як засіб організації роботи підприємства URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/viewFile/1844/1562 (дата звернення 01.05.2023).

4 Computer Network Architecture. URL: https://www.javatpoint.com/computer-network-architecture (дата звернення: 23.04.2023)

5 Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. Львів, «Магнолія 2006», 2016. 256 с.

6 Коробейнікова Т. І., Захарченко С. М. Комп'ютерна мережа. Львів : Вид-во Львів. політехніки, 2022. 228 с.

7 Принципи побудови і призначення комп’ютерних мереж. URL: https://tdmuv.com/kafedra/internal/informatika/classes_stud/uk/nurse/and/03.Принципи%20побудови%20і%20призначення%20компютерних%20мереж.html (дата звернення: 24.04.2023)

8 Hierarchical Network Model. URL: https://networkdirection.net/articles/network-theory/hierarchicalnetworkmodel/ (дата звернення: 30.04.2023)

9 Що таке демілітаризована зона (DMZ)?. URL: https://uk.itpedia.nl/2023/01/28/wat-is-een-demilitarized-zone-dmz (дата звернення: 30.04.2023)

10 Stateful inspection URL: https://www.techtarget.com/searchnetworking/definition/stateful-inspection. – (дата звернення 01.06.2023).

11 Ліхтарников О.М, Хорошко М.П, Слободяник В.О. Основи комп'ютерних мереж: навчальний посібник. Київ : Ленвіт, 2018. 320 с.

12 Демілітаризована зона URL: http://nickshevtsov.blogspot.com/2017/11/blog-post_86.html (дата звернення 01.05.2023).

13 DMZ Network: How It Works, Its Uses, and Benefits in Network Security. URL: https://www.linkedin.com/pulse/dmz-network-how-works-its-uses-benefits-security-valdemar-závadský (дата звернення: 10.05.2023)

14 Організація комп'ютерних мереж «демілітаризована зона» URL: https://kremenetskyy.blogspot.com/2017/11/blog-post.html (дата звернення 25.05.2023).

15 DMZ URL: https://www.fortinet.com/resources/cyberglossary/what-is-dmz (дата звернення 07.05.2023)

16 Gary A. Donahue Network Warrior / Gary A. Donahue. – Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2011. – 627 p.

17 Cisco IOS. URL: https://docs.oracle.com/en-us/iaas/Content/Network/Reference/ciscoiosCPE.htm (дата звернення: 28.04.2023)

18 Tanenbaum A.S, Wetherall D.J. Computer networks. Pearson, 2010. 960 p.

19 Основні вимоги до проектування кампусних мереж. URL: https://studfile.net/preview/5199546/page:2/ (дата звернення: 15.05.2023)

20 Yanko A., Vyhivskyi R. Система захисту комп'ютерної мережі. Системи управління, навігації та зв'язку. Збірник наукових праць. 2022. Т. 2, № 68. С. 91–94. URL: https://doi.org/10.26906/sunz.2022.2.091 (дата звернення: 10.05.2023)

21 Комп'ютерні мережі. URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 (дата звернення: 16.05.2023)

22 Тарбаєв С.І. Проектування інфокомунікаційних мереж. 2015. 268 с.

23 Мережева модель OSI URL: https://uk.wikipedia.org/wiki/Мережева_модель_OSI. (дата звернення 01.05.2023)

24 Топології комп’ютерних мереж. URL: http://blogkkzshnika.blogspot.com/2017/10/blog-post_10.html (дата звернення: 17.05.2023)

25 Hari Subedi. A guide to network topology: 2020 URL: https://www.itjones.com/blogs/2020/11/22/a-guide-to-network-topology (дата звернення: 17.05.2023)

26 Топологія комп'ютерних мереж. URL: https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh (дата звернення: 17.05.2023)

27 Організація комп'ютерних мереж. URL: http://nickshevtsov.blogspot.com/2017/10/blog-post.html (дата звернення: 17.05.2023)

28 Канальний рівень моделі OSI URL: https://static-course-assets.s3.amazonaws.com/ITE50UK/course (дата звернення 01.05.2023).

