

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Комп'ютерних наук і технологій
(повне найменування факультету)

Комп'ютерні системи та мережі
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

бакалаврський
(ступінь вищої освіти)

на тему ПРОЄКТУВАННЯ РОЗПОДІЛЕНОЇ МЕРЕЖІ БІБЛІОТЕК МІСТА
З ВИКОРИСТАННЯМ VLAN ТА VPN

Виконав: студент 4 курсу, групи КНТ-512
Спеціальності 123 Комп'ютерна інженерія
(код і найменування спеціальності)

Освітня програма (спеціалізація) _____
Комп'ютерна інженерія

ШЛАПІК О. А.
(прізвище та ініціали)

Керівник КИРИЧЕК Г.Г.
(прізвище та ініціали)

Рецензент ТЯГУНОВ Д. В.
(прізвище та ініціали)

м. Запоріжжя
2026 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
 (повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій
 Кафедра комп'ютерних систем та мереж
 Ступінь вищої освіти бакалаврський
 Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
 Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри КУДЕРМЕТОВ Р.К.

«14» квітня 2026 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ШЛАПКУ Олексію Андрійовичу

(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Проектування розподіленої мережі бібліотек міста з використанням VLAN та VPN

керівник проєкту (роботи) к.т.н., доцент, КИРИЧЕК Г.Г.

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від « 14 » квітня 2026 року № 160

2. Строк подання студентом проєкту (роботи) 01.06.2026 р.

3. Вихідні дані до проєкту (роботи) Технічне завдання на розробку мережі бібліотек міста на базі стандартів IEEE 802.1Q і IEEE 802.1ad. Технології, що використовуються: FastEthernet, GigabitEthernet, VLAN. Протоколи: OSPF, STP, DHCP. Стандарти: 100BASE-TX, 1000BASE-TX, IEEE 802.1Q, IEEE802.1ad. Виробники обладнання: Cisco, Panduit, D-Link. Обладнання: маршрутизатори Cisco 7201 (11 шт), комутатори Cisco Catalyst 9300 (45 шт), ПК (237 шт), сервер (3 шт). Програмне забезпечення: Cisco Packet Tracer.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз технічного завдання. Вибір технологій та мережевого обладнання. Проектування мережі бібліотек міста. Налаштування мереж і міжмережевих з'єднань.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Слайди презентації

6. Консультанти розділів проекту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	приймав виконане завдання
1-4	КИРИЧЕК Г.Г.		
Нормоконтроль	ДЬЯЧУК Т.С.		

7. Дата видачі завдання «14» квітня 2026 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	18.04.2026	
2	Визначення та аналіз вимог до структури мережі бібліотек міста	22.04.2026	
3	Проектування моделі. Постановка завдань	24.04.2026	
4	Вибір технологій та обладнання	28.04.2026	
5	Розробка структурної схеми мережі	01.05.2026	
6	Проектування мережі в системі моделювання	05.05.2026	
7	Налаштування мережевих з'єднань в бібліотеках міста	12.05.2026	
8	Налаштування міжмережевих з'єднань	22.05.2026	
9	Оформлення пояснювальної записки	25.05.2026	
10	Проходження нормоконтролю	27.05.2026	
11	Перевірка на наявність академічного плагіату	28.05.2026	
12	Проходження рецензування	01.06.2026	

Студент(ка)

(підпис)

Олексій ШЛАПІК

(Ім'я ПРІЗВИЩЕ)

Керівник проекту (роботи)

(підпис)

Галина КИРИЧЕК

(Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:
74 с., 15 табл., 21 рис., 2 дод., 21 джерело.

КОРПОРАТИВНА МЕРЕЖА, ТОЧКА ДОСТУПУ, КОМУТАТОР,
МАРШРУТИЗАТОР, МАРШРУТИЗАЦІЯ, МЕРЕЖЕВА БЕЗПЕКА, VPN,
ETHERNET, 1000BASE-LX, VLAN, WLAN

Об'єктом розробки є процес проєктування інформаційно-комунікаційної мережі міських бібліотек та організації розподіленої мережевої інфраструктури з використанням VLAN та VPN.

Метою роботи є проєктування архітектури та впровадження принципів організації розподіленої мережі бібліотек міста з використанням технологій VLAN і VPN, що забезпечить ефективну організацію мережевих сервісів, підвищення продуктивності обміну даними та покращення рівня інформаційної безпеки.

Предметом є методи, моделі, мережеві стандарти та технології проєктування, моделювання, конфігурації та оптимізації комп'ютерних мереж.

Технології комп'ютерних мереж для реалізації загальних сегментів мережі: VLAN, FastEthernet та GigabitEthernet, з підтримкою стандартів IEEE 802.1Q і IEEE 802.1ad, 100BASE-TX, 1000BASE-LX. Протоколи: STP, OSPF, DHCP, DNS. Виробники обладнання: Cisco, Panduit, Dell, HP, D-Link. Обладнання: маршрутизатори, комутатори, точки доступу, мережеві принтери, персональні комп'ютери, термінали збору даних, патч-панелі, мережеві розетки, кабельні організатори, комутаційні стійки.

ЗМІСТ

Вступ.....	6
Скорочення та умовні позначки	8
1 Аналіз технічного завдання	9
1.1 Актуальність теми та аналіз структури.....	9
1.2 Вимоги до сучасної розподіленої бібліотечної мережі	13
1.3 Аналіз подібних рішень і технологій	14
1.4 Постановка завдань	17
2 Вибір технологій та мережевого обладнання	19
2.1 Технології каналного рівня (Ethernet, Wi-Fi 6)	19
2.2 Технологія VLAN, особливості використання	22
2.3 VPN-рішення	26
2.4 Технології та протоколи маршрутизації	30
2.5 Серверні технології (Linux/Windows Server, віртуалізація).....	33
2.6 Системи зберігання даних (NAS/SAN)	35
3 Проектування мережі бібліотек міста	37
3.1 Логічна структура мережі	37
3.2 Мережеве обладнання та апаратна інфраструктура	40
3.3 Структурна схема мережі	43
4 Налаштування мереж і міжмережових з'єднань.....	45
4.1 Поетапне впровадження VLAN у мережі бібліотечної системи	45
4.2 Налаштування access-комутаторів та маршрутизації.....	53
4.3 Додаткові налаштування безпечних підключень	56
4.4 Налаштування VPN IPSec	59
Висновки.....	64
Перелік джерел посилання	65
Додаток А Логічна схема мережі	68
Додаток Б Слайди презентації.....	69

ВСТУП

Інтенсивний розвиток цифрових технологій та широке впровадження мережових рішень у різні сфери суспільної діяльності зумовлюють необхідність модернізації інформаційної інфраструктури закладів культури, зокрема бібліотек. Сьогодні бібліотечні установи поступово трансформуються у сучасні інформаційні центри, що забезпечують не лише доступ до традиційних фондів, але й до електронних ресурсів, цифрових каталогів та віддалених сервісів. У таких умовах особливо важливим стає питання побудови ефективної, масштабованої та захищеної мережевої системи, яка б об'єднувала всі підрозділи бібліотечної мережі міста в єдиний інформаційний простір.

Актуальність теми обумовлена потребою проектування розподіленої мережі бібліотек міста, що дозволить забезпечити стабільний обмін даними між окремими підрозділами та іншими структурами, централізоване управління інформаційними ресурсами та високий рівень захисту даних, які передаються у відкритих мережах [1]. Важливу роль у реалізації таких рішень відіграють технології VLAN та VPN, які надають можливість логічно розділяти мережеву інфраструктуру на окремі сегменти, оптимізувати трафік і забезпечувати безпечне з'єднання між віддаленими вузлами через незахищені мережі [2].

Для досягнення поставленої мети необхідно вирішити наступні завдання: проаналізувати сучасні підходи до побудови розподілених корпоративних мереж; дослідити принципи функціонування технологій VLAN та VPN; визначити вимоги до мережевої інфраструктури бібліотечної системи; розробити логічну та фізичну структуру мережі; обґрунтувати вибір мережевого обладнання, протоколів і засобів захисту інформації; а також розглянути аспекти забезпечення кібербезпеки в межах запропонованої архітектури [3].

В першій частині роботи проаналізоване технічне завдання до проектування. Проведене моделювання інформаційно-комунікаційної мережі міських бібліотек для організації розподіленої мережевої інфраструктури.

Визначені та наведені основні завдання, які потрібно вирішити в процесі проєктування.