29 Канальний рівень моделі OSI URL: https://uk.wikipedia.org/wiki/Канальний_рівень. (дата звернення 01.05.2023)

30 Комутатор URL: https://uk.wikipedia.org/wiki/Мережевий_комутатор. (дата звернення 01.05.2023).

31 Що таке корпоративний сервер? URL: https://uk.icyscience.com/enterprise-server (дата звернення 25.05.2023).

32 Топологія локальних мереж. URL: https://ua5.org/lan/125-topologja-lokalnikh-merezh.html (дата звернення: 17.05.2023)

33 David Scott The IT Professional's Guide To Corporate Networks URL: https://www.techopedia.com/the-it-professionals-guide-to-corporate-networks/2/25665 (дата звернення: 18.05.2023)

34 Топологія комп’ютерних мереж. Класифікація комп’ютерних мереж з топології. URL: https://creativnost.com.ua/topologiya-kompyuternix-merezh-klasifikaciya-kompyuternix-merezh-z-topologii/ (дата звернення: 18.05.2023)

35 Топологія мережі: 6 пояснених та порівняних мережевих топологій. URL: https://instagalleryapp.com/chistij-administrator-2/topologija-merezhi-6-pojasnenih-ta-porivnjanih/ (дата звернення: 18.05.2023)

36 Докучаєв А.В, Засов А.В, Казакевич П.В. Інформаційна безпека комп'ютерних систем: навчальний посібник. Київ : Наук. думка, 2017. 152 с.

37 Інформаційні мережі / Полоневич О.В та ін. Київ, 2019. 94 с.

38 Setting up an FTP Server URL: https://www.ocf.berkeley.edu/reinholz/freebsd/ftp.html (дата звернення 15.05.2023).

39 Kim D.J, Solomon, M.G. Network security bible. Wiley, 2019. 816 с.

40 Vulnerabilities of network OS and mitigation withstate-based permission system [Electronic resource] / J. Noh, S. Lee, J. Park, S. Shin, B. B. Kang // Graduate School of Information Security, School of Computing, Korea Advanced Institute of Science and Technology, Daejeon, Korea. – URL: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1369 (дата звернення: 18.05.2023)

41 Методика розрахунку конфігурації мережі Ethernet URL: http://um.co.ua/7/7-8/7-87320.html (дата звернення 25.05.2023).

42 Configuring dynamic NAT in Cisco devices URL: https://www.manageengine.com/network-configuration-manager/configlets/configure-dynamic-nat-cisco.html (дата звернення: 18.05.2023)

43 Configuring IP Access Lists URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html (дата звернення: 18.05.2023)

44 How to Enable SSH on Cisco Switch, Router and ASA URL: https://www.thegeekstuff.com/2013/08/enable-ssh-cisco/ (дата звернення: 18.05.2023)

45 Whitman M. E, Mattord H. J. Principles of information security. 7-ме вид. Cengage Learning, 2018. 658 p.

ДОДАТОК А

(обов'язковий)

Налаштування брандмауера Cisco ASA 5506-х

```
ASA Version 9. 6(1)
!
hostname ASA
domain-name ASA. com names
!
interface GigabitEthernet1/1 description LAN1
nameif LAN1 security-level 95
ip address 192. 168. 6. 1 255. 255. 255. 0
!
interface GigabitEthernet1/2 description LAN2
nameif LAN2 security-level 95
ip address 10. 0. 3. 1 255. 255. 255. 0
!
interface GigabitEthernet1/3 nameif DMZ
security-level 50
ip address 10. 0. 1. 1 255. 255. 255. 0
!
interface GigabitEthernet1/4 description to CorporateRouter nameif outside
security-level 0
ip address 10. 0. 2. 2 255. 255. 255. 252
!
interface GigabitEthernet1/5 no nameif
no security-level no ip address shutdown
!
interface GigabitEthernet1/6 no nameif
no security-level no ip address shutdown
!
interface GigabitEthernet1/7 no nameif
no security-level no ip address shutdown
!
interface GigabitEthernet1/8 no nameif
no security-level no ip address shutdown
```

!

interface Management1/1 management-only

no nameif

no security-level no ip address shutdown

!

!

route outside 0. 0. 0. 0 0. 0. 0. 0 10. 0. 2. 1 1

!

access-list FROM-LAN1 extended deny ip 192. 168. 6. 0 255. 255. 255. 0 10. 0. 1. 0

255. 255. 255. 0

access-list FROM-LAN1 extended deny ip 192. 168. 6. 0 255. 255. 255. 0 10. 0. 3. 0

255. 255. 255. 0

access-list FROM-LAN1 extended permit ip 192. 168. 6. 0 255. 255. 255. 0 any

access-list FROM-OUTSIDE extended permit icmp any 192. 168. 6. 0 255. 255. 255. 0 echo- reply

access-list FROM-OUTSIDE extended permit icmp any 10. 0. 3. 0 255. 255. 255. 0 echo-reply
access-list FROM-OUTSIDE extended permit icmp any 10. 0. 1. 0 255. 255. 255. 0 echo-reply
access-list FROM-OUTSIDE extended permit tcp any eq www any

access-list FROM-OUTSIDE extended permit tcp any eq 433 any

access-list FROM-OUTSIDE extended permit tcp any 10. 0. 1. 0 255. 255. 255. 0 eq www access-list FROM-OUTSIDE extended permit tcp any 10. 0. 1. 0 255. 255. 255. 0 eq 443 access-list FROM-LAN2 extended deny ip 10. 0. 3. 0 255. 255. 255. 0 10. 0. 1. 0 255. 255. 255. 0

access-list FROM-LAN2 extended deny ip 10. 0. 3. 0 255. 255. 255. 0 192. 168. 6. 0

255. 255. 255. 0

access-list FROM-LAN2 extended permit ip 10. 0. 3. 0 255. 255. 255. 0 any

access-list FROM-DMZ extended deny ip 10. 0. 1. 0 255. 255. 255. 0 10. 0. 3. 0 255. 255. 255. 0

access-list FROM-DMZ extended deny ip 10. 0. 1. 0 255. 255. 255. 0 192. 168. 6. 0

255. 255. 255. 0

access-list FROM-DMZ extended permit ip 10. 0. 1. 0 255. 255. 255. 0 any

!

!

access-group FROM-LAN1 in interface LAN1 access-group FROM-OUTSIDE in interface outside
access-group FROM-LAN2 in interface LAN2 access-group FROM-DMZ in interface DMZ

!

aaa authentication ssh console LOCAL

!

username admin password pqrZ2iqRGgDD9cbU encrypted

!