В другій частині розглянуті питання пов'язані з вибором технологій каналного рівня, стандартів, протоколів та фізичних інтерфейсів. Проведено вибір основного мережевого, міжмережевого та клієнтського обладнання.

В третій частині зпроєктована розподілена мережа бібліотек міста, проведене її моделювання в системі Cisco Packet Tracer.

Четверта частина роботи присвячена налаштуванню мережевих з'єднань та підключення кінцевого обладнання в окремих бібліотеках, із застосуванням технології VLAN та налаштуванню міжмережевих з'єднань, із використанням технології VPN.

Практична цінність роботи полягає у можливості використання запропонованих рішень для модернізації або створення сучасної бібліотечної мережі міського рівня, яка дозволить підвищити ефективність доступу до інформаційних ресурсів, забезпечити централізоване адміністрування та посилити рівень захищеності даних.

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ABIC	– Автоматизована бібліотечна інформаційна система
VLAN	– Virtual Local Area Network, віртуальна локальна мережа
STP	– Spanning Tree Protocol, протокол сполучного дерева
OSPF	– Open Shortest Path First, протокол динамічної маршрутизації стану зв'язків
DHCP	– Dynamic Host Configuration Protocol, протокол динамічного конфігурування мережевих параметрів
DNS	– Domain Name Server, система доменних імен
CKC	– Структурована кабельна система
KC	– Комутаційна стійка
NAS/SAN	– Network attached storage/Storage Area Network, мережева система зберігання даних/архітектурне рішення для підключення зовнішніх пристроїв
VPN	– Virtual Private Network, віртуальна приватна мережа
ILS	– Integrated Library System, інтегрована бібліотечна система
RAID	– Redundant Array of Independent Disks, технологія віртуалізації даних
LMS	– Learning management system, система управління навчальною діяльністю
SSL/TLS	– Secure Sockets Layer/Transport Layer Security, рівень захищених сокетів/захист на транспортному рівні
URL	– Uniform Resource Locator, адреса ресурсу в мережі Інтернет
IPSEC	– Internet Protocol Security, набір протоколів для захисту даних за допомогою автентифікації та шифрування кожного IP-пакета
QoS	– Quality of service, якість обслуговування

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Актуальність теми та аналіз структури

Міська публічна бібліотечна система є інформаційною, культурною й освітньою установою. Основними цілями її діяльності є: вільний пошук і отримання інформації; сприяння реалізації права людини і громадянина щодо долучення до цінностей культури й науки; створення умов для розвитку особистості, освіти та самоосвіти, культурної діяльності й дозвілля.

Відповідно до цілей основними задачами діяльності бібліотечної системи є: організація і забезпечення збереження книжкових фондів; створення бібліографічних каталогів; задоволення культурних, пізнавальних потреб читачів; просвітницька та культурна діяльність; участь у формуванні освітніх ресурсів та інформаційне обслуговування мешканців міста; залучення населення до культурних цінностей суспільства; науково-дослідна та методична діяльність у сфері бібліотечної справи.

Центральна міська бібліотека розглядається як базовий елемент перспективної єдиної інформаційно-комунікаційної системи бібліотечної мережі міста. У межах інфраструктури, що проектується, вона визначається як центральний вузол зберігання, обробки, маршрутизації та розподілу інформаційних потоків між усіма структурними підрозділами та філіями бібліотечної системи (рис.1.1). При цьому необхідно зазначити, що на даному етапі така мережева інфраструктура існує переважно у вигляді концептуального проекту та потребує подальшого технічного впровадження, закупівлі мережевого обладнання, серверних платформ, засобів захисту інформації та налаштування програмно-апаратного комплексу [4].

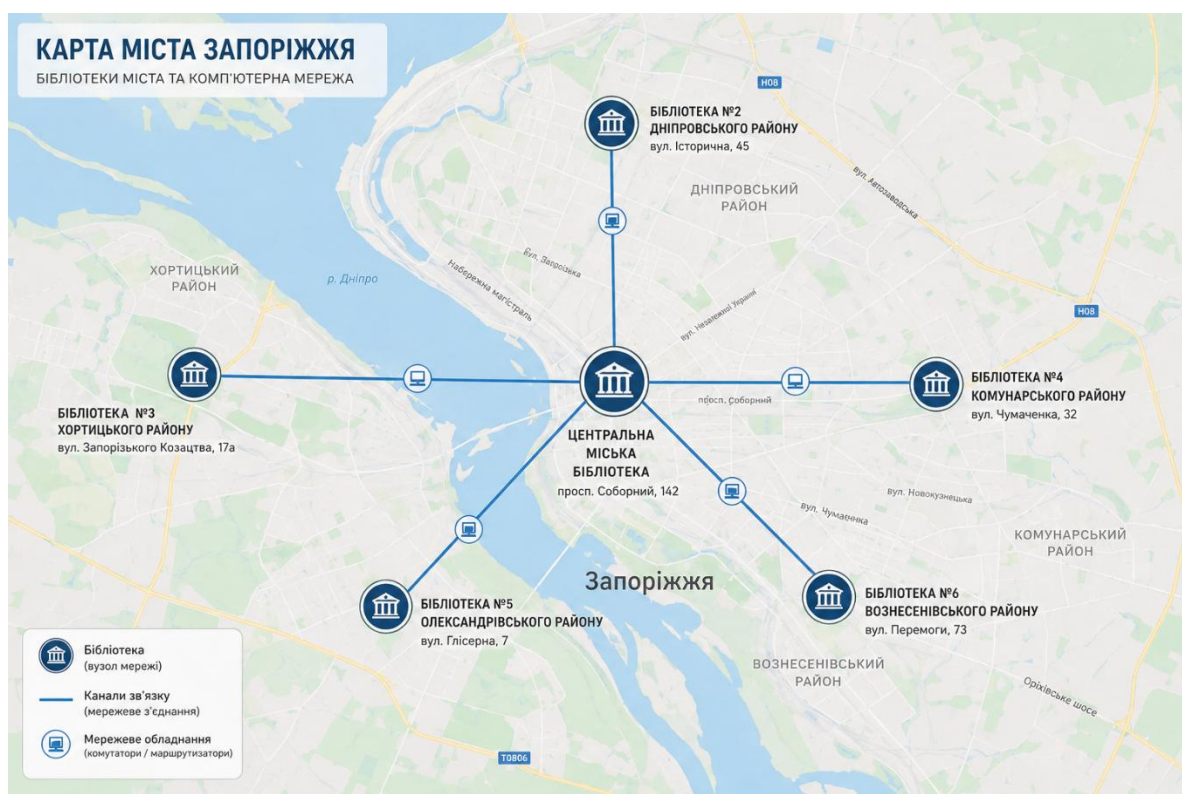


Рисунок 1.1 – Архітектура бібліотечної мережі

Виходячи з актуальності теми та мети роботи, розглянемо структуру мережі бібліотек міста: центральна бібліотека та 5 бібліотек філій.

Структура центральної бібліотеки: дирекція; бухгалтерія; відділ обслуговування користувачів; відділ комплектування; технічний відділ (відділ автоматизації та інформаційних технологій); читальні зали та коворкінг -зона. Кожен із структурних елементів виконує спеціальні функції в загальній архітектурі бібліотечної системи. Зокрема, дирекція забезпечує стратегічне управління системою, кадрову політику та адміністративну координацію роботи всіх підрозділів. Бухгалтерія здійснює оперативний та бухгалтерський облік, а також фінансове супроводження діяльності бібліотечної мережі.

Відділ обслуговування користувачів є одним із основних структурних підрозділів бібліотеки, який забезпечує безпосередню взаємодію з відвідувачами. До його функцій належать реєстрація нових користувачів, ведення статистичного обліку відвідувань та видачі документів, популяризація бібліотечного фонду, організація культурно-просвітницьких заходів, а також

надання інформаційних послуг у дистанційному форматі через офіційний вебсайт, електронну пошту та соціальні мережі, зокрема шляхом функціонування сервісу віртуальної довідки.

Відділ комплектування здійснює централізоване управління процесами формування та оновлення бібліотечного фонду всієї системи. Його діяльність спрямована на забезпечення своєчасного надходження нових документів до структурних підрозділів, ведення їх обліку, класифікацію та систематизацію, а також створення й підтримку довідково-пошукового апарату, включаючи електронні та зведені каталоги. Відділ автоматизації та інформаційних технологій забезпечує функціонування цифрової інфраструктури бібліотеки. До його завдань належать впровадження сучасних інформаційних технологій, технічне супроводження комп'ютерної та мережевої інфраструктури, підтримка автоматизованих бібліотечних систем, а також розвиток електронних сервісів і цифрових ресурсів для користувачів.