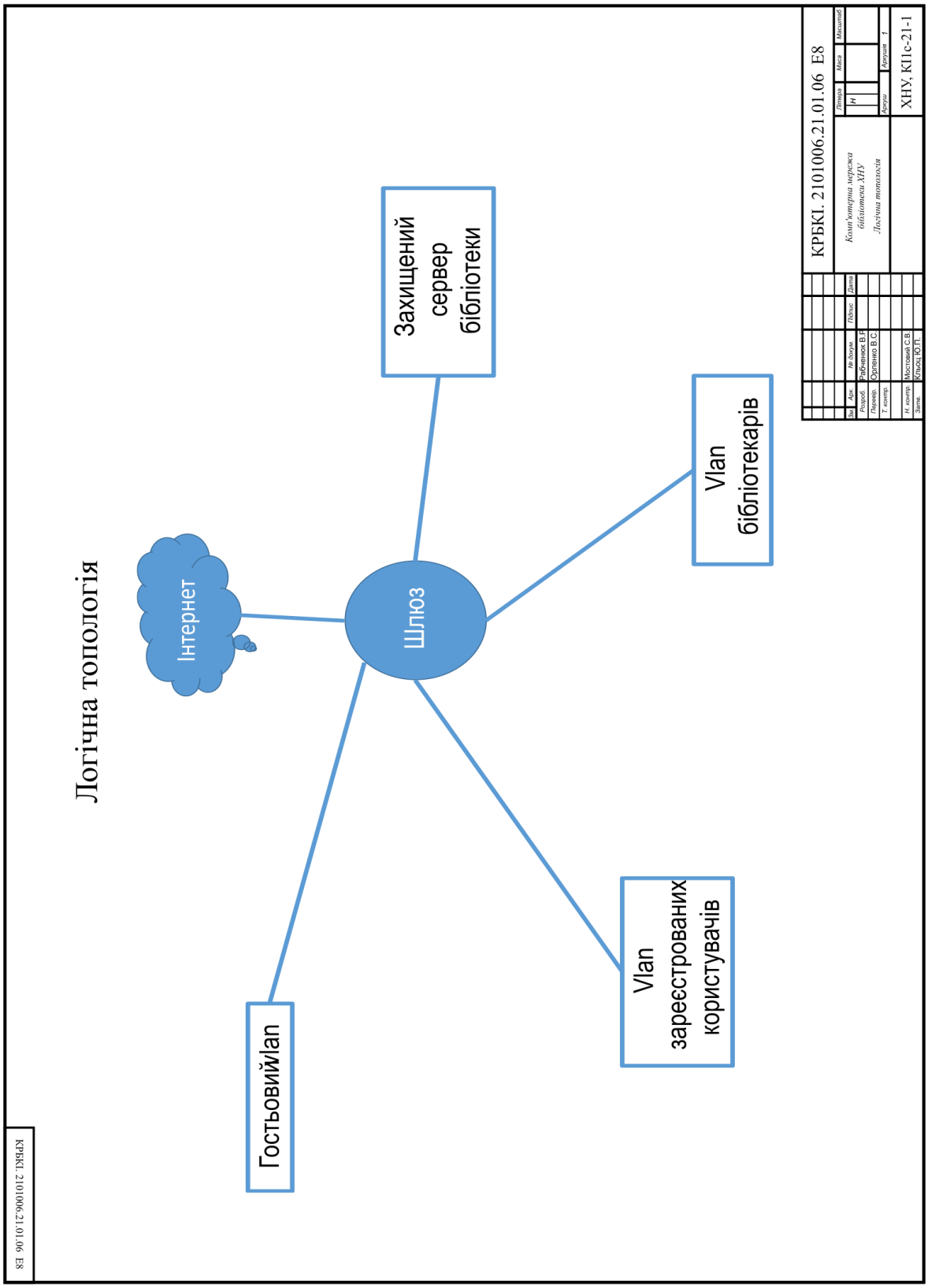
class-map inspection_default match default-inspection-traffic

```
!
policy-map global_policy class inspection_default inspect http
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh 10. 0. 3. 0 255. 255. 255. 0 LAN2
ssh 192. 168. 6. 0 255. 255. 255. 0 LAN1
ssh timeout 5
!
```

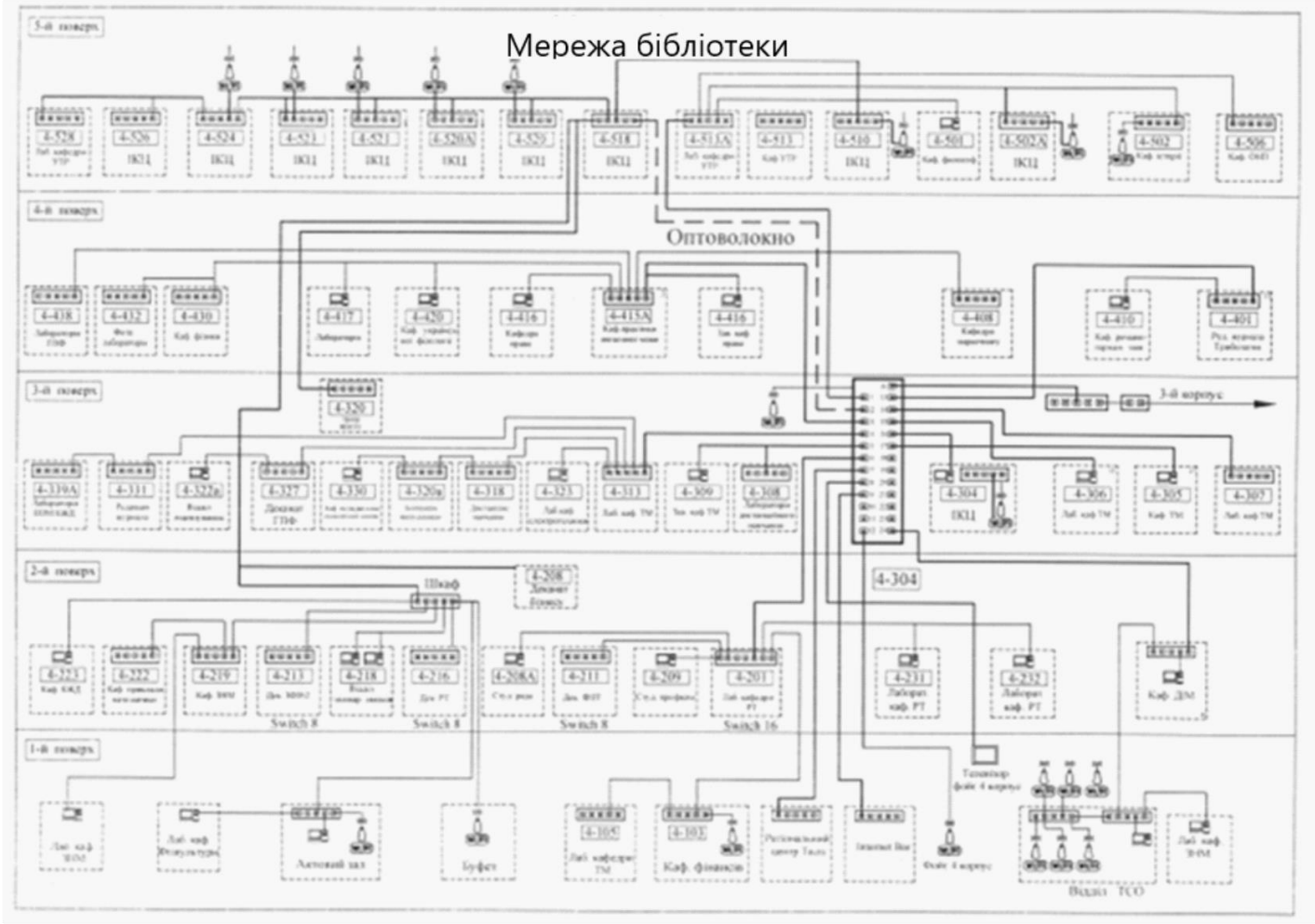
ДОДАТОК Б

(обов'язковий)