Важливе місце в організаційній структурі центральної бібліотеки займають зони безпосереднього доступу до інформаційних ресурсів. Читальна зала призначена для роботи з документами, що використовуються виключно в межах бібліотеки, та забезпечує інформаційно-бібліографічне обслуговування відвідувачів. Коворкінг-простір виконує функцію сучасного цифрового середовища, де користувачі можуть працювати з власними мобільними пристроями або стаціонарними комп'ютерами, користуватися бездротовим доступом до мережі Інтернет, а також застосовувати додаткове периферійне обладнання, зокрема засоби друкування, сканування та копіювання документів.

Архітектура бібліотечної мережі формується відповідно до принципів сучасних корпоративних інформаційних систем і враховує вимоги до масштабованості, централізованого адміністрування, відмовостійкості, безперервності надання послуг та інформаційної безпеки. Основним призначенням такої інфраструктури є забезпечення стабільного доступу користувачів до електронних каталогів, цифрових архівів, бібліографічних баз даних, мультимедійних ресурсів, освітніх платформ і автоматизованих

бібліотечних систем типу ILS. Крім того, проєкт передбачає підтримку сервісів дистанційного обслуговування користувачів, електронної реєстрації читачів та організації віддаленого доступу до інформаційних ресурсів через вебтехнології та мережу Інтернет [5].

З точки зору мережевої архітектури, у проєкті пропонується реалізація багаторівневої корпоративної моделі типу Core–Distribution–Access, яка широко застосовується у великих інформаційно-комунікаційних системах (рис.1.2). Така структура дозволяє ефективно розподілити функції між мережевими пристроями, оптимізувати маршрутизацію трафіку, забезпечити централізоване керування мережею та підвищити загальну продуктивність системи.

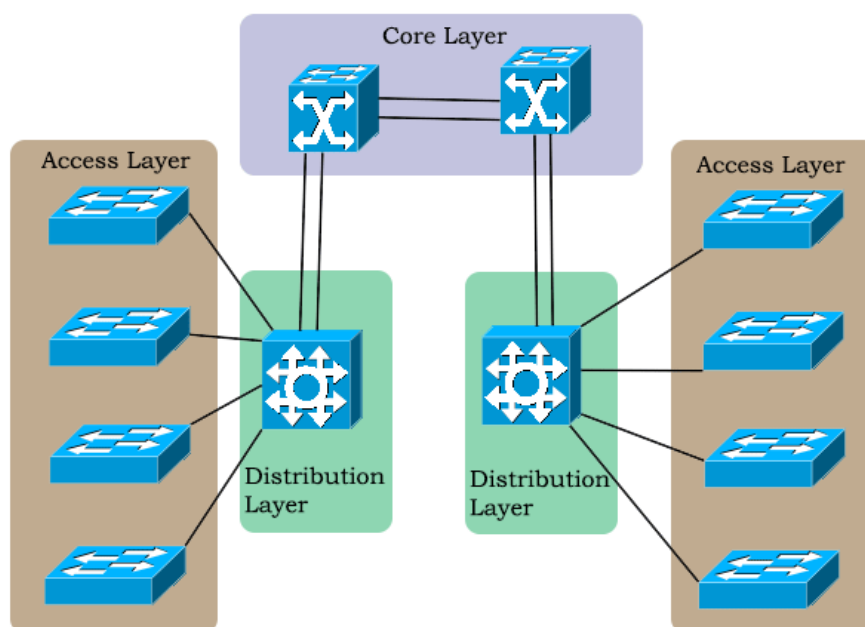


Рисунок 1.2 – Багаторівнева мережева модель Core–Distribution–Access

У межах цієї моделі центральна бібліотека виконує роль ядра мережі, де передбачається розміщення серверного обладнання, систем централізованого зберігання даних, мережних шлюзів та засобів моніторингу інфраструктури. Рівень Distribution призначений для агрегації трафіку між окремими сегментами мережі та реалізації політик маршрутизації, VLAN-сегментації й контролю доступу [6]. Access-рівень забезпечує підключення кінцевих пристроїв

користувачів, робочих станцій бібліотекарів, точок бездротового доступу та спеціалізованого периферійного обладнання.

З позиції структурного аналізу можна виділити такі ключові функціональні підсистеми:

- серверна підсистема зберігання та обробки даних;
- комутаційна мережева інфраструктура;
- система інформаційної безпеки;
- підсистема віддаленого доступу та клієнтської взаємодії.

Таким чином, інтеграція організаційної структури бібліотечної мережі з сучасною мережевою архітектурою дозволяє сформувати єдиний інформаційний простір міста, забезпечити централізоване управління ресурсами та підвищити ефективність бібліотечного обслуговування користувачів.

1.2 Вимоги до сучасної розподіленої бібліотечної мережі

Сучасна розподілена бібліотечна мережа – це складна екосистема, яка поєднує традиційні бібліотеки, цифрові архіви та користувачів в єдиний інформаційний простір. Її основне завдання – забезпечити швидкий, стабільний і безпечний доступ до знань незалежно від того, де знаходиться користувач. До такої мережі висувається низка ключових вимог.

Передусім важливо створити єдиний інформаційний простір, де користувач може здійснювати пошук одразу по всіх бібліотечних каталогах. Система повинна підтримувати масштабування – тобто легко розширюватися зі зростанням кількості бібліотек і обсягів даних без втрати ефективності. Не менш важливо забезпечити синхронізацію даних у реальному часі, щоб інформація про фонди завжди залишалася актуальною. Крім того, необхідна сумісність різних систем, що досягається завдяки використанню міжнародних стандартів і протоколів обміну даними.

Мережа має бути максимально відкритою – користувачі повинні мати цілодобовий доступ до електронних ресурсів, включаючи книги та бази даних. Інтерфейси повинні бути зручними та адаптованими як для комп'ютерів, так і для мобільних пристроїв. Важливо також враховувати принципи інклюзивності, забезпечуючи доступ до ресурсів для людей з різними фізичними можливостями.

Система повинна працювати безперебійно навіть у разі технічних збоїв. Для цього використовуються резервні сервери та регулярне копіювання даних. Особливу увагу варто приділити захисту персональної інформації користувачів і дотриманню політик конфіденційності. Також необхідно забезпечити захист від кібератак і несанкціонованого доступу.

Ефективна робота мережі передбачає співпрацю бібліотек у форматі консорціуму, що дозволяє оптимізувати витрати та спільно розвивати ресурси. Важливим є дотримання авторських прав під час використання цифрових матеріалів. Крім того, персонал повинен мати достатній рівень цифрових компетенцій для роботи з сучасними технологіями та підтримки користувачів.

1.3 Аналіз подібних рішень і технологій

Під час проектування розподіленої мережі бібліотек доцільно враховувати практичні підходи, які вже застосовуються в корпоративних і освітніх мережах. Такі системи мають подібні вимоги: стабільна робота, контроль доступу, можливість підключення віддалених підрозділів та поступове розширення інфраструктури. Найпростішим варіантом є побудова мережі на базі класичної локальної інфраструктури без чіткої сегментації. Подібні рішення можна зустріти у невеликих організаціях. Вони не потребують складного налаштування, однак при збільшенні кількості користувачів починають виникати обмеження: зростає навантаження на мережу, ускладнений контроль доступу, важче відокремити службовий і користувацький трафік.

Важливою складовою аналізу проєкту є аналіз логічної структури мережі та взаємодії її компонентів. Передбачається використання технологій VLAN для сегментації мережевого простору між адміністративними, службовими та користувацькими підмережами, що дозволить підвищити рівень інформаційної безпеки та зменшити навантаження на мережеву інфраструктуру. Для забезпечення захищеної взаємодії між філіями бібліотечної системи планується впровадження VPN-технологій, які дозволять організувати безпечні канали передачі даних через публічні мережі [7]. Також проєктом передбачено використання керованих комутаторів, маршрутизаторів корпоративного класу, серверів баз даних та систем резервного копіювання інформації.

Більш стійким рішенням є використання керованих комутаторів із підтримкою VLAN та маршрутизації. У цьому випадку мережа логічно поділяється на сегменти, що дозволяє розмежувати різні групи користувачів і сервіси. Такий підхід широко використовується у навчальних закладах і корпоративних системах, оскільки дає змогу краще контролювати трафік і спрощує адміністрування.

При виборі обладнання часто поєднують рішення різного рівня. Для невеликих вузлів або філій можуть застосовуватись пристрої середнього класу, наприклад MikroTik. Вони, без значних витрат, дозволяють реалізувати базові функції: маршрутизацію; VPN; фільтрацію трафіку. Для центрального вузла зазвичай використовують обладнання корпоративного рівня (Cisco, HPE Aruba), яке краще справляється з великим навантаженням і підтримує розширені механізми управління мережею. Окремо слід відмітити хмарні рішення. Вони дозволяють винести частину сервісів (бази даних, вебресурси) у зовнішню інфраструктуру. Це спрощує масштабування, але підвищує залежність від якості інтернет-з'єднання і вимагає додаткової уваги до захисту даних.

Сучасні підходи, такі як SDN або SD-WAN, забезпечують централізоване управління мережею та більш гнучке використання каналів зв'язку. Водночас їх впровадження потребує складнішої інфраструктури, тому для мереж середнього масштабу вони частіше розглядаються як перспектива розвитку, а не базове

рішення. Для кращого розуміння доцільності використання різних підходів наведено порівняльну таблицю (табл.1.1).

Таблиця 1.1 – Порівняння мережевих рішень для бібліотечної системи

Тип рішення	Основні характеристики	Переваги	Обмеження	Доцільність використання
Локальна мережа без сегментації	Єдина мережа без VLAN, базова маршрутизація	Простота реалізації, низька вартість	Відсутність ізоляції, складність контролю доступу, низька масштабованість	Невеликі бібліотеки
VLAN + L3 комутація	Логічне розділення мережі, маршрутизація між сегментами	Кращий контроль трафіку, підвищена безпека, гнучкість	Потребує налаштування та керованого обладнання	Міські бібліотечні мережі
MikroTik-рішення	Єдиний пристрій із функціями маршрутизації, VPN, firewall	Доступність, гнучкість налаштувань	Обмеження при великому навантаженні	Філії, невеликі вузли
Корпоративні рішення (Cisco, HPE)	Високопродуктивне обладнання з розширеними функціями	Надійність, масштабованість, централізоване управління	Висока вартість, складне адміністрування	Центральний вузол мережі
Хмарні рішення	Розміщення сервісів у віддалених дата-центрах	Гнучке масштабування, зменшення локальної інфраструктури	Залежність від інтернету, сумнівна безпека даних	Додаткові сервіси
SDN / SD-WAN	Програмно-керована мережа, централізоване управління	Гнучкість, оптимізація трафіку	Складність впровадження	Перспективний розвиток

Можемо зробити висновок, що найреалістичнішим та зваженим виглядає комбінований підхід. Центральний вузол будується на потужнішому обладнанні, філії – на більш простіших рішеннях, мережа ділиться на VLAN, а взаємодія між вузлами організовується через VPN. Це добре збалансована схема що не вимагає надмірно складної реалізації.

1.4 Постановка завдань

Метою даного проєкту є створення централізованої сучасної мережевої інфраструктури бібліотечної системи міста, яка забезпечить ефективну обробку, зберігання, маршрутизацію та розподіл інформаційних ресурсів між центральною бібліотекою та її філіями. Проєкт розглядається як концептуальне рішення, що передбачає подальше технічне впровадження, закупівлю обладнання та налаштування програмно-апаратних компонентів.

Для досягнення поставленої мети передбачається розробка та впровадження багаторівневої мережевої архітектури за моделлю Core–Distribution–Access, що дозволить централізовано керувати мережевим трафіком, підвищити продуктивність, масштабованість і відмовостійкість системи. У межах проєкту планується використання корпоративного мережевого обладнання (маршрутизаторів, комутаторів доступу, бездротових точок доступу), побудова структурованої кабельної системи та впровадження систем резервного живлення.

Важливою складовою є розгортання трирівневої серверної інфраструктури, що включає файловий сервер для зберігання цифрових ресурсів, сервер баз даних для ведення електронного каталогу та обліку користувачів, а також сервер прикладних сервісів для забезпечення роботи вебпорталу, електронного документообігу та систем дистанційного обслуговування. Додатково передбачається впровадження технологій віртуалізації серверів для підвищення гнучкості та відмовостійкості системи.

Інтеграція існуючих інформаційних сервісів у єдину централізовану платформу забезпечить стабільний доступ користувачів до електронних каталогів, цифрових архівів, бібліографічних баз даних і мультимедійних ресурсів. З метою підвищення безпеки та ефективності функціонування мережі передбачається впровадження VLAN-сегментації з логічним розділенням мережі на окремі сегменти (серверний, адміністративний, користувачів, кабельний та бездротовий).

Для забезпечення захищеної взаємодії між центральною бібліотекою та філіями планується реалізація VPN-з'єднань із використанням технологій IPsec (site-to-site) та SSL/TLS (віддалений доступ), що гарантуватиме конфіденційність і цілісність переданих даних. Проєкт також передбачає розгортання бездротової мережі Wi-Fi у публічних зонах бібліотеки з використанням сучасних стандартів IEEE 802.11ac/ax, централізованого керування та забезпечення якості обслуговування (QoS) для приблизно 100 одночасно підключених пристроїв.

Відповідно до поставленої мети визначено такі основні завдання проєкту:

- провести аналіз сучасних технологій локальних (LAN) та глобальних (WAN) мереж, їх порівняння та вибір оптимальних рішень;
- виконати обґрунтований вибір мережевого обладнання для центральної бібліотеки та філій;
- змодельовати мережеву інфраструктуру в середовищах симуляції для перевірки працездатності архітектури;
- розробити структурну та логічну схеми мережі;
- реалізувати логічне розділення мережі на VLAN для серверів, адміністрації, користувачів, Wi-Fi та мережевого обладнання;
- налаштувати міжвланову маршрутизацію та політики доступу;
- впровадити VPN-рішення (IPsec та SSL/TLS) для захищеної взаємодії між вузлами мережі;
- виконати розгортання та налаштування обладнання;
- організувати підключення до мережі Інтернет з тестуванням мережі;
- розгорнути бездротову мережу з централізованим керуванням, забезпечити покриття публічних зон та реалізувати QoS і балансування трафіку;
- впровадити системи моніторингу, адміністрування та резервування;
- організувати технічне обслуговування та підтримку інфраструктури.

У підсумку, реалізація проєкту дозволить створити масштабовану, керовану та відмовостійку інформаційно-комунікаційну систему, що забезпечить якісний доступ користувачів до сучасних бібліотечних та електронних сервісів.

2 ВИБІР ТЕХНОЛОГІЙ ТА МЕРЕЖЕВОГО ОБЛАДНАННЯ

2.1 Технології каналного рівня (Ethernet, Wi-Fi 6)

У межах проєктованої бібліотечної мережі ключову роль відіграють технології каналного та мережевого рівня, оскільки саме вони визначають базові принципи передачі даних між вузлами системи, забезпечують стабільність з'єднань та впливають на загальну продуктивність інфраструктури.

Для реалізації дротового сегмента мережі застосовується технологія Ethernet (IEEE 802.3), яка є стандартом де-факто для сучасних локальних мереж завдяки високій надійності, масштабованості та широкій сумісності з мережевим обладнанням різних виробників. Ethernet забезпечує передачу даних у вигляді кадрів на основі MAC-адресації, що дозволяє ефективно організовувати комутацію трафіку на рівні L2. У проєкті передбачається використання гігабітних та мультигігабітних рішень (1000Base-T/1000Base-LX), що дозволяє забезпечити достатню пропускну здатність для роботи серверної інфраструктури, доступу до електронних каталогів, цифрових архівів та внутрішніх інформаційних сервісів бібліотеки.

Узагальнюючи, слід зазначити, що запропонована мережева архітектура центральної бібліотеки є комплексною концептуальною моделлю сучасної інформаційної інфраструктури міського рівня. Вона включає використання стандартів Ethernet IEEE 802.3, оптоволоконних технологій Gigabit Ethernet, бездротових стандартів Wi-Fi 5/6, а також технологій VLAN та VPN для забезпечення логічної сегментації та захищеного доступу [8].

У контексті подальшого розвитку системи доцільним є проведення детального аналізу та порівняння альтернативних технологічних рішень і мережевого обладнання, що можуть бути використані для реалізації даної архітектури. Зокрема, необхідно здійснити оцінювання різних типів комутаторів (керованих і некерованих), маршрутизаторів корпоративного класу, серверного обладнання, систем зберігання даних (NAS/SAN), а також бездротових точок

доступу з підтримкою сучасних стандартів безпеки та високої пропускної здатності. Окрему увагу слід приділити порівнянню рішень різних виробників за критеріями продуктивності, масштабованості, надійності, вартості володіння та можливостей централізованого керування [9]. На даний момент запропонована архітектура існує виключно на рівні проєктної моделі і не реалізована у вигляді діючої фізичної інфраструктури. Це зумовлює необхідність подальшого етапу впровадження, який має включати закупівлю та встановлення обладнання, побудову фізичної топології мережі, конфігурацію маршрутизації та комутації, впровадження VLAN і VPN-рішень, а також проведення тестування навантаження і перевірки рівня інформаційної безпеки [10].

Таким чином, перехід від концептуального проєктування до практичної реалізації з одночасним аналізом і порівнянням технологій та обладнання є ключовою умовою створення сучасної, масштабованої та надійної бібліотечної мережі міського рівня, здатної забезпечити стабільне функціонування цифрових сервісів і високий рівень якості інформаційного обслуговування користувачів.

Нижче наведено аналітичні таблиці (табл. 2.1-2.3) порівняння основних технологій, які використовуються при проєктуванні моделі бібліотечної мережі, з їх альтернативами. Порівняння виконано з точки зору продуктивності, масштабованості, вартості та доцільності застосування.

Таблиця 2.1 – Порівняння технологій дротового доступу (Ethernet)

Технологія	Швидкість	Середовище	Переваги	Недоліки	Альтернативи
100Base-TX	до 100 Мбіт/с	Вита пара Cat5e	Низька вартість, проста реалізація	Обмежена пропускна здатність	1000Base-T
1000Base-T	до 1 Гбіт/с	Вита пара Cat5e/Cat6	Висока швидкість, сумісність	Вища вартість обладнання	10GBase-T
1000Base-LX	до 1 Гбіт/с	Оптоволокно	Велика дальність, завадостійкість	Висока вартість інсталяції	10GBase-LR

Для сучасної бібліотечної мережі 100Base-TX є застарілим рішенням, тоді як 1000Base-T та 1000Base-LX забезпечують оптимальний баланс між продуктивністю та надійністю [11].

Використання оптоволоконних каналів зв'язку для з'єднання центральної бібліотеки з філіями має особливе значення, оскільки вони забезпечують високу швидкість передачі даних, низький рівень затримок та стійкість до електромагнітних завад. Це є критично важливим для стабільного функціонування розподіленої інформаційної системи.

Таблиця 2.2 – Порівняння комутаційних технологій (L2 vs L3)

Тип комутатора	Функціональність	Переваги	Недоліки	Використання
L2 Switch	Комутація за MAC-адресами	Дешевий, простий	Немає маршрутизації	Кінцеві пристрої
L3 Switch	Маршрутизація + комутація	VLAN routing, продуктивність	Вища вартість	Core мережі
Router-on-a-stick	Маршрутизація через VLAN	Гнучкість	Обмежена швидкість	Малий масштаб

Для центральної бібліотеки оптимальним є L3-комутатор, оскільки він забезпечує між VLAN-маршрутизацію без перевантаження маршрутизаторів.

Таблиця 2.3 – Порівняння технологій бездротового доступу (Wi-Fi)

Стандарт	Швидкість	Частота	Переваги	Недоліки
802.11n (Wi-Fi 4)	до 600 Мбіт/с	2.4/5 ГГц	Сумісність, дешевизна	Нижча продуктивність
802.11ac (Wi-Fi 5)	до 3.5 Гбіт/с	5 ГГц	Висока швидкість	Обмежене покриття
802.11ax (Wi-Fi 6)	до 9.6 Гбіт/с	2.4/5 ГГц	Висока щільність користувачів	Вища вартість

Для бібліотеки із ~100 пристроями доцільно використовувати Wi-Fi 6 (IEEE 802.11ax), яка є сучасним розвитком бездротових локальних мереж, через підтримку великої кількості одночасних підключень. Вона забезпечує підвищену пропускну здатність, покращену роботу в умовах високої щільності підключень та ефективніше використання радіочастотного спектра. Це особливо актуально для бібліотечного середовища, де одночасно може працювати велика кількість користувачів із мобільними пристроями.

Wi-Fi 6 також підтримує технології OFDMA(Orthogonal Frequency Division Multiple Access) та MU-MIMO(multi-user, multi-in multi-out), що дозволяє

одночасно обслуговувати декілька клієнтів без суттєвого зниження швидкості передачі даних. У межах проєкту передбачається централізоване керування точками доступу, що дозволяє оптимізувати навантаження, забезпечити рівномірне покриття приміщень та реалізувати політики доступу відповідно до VLAN-сегментації.

Таким чином, поєднання Ethernet як базової дротової технології та Wi-Fi 6 як сучасного бездротового рішення дозволяє сформувати гібридну мережеву інфраструктуру, яка забезпечує баланс між продуктивністю, мобільністю та масштабованістю всієї бібліотечної системи.

2.2 Технологія VLAN, особливості використання

Виходячи з вимог організації бібліотечної мережі, інфраструктура розподіляється на логічні сегменти відповідно до функціонального призначення підрозділів. Це дозволяє забезпечити диференційований доступ до серверних ресурсів для різних груп користувачів, які можуть фізично перебувати в різних частинах мережі або навіть у різних будівлях.

VLAN є логічною структурою мережі, яка об'єднує набір вузлів із спільними вимогами до обміну даними так, ніби вони підключені до одного фізичного сегмента, незалежно від їх фактичного розташування [12]. На відміну від класичної фізичної локальної мережі, VLAN дозволяє формувати логічні групи пристроїв без зміни фізичної топології (табл. 2.4).

Завдяки цьому зміни в структурі мережі можуть виконуватися програмно, без необхідності фізичного переміщення обладнання. Основними причинами використання VLAN у розподіленій бібліотечній мережі міста є:

- VLAN є економічно доцільним рішенням, оскільки обмін даними всередині одного логічного сегмента здійснюється через комутатор без залучення

маршрутизатора, що знижує навантаження на маршрутизатори та зменшує затримки в мережі;

- VLAN забезпечує гнучкість конфігурації, оскільки сегментація може здійснюватися за різними критеріями, зокрема за портами комутатора, протоколами або IP-підмережами, що дозволяє оперативно змінювати структуру мережі відповідно до потреб організації;

- VLAN спрощує адміністрування мережі, оскільки дозволяє централізовано керувати доступом користувачів до ресурсів і розділяти їх на логічні групи без необхідності фізичних змін у мережевій інфраструктурі.

Таблиця 2.4 – Порівняння VLAN та альтернативних підходів сегментації

Технологія	Принцип	Переваги	Недоліки	Альтернатива
VLAN (802.1Q)	Логічна сегментація L2	Безпека, ізоляція, масштабованість	Потребує керованих комутаторів	Фізична сегментація
Фізичні мережі	Окремі кабельні сегменти	Максимальна ізоляція	Висока вартість	VLAN
Subnetting (L3)	IP-сегментація	Гнучкість маршрутизації	Менше ізоляції L2	VLAN + routing

VLAN є оптимальним рішенням, оскільки забезпечує баланс між безпекою та економічністю. Стандарт IEEE 802.1Q [13] визначає механізм реалізації VLAN у мережах Ethernet шляхом додавання спеціального тегу до стандартного кадру. Це забезпечує одночасну передачу трафіку декількох віртуальних мереж через одну фізичну інфраструктуру.

У класичному форматі кадру Ethernet передбачено поле типу або довжини, що забезпечує сумісність із попередніми версіями стандарту IEEE 802.3. Для реалізації механізму віртуальних локальних мереж у стандарті IEEE 802.1Q до структури кадру додається спеціальний VLAN-тег, який містить службову інформацію для ідентифікації належності кадру до певної віртуальної мережі.

Модифікований кадр IEEE 802.1Q включає додатковий 4-байтовий заголовок, що розташовується між MAC-адресою відправника та полем типу протоколу. Цей заголовок складається з двох 2-байтових полів. Перше поле, Tag

Protocol Identifier (TPID), має фіксоване значення 0x8100 і використовується мережевими пристроями для визначення наявності VLAN-тегу в кадрі. Друге поле, Tag Control Information (TCI), містить службові підполя, необхідні для керування трафіком і визначення належності кадру до конкретної VLAN. До складу поля TCI входять:

- 3-бітове поле пріоритету (Priority Code Point, PCP), яке використовується для класифікації та пріоритезації мережевого трафіку відповідно до вимог якості обслуговування (QoS);
- біт CFI/DEI (Canonical Format Indicator або Drop Eligible Indicator), що застосовується для службових цілей під час обробки кадрів;
- 12-бітове поле VLAN Identifier (VID), призначене для визначення номера віртуальної локальної мережі.

Завдяки використанню поля VID стандарт IEEE 802.1Q дозволяє створювати до 4094 логічно ізольованих VLAN у межах однієї фізичної мережевої інфраструктури. Кожному VLAN призначається унікальний ідентифікатор, а передавання даних між пристроями здійснюється в межах відповідного логічного сегмента. Такий підхід забезпечує ефективне розмежування широкомовних доменів, підвищує рівень інформаційної безпеки та спрощує адміністрування мережі. Порівняльну структуру звичайного Ethernet-кадру та кадру з тегом IEEE 802.1Q наведено на рисунку 2.1.

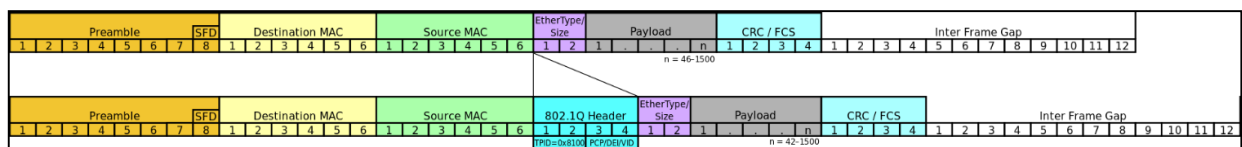


Рисунок 2.1 – Структура Ethernet-кадру та кадру з тегом IEEE 802.1Q

Для забезпечення коректної роботи багаторівневих мережевих інфраструктур та запобігання конфліктам ідентифікаторів VLAN між клієнтськими мережами та мережею оператора зв'язку використовується стандарт IEEE 802.1ad, відомий також як Provider Bridging або QinQ. Цей

стандарт є розвитком технології IEEE 802.1Q та розширює її функціональні можливості шляхом підтримки подвійного тегування Ethernet-кадрів.

Принцип роботи IEEE 802.1ad полягає в інкапсуляції клієнтського VLAN-тегу в додатковий тег провайдера. У результаті кадр містить два незалежні VLAN-заголовки: внутрішній тег (Customer Tag, C-tag), який використовується для ідентифікації VLAN у мережі клієнта, та зовнішній тег (Service Tag, S-tag), що застосовується оператором зв'язку для організації транспортування трафіку через власну інфраструктуру.

На відміну від стандарту IEEE 802.1Q, який передбачає використання лише одного VLAN-тегу в Ethernet-кадрі, технологія QinQ дозволяє передавати трафік багатьох клієнтських VLAN через єдину мережу провайдера без зміни внутрішньої структури адресації та логічної сегментації. Це забезпечує високий рівень ізоляції клієнтських мереж, спрощує адміністрування великих корпоративних інфраструктур і суттєво підвищує масштабованість телекомунікаційних мереж.

Використання IEEE 802.1ad є особливо доцільним під час побудови територіально розподілених корпоративних мереж, центрів обробки даних та мультисервісних мереж операторського класу, де необхідно забезпечити прозору передачу трафіку між віддаленими сегментами локальної мережі через інфраструктуру провайдера. Порівняння структури Ethernet-кадру без тегування, кадру з одним VLAN-тегом IEEE 802.1Q та кадру з подвійним тегуванням IEEE 802.1ad наведено на рисунку 2.2.

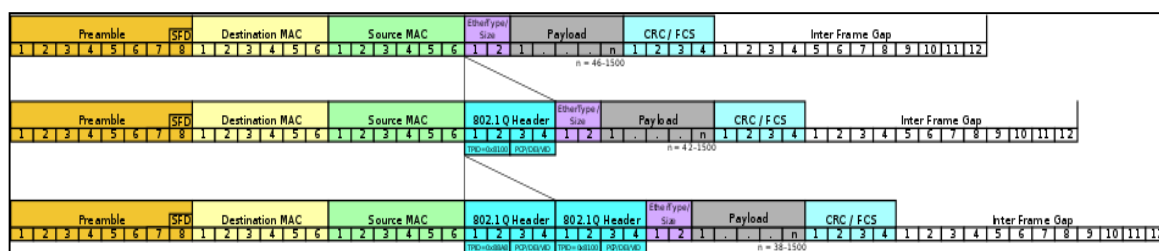


Рисунок 2.2 – Порівняння структури кадрів

У запропонованому проєкті для логічної сегментації мережевої інфраструктури використовується технологія VLAN відповідно до стандарту IEEE 802.1Q. Для організації взаємодії між окремими сегментами мережі та забезпечення коректної передачі трафіку через зовнішню транспортну інфраструктуру передбачено застосування механізмів IEEE 802.1ad (QinQ), які дозволяють реалізувати багаторівневе тегування кадрів і гарантують ізоляцію мережевого трафіку між різними рівнями архітектури.

Використання зазначених технологій створює основу для побудови гнучкої, масштабованої та безпечної мережевої інфраструктури бібліотечної системи. Логічне розділення мережі на окремі VLAN забезпечує ефективне розмежування службового, адміністративного та користувацького трафіку, зменшує обсяг широкомовних повідомлень у межах мережі та підвищує продуктивність її функціонування. Сегментація мережі сприяє посиленню інформаційної безпеки завдяки обмеженню доступу між окремими групами користувачів і сервісів.

Таким чином, впровадження технологій IEEE 802.1Q та IEEE 802.1ad дозволяє підвищити керованість мережевої інфраструктури, спростити процес її адміністрування, забезпечити необхідний рівень масштабованості та створити надійну основу для функціонування єдиної інформаційно-комунікаційної системи бібліотек міста.

2.3 VPN-рішення

Під час проєктування корпоративної мережі бібліотечної системи особливу увагу приділено забезпеченню захищеного обміну даними між центральною бібліотекою та її територіально віддаленими філіями, а також організації безпечного віддаленого доступу для працівників. Для реалізації цих завдань передбачається використання технологій віртуальних приватних мереж

VPN, які дають змогу створювати захищені логічні канали зв'язку поверх загальнодоступних мереж передачі даних, зокрема мережі Інтернет.

Технологія VPN базується на принципах тунелювання (рис. 2.3) та криптографічного захисту інформації, що забезпечує конфіденційність, цілісність і автентичність переданих даних. Завдяки цьому користувачі та віддалені підрозділи можуть безпечно взаємодіяти з внутрішніми інформаційними ресурсами бібліотечної системи незалежно від свого фізичного розташування, отримуючи доступ до сервісів так, ніби вони підключені безпосередньо до локальної мережі центральної бібліотеки.

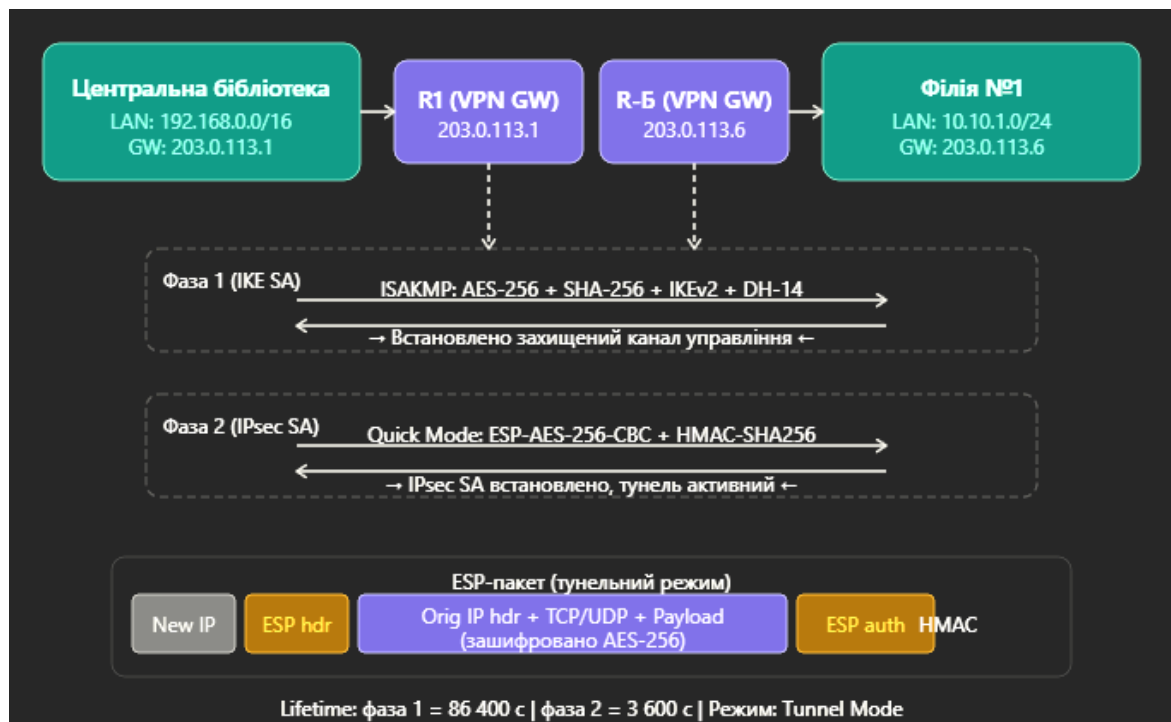


Рисунок 2.3 – Схема IPsec VPN-тунелю (site-to-site)

Для аналізу та вибору оптимального рішення в межах проекту розглядаються три сучасні технології побудови VPN-з'єднань: IPsec, SSL/TLS VPN та WireGuard. Кожна з них має власні особливості функціонування, рівень безпеки, складність впровадження та сфери застосування.

Технологія IPsec є одним із найбільш поширених рішень для побудови захищених міжмережових з'єднань типу site-to-site між центральною

бібліотекою та її філіями. Вона функціонує на мережевому рівні моделі OSI та забезпечує захист IP-трафіку шляхом автентифікації, шифрування й контролю цілісності пакетів. Для реалізації механізмів безпеки використовуються протоколи Authentication Header (AH) та Encapsulating Security Payload (ESP), які дозволяють захищати інформацію від несанкціонованого доступу, модифікації та підміни. Основними перевагами IPsec є високий рівень криптографічного захисту, підтримка сучасних алгоритмів шифрування, можливість апаратного прискорення на мережевому обладнанні та широка сумісність із маршрутизаторами, міжмережевими екранами й іншими корпоративними засобами зв'язку. Завдяки цим характеристикам IPsec залишається одним із найбільш надійних рішень для організації захищених каналів між віддаленими підрозділами. Водночас впровадження даної технології потребує ретельного налаштування політик безпеки, параметрів шифрування та механізмів автентифікації, що робить процес конфігурування складнішим порівняно з деякими сучасними VPN-рішеннями.

Технологія SSL/TLS VPN використовується для забезпечення віддаленого доступу користувачів і співробітників бібліотечної системи до внутрішніх інформаційних ресурсів через вебінтерфейс або спеціалізовані клієнтські застосунки. Основною перевагою даного підходу є простота експлуатації та налаштування, оскільки підключення може здійснюватися безпосередньо через веббраузер без необхідності складної конфігурації мережевого обладнання або встановлення додаткових мережевих сервісів. Водночас до недоліків SSL/TLS VPN можна віднести дещо нижчий рівень продуктивності порівняно з IPsec-рішеннями, що зумовлено функціонуванням на прикладному або сеансовому рівні моделі OSI та додатковими витратами на обробку трафіку.

WireGuard є сучасною технологією VPN, яка характеризується спрощеною архітектурою та високою ефективністю реалізації криптографічних механізмів. Вона функціонує поверх протоколу UDP і використовує сучасні алгоритми шифрування, що забезпечує високу швидкість передачі даних, мінімальні затримки та ефективне використання обчислювальних ресурсів. Завдяки

компактній кодовій базі та оптимізованим механізмам захисту WireGuard демонструє суттєво вищу продуктивність у порівнянні з традиційними VPN-рішеннями. Однак слід зазначити, що рівень його інтеграції та підтримки в корпоративних мережевих інфраструктурах поки що поступається більш усталеним рішенням, таким як IPsec, хоча поступово розширюється завдяки активному впровадженню у сучасних операційних системах і мережевому обладнанні. Для наочності наведено порівняльну характеристику основних VPN-рішень, які розглядаються в межах проєкту (табл. 2.5).

Таблиця 2.5 – Порівняння VPN-технологій

Тип VPN	Протокол	Переваги	Недоліки	Використання
IPsec VPN	ESP/AH	Висока безпека, site-to-site	Складна конфігурація	Філії
SSL VPN	TLS	Простий доступ через браузер	Менша продуктивність	Користувачі
L2TP/IPsec	Комбінований	Сумісність	Середня швидкість	Мобільні клієнти
WireGuard	UDP	Висока швидкість, простота	Менша традиційна підтримка	Сучасні мережі

За результатами проведеного аналізу визначено, що для побудови ефективної та безпечної мережевої інфраструктури бібліотечної системи доцільним є використання комбінованого підходу до впровадження VPN-рішень. Зокрема, технологія IPsec VPN рекомендується для організації захищеної міжфіліальної взаємодії, оскільки вона забезпечує стабільні site-to-site з'єднання та високий рівень криптографічного захисту між сегментами мережі.

У свою чергу, SSL/TLS VPN є найбільш придатним рішенням для організації віддаленого доступу користувачів і співробітників, оскільки забезпечує простоту підключення та зручність використання без необхідності складного налаштування мережевого обладнання. Це робить його оптимальним для реалізації клієнтського доступу до внутрішніх ресурсів бібліотечної системи.

Технологія WireGuard може розглядатися як перспективний напрям розвитку VPN-інфраструктури, який у майбутньому здатний частково або

повністю замінити традиційні рішення завдяки високій продуктивності, сучасній криптографії та простоті конфігурації.

Таким чином, застосування VPN-технологій у межах проєктованої бібліотечної мережі забезпечує захищену передачу даних, збереження їх цілісності та конфіденційності, а також сприяє інтеграції територіально розподілених підрозділів у єдиний інформаційний простір із централізованим керуванням.

2.4 Технології та протоколи маршрутизації

У межах проєктування розглянуто три основні підходи до організації маршрутизації в мережевій інфраструктурі: статичну маршрутизацію, динамічну маршрутизацію на основі протоколу OSPF, а також концепцію SD-WAN як сучасну модель керування розподіленими мережами.

Статична маршрутизація передбачає ручне налаштування маршрутів на кожному мережевому пристрої. Вона відзначається простотою реалізації, високим рівнем передбачуваності та контрольованістю трафіку. Такий підхід є доцільним для невеликих мережесегментів або для організації резервних маршрутів. Однак у випадку масштабних розподілених інфраструктур статична маршрутизація ускладнює адміністрування, оскільки будь-які зміни топології потребують ручного оновлення конфігурацій на значній кількості пристроїв.

Протокол OSPF належить до класу протоколів динамічної маршрутизації та базується на принципі стану каналів зв'язку. Для обчислення оптимальних маршрутів у мережі використовується алгоритм Дейкстри, який дозволяє визначати найкоротші шляхи між вузлами. Серед ключових переваг OSPF слід відзначити високу масштабованість, швидку збіжність (convergence) мережі після змін топології, а також підтримку ієрархічної організації мережі за допомогою поділу на області. У контексті бібліотечної мережі OSPF є доцільним

рішенням для організації маршрутизації між центральним вузлом і філіями, особливо з урахуванням можливого подальшого розширення інфраструктури.

Принцип функціонування протоколу OSPF передбачає послідовну взаємодію маршрутизаторів для формування узгодженої топологічної картини мережі та побудови оптимальних маршрутів передачі даних. На першому етапі маршрутизатори обмінюються Hello-пакетами через інтерфейси, на яких активовано OSPF. У разі збігу основних параметрів цих пакетів між пристроями встановлюються сусідські відносини. Далі, залежно від типу мережі та характеристик з'єднання, відбувається формування суміжності між маршрутизаторами. Після встановлення суміжних відносин пристрої виконують синхронізацію баз даних стану каналів. На наступному етапі кожен маршрутизатор формує та розповсюджує оголошення про стан своїх каналів (Link-State Advertisements, LSA) до сусідніх пристроїв. Отримана інформація з LSA накопичується у базі даних стану каналів, яка поступово синхронізується між усіма маршрутизаторами в межах однієї області. Таким чином забезпечується однакове уявлення про топологію мережі на всіх пристроях даного сегмента. На основі сформованої LSDB кожен маршрутизатор виконує розрахунок найкоротших шляхів за допомогою алгоритму Дейкстри, в результаті чого будується дерево оптимальних маршрутів. Завершальним етапом є формування таблиці маршрутизації, яка містить найефективніші шляхи до всіх доступних мережевих вузлів.

Концепція SD-WAN (Software-Defined Wide Area Network) є сучасним підходом до побудови та управління розподіленими мережами, який ґрунтується на програмно-визначеному керуванні трафіком через централізовану політику. SD-WAN дозволяє абстрагувати фізичну інфраструктуру від логіки маршрутизації, забезпечуючи гнучке використання різних каналів зв'язку, а також автоматичну оптимізацію маршрутів залежно від якості каналу. Даний підхід підвищує ефективність використання мережевих ресурсів, спрощує адміністрування та забезпечує кращу адаптивність до змін навантаження.

Серед основних переваг SD-WAN слід відзначити високу гнучкість, централізоване адміністрування та підвищену продуктивність використання мережевих ресурсів. Водночас впровадження даної технології потребує значних інфраструктурних ресурсів, а також складнішої організації мережевого середовища порівняно з традиційними підходами маршрутизації.

Таким чином, кожен із розглянутих підходів має власну сферу застосування, а їх використання в проєктованій бібліотечній мережі може бути комбінованим залежно від рівня складності та вимог до масштабованості інфраструктури. Для наочності наведено порівняльну характеристику основних підходів до маршрутизації (табл. 2.6).

Таблиця 2.6 – Порівняння технологій маршрутизації

Тип маршрутизації	Принцип роботи	Переваги	Недоліки
Static routing	Ручне налаштування маршрутів	Простота, контрольованість	Немає автоматизації
OSPF	Динамічний обмін маршрутами	Швидка адаптація, масштабованість	Складніше налаштування
SD-WAN	Програмно-керована маршрутизація	Гнучкість, оптимізація трафіку	Висока вартість впровадження

У межах даного проєкту базовим рішенням обрано протокол OSPF як основний механізм динамічної маршрутизації між сегментами мережі. Статична маршрутизація використовується як допоміжний інструмент для налаштування резервних шляхів та шлюзів за замовчуванням. SD-WAN розглядається як перспективний напрямок розвитку інфраструктури у випадку масштабування бібліотечної системи до рівня міської або регіональної мережі.

Таким чином, поєднання статичної та динамічної маршрутизації забезпечує баланс між простотою адміністрування, надійністю та можливістю подальшого розширення мережевої інфраструктури бібліотеки. В перспективі доцільний перехід до SD-WAN. Порівняльний аналіз показує, що проєктована мережа бібліотеки базується на сучасних, але поступово змінюваних технологіях [15]. Найбільш критичними для впровадження є: перехід на Gigabit Ethernet

(1000Base-T / LX); використання Wi-Fi 6 (802.11ax); впровадження VLAN (802.1Q) як базового механізму сегментації; реалізація IPsec VPN для міжфіліальної взаємодії та використання L3-комутатора як ядра мережі.

2.5 Серверні технології (Linux/Windows Server, віртуалізація)

Виходячи з основних завдань проєктування, передбачається використання комбінованого підходу до серверних платформ із застосуванням операційних систем Linux та Windows Server, а також технологій віртуалізації для підвищення ефективності використання апаратних ресурсів.

Операційна система Windows Server доцільна для реалізації сервісів, які потребують тісної інтеграції з корпоративними службами Microsoft, зокрема Active Directory, файловими сервісами та централізованим керуванням користувачами. Вона забезпечує зручний графічний інтерфейс адміністрування, широкі можливості політик безпеки та підтримку корпоративних служб каталогів.

У свою чергу, Linux-сервери (Ubuntu Server, Debian, CentOS/Rocky Linux) використовуються для розгортання вебсервісів, баз даних та мережевих служб. Основними перевагами Linux є стабільність, висока продуктивність, низькі вимоги до ресурсів та гнучкість конфігурації. Саме на базі Linux доцільно реалізовувати вебпортал бібліотеки, API-сервіси та системи дистанційного доступу до ресурсів.

У проєкті передбачається трирівнева серверна архітектура:

- файловий сервер (зберігання цифрових документів та архівів);
- сервер баз даних (електронний каталог, облік користувачів, бібліографічні записи);
- сервер прикладних сервісів (вебпортал, електронні сервіси, інтеграційні API).

Для оптимізації використання фізичних ресурсів та підвищення відмовостійкості застосовується віртуалізація серверів, яка дозволяє запускати декілька логічних серверів на одному фізичному обладнанні. Це спрощує адміністрування, зменшує витрати на апаратне забезпечення та забезпечує швидке відновлення систем у разі збоїв.

В рамках трирівневої серверної архітектури можуть використовуватись так платформи віртуалізації:

- VMware ESXi – корпоративне рішення з високою стабільністю та широкими можливостями керування;
- Microsoft Hyper-V – інтегроване рішення для Windows-екосистеми;
- Proxmox VE – відкрита платформа, яка поєднує KVM і контейнеризацію LXC.

Для наочності наведено порівняння серверних платформ та технологій віртуалізації (табл. 2.7-2.8).

Таблиця 2.7 – Порівняння серверних операційних систем

Платформа	Переваги	Недоліки	Основне застосування
Windows Server	Зручне адміністрування, Active Directory	Високі ліцензійні витрати	Файлові сервіси, доменна інфраструктура
Linux Server	Стабільність, продуктивність, безкоштовність	Потребує кваліфікації	Вебсервіси, бази даних, API

Таблиця 2.8 – Порівняння технологій віртуалізації

Технологія	Тип	Переваги	Недоліки	Використання
VMware ESXi	Hypervisor Type 1	Висока продуктивність, надійність	Ліцензійна модель	Корпоративні середовища
Hyper-V	Hypervisor Type 1	Інтеграція з Windows	Обмежена кросплатформеність	Windows-інфраструктура
Proxmox VE	KVM/LXC	Безкоштовність, гнучкість	Менша підтримка vendor-рішень	Освітні та середні проєкти

Таким чином, поєднання Windows Server та Linux дозволяє реалізувати гнучку та ефективну серверну інфраструктуру, яка відповідає вимогам бібліотечної системи. Використання віртуалізації забезпечує масштабованість, підвищує рівень відмовостійкості та спрощує адміністрування серверного середовища.

2.6 Системи зберігання даних (NAS/SAN)

З урахуванням обсягів інформації та вимог до високої доступності даних у межах проєктованої бібліотечної інфраструктури розглядаються два основні підходи до організації сховищ даних: NAS та SAN.

Технологія NAS є мережевим файловим сховищем, яке забезпечує доступ до даних на рівні файлів із використанням стандартних мережевих протоколів, зокрема SMB/CIFS або NFS. Основною перевагою NAS є відносна простота впровадження та адміністрування, а також економічна доцільність у порівнянні з більш складними рішеннями.

У контексті бібліотечних систем NAS є ефективним рішенням для централізованого зберігання електронних документів, книг, мультимедійних ресурсів, а також резервних копій інформаційних систем.

Архітектура SAN є більш складною високопродуктивною системою зберігання даних, яка забезпечує доступ на рівні блоків через спеціалізовані високошвидкісні канали передачі даних, такі як Fibre Channel або iSCSI. SAN застосовується у випадках, коли необхідна висока швидкість обробки великих масивів даних і мінімальні затримки, зокрема для роботи з критичними сервісами, базами даних та серверними додатками.

До основних переваг SAN належать висока продуктивність, масштабованість та відмовостійкість, однак її впровадження супроводжується значно вищою вартістю та складністю адміністрування.

У межах розробки бібліотечної інфраструктури доцільним є застосування комбінованого підходу до організації сховищ даних. Зокрема, NAS використовується для зберігання файлів користувачів, цифрових архівів та загальнодоступних ресурсів, тоді як SAN застосовується для обслуговування високонавантажених серверних додатків і баз даних, що потребують підвищеної продуктивності та надійності. Для наочності наведено порівняльну характеристику основних технологій зберігання даних (табл. 2.9).

Таблиця 2.9 – Порівняння систем зберігання даних NAS і SAN

Критерій	NAS (Network Attached Storage)	SAN (Storage Area Network)
Рівень доступу	Файловий рівень	Блоковий рівень
Протоколи	SMB, NFS, FTP	iSCSI, Fibre Channel
Продуктивність	Середня	Висока
Масштабованість	Обмежена	Висока
Вартість	Низька/середня	Висока
Складність	Проста	Складна
Застосування	Файли, архіви, резервні копії	Бази даних, критичні сервіси

До того ж, суттєве значення має організація систем резервного копіювання (backup), які можуть реалізовуватися як на базі NAS