Копія графічної частини



Фізична топологія

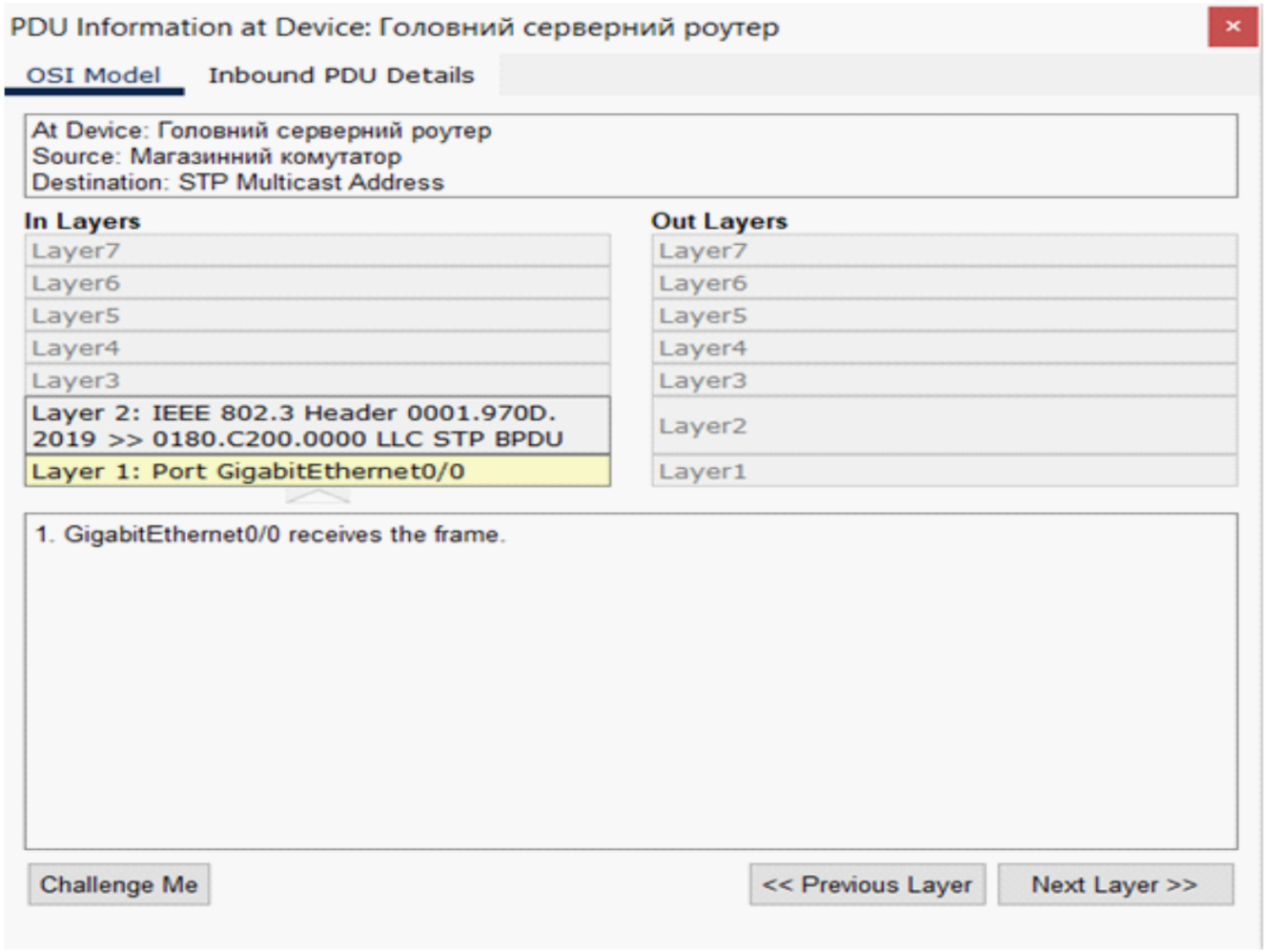


					КРБКІ. 2101006.21.01.06 Е8
Зм.	Арк.	№ докум.	Підпис	Дата	Комп'ютерна мережа бібліотеки ХНУ Фізична топологія
Розроб.		Рабченюк В.Р.			
Перевір.		Орленко В.С.			
Т. контр.					
Н. контр.		Мостовий С.В.			
Затв.		Кльоц Ю.П.			

Літера	Маса	Масштаб
Н		
Аркуш	Аркушів 1	

ХНУ, КІ1с-21-1

Тестування моделі мережі



Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1		Завдання на кваліфікаційну	1	
				роботу		
А4		2		Анотація	1	
А4		3	КРБКІ. 2101006.21.01.06 ПЗ	Комп'ютерна мережа	63	
				наукової		
				бібліотеки ХНУ		
				Пояснювальна записка		
А2		4	КРБКІ. 2101006.21.01.06 Е8	Логічна топологія	1	
А2		5	КРБКІ. 2101006.21.01.06 Е8	Фізична топологія	1	

Зм.	Арк.	№ Докум.	Підп.	Дата	КРБКІ. 2101006.21.01.06 ВП		
Розробив		Рабченюк В.Р.			Комп'ютерна мережа наукової бібліотеки ХНУ Відомість проєкту	Літера	Аркуш 1 / Аркушів 1
Перев.		Орленко В.С.				н	
Н. контр.		Мостовий С.В.				ХНУ, КІ1с-21-1	
Затв.		Кльоц Ю.П.					

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015975242

Дата перевірки:
06.12.2023 10:20:47 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2023 10:45:16 EET

ID користувача:
100008300

Назва документа: Рабченюк_**плагіат**

Кількість сторінок: 63 **Кількість слів:** 14800 **Кількість символів:** 118285 **Розмір файлу:** 2.86 MB **ID файлу:** 1015654798

1.07%
Схожість

Найбільша схожість: 0.46% з Інтернет-джерелом (https://el-conf.com.ua/wp-content/uploads/2020/04/8%D1%87%D0%B...

0.82% Джерела з Інтернету	137	Сторінка 80
0.54% Джерела з Бібліотеки	47	Сторінка 80

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	2

Wed Jun 26 09:49:00 EEST 2024, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

	Документ		Сумарний збіг по Базі Даних	
ID: 132631 Назва: Комп'ютерна мережа наукової бібліотеки ХНУ Додано в БД: 2024-06-26 Автора: Рабченюк В.Р. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	59224	539	591 (1%)	5 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Комп'ютерна мережа наукової бібліотеки ХНУ

Автор: Рабченюк Валентин Русланович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: Програмування та захист комп`ютерних систем і мереж

Науковий керівник: Орленко В.С.

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1.20% і адресується до 138 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи В.С. Орленко

Завідувач кафедри КБ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Рабченюк Валентин Русланович
Тема: «Комп'ютерна мережа наукової бібліотеки ХНУ»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 123 «*Комп'ютерна інженерія*» Освітня програма «Програмування та захист комп'ютерних систем і мереж»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 67;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою комп'ютерної мережі з розмежуванням доступу. Для досягнення цієї мети було проведено аналіз топологій мереж та підходи до розмежування доступу. Створено і розроблену мережу, яка дозволяє забезпечити надійну роботу мережі з гарантованими затримками та належним рівнем безпеки. Робота має на меті забезпечити належний рівень доступу до ресурсів мережі всіма співробітниками та відвідувачами бібліотеки та мінімізувати ризики витоку персональних даних.
2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Комп'ютерна інженерія», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз вимог та засобів до проектування мережі бібліотеки. У другому розділі розроблено політики безпеки та правила розмежування доступу користувачів. Обґрунтовано вибір топології мережі та способу підключення кінцевих пристроїв. Розроблено логічну та фізичну топології мережі. У третьому розділі проведено налаштування мережевого обладнання бібліотеки, здійснено вимірювання продуктивності роботи мережі та перевірено відповідні доступи.
4. Позитивні сторони кваліфікаційної роботи полягають у тому що, застосування розробленої мережі забезпечить гарантований доступ користувачів мережі як до локальних ресурсів бібліотеки, доступу до бібліотек-партнерів, ресурсів, що розміщені в хмарних сервісах та до інтернету. Використання обґрунтованих політик та обмеження в доступах до ресурсів забезпечують високу швидкість доступу до ресурсів бібліотеки при недопущенні несанкціонованого доступу до ресурсів бібліотеки, що в свою чергу, сприяє покращенню якості обслуговування та дотримання авторських прав.

5. Негативні сторони проекту: варто приділити більше уваги налаштуванню обмежень доступу та обґрунтувати прийняті рішення

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Слід відмітити деяку непослідовність роботи, що не дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці не достатньо наглядних пояснень, та деякі розділи варто розширити. Графічний матеріал не в повному обсязі дозволяє побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «задовільно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 5 » червня 2023 . (підпис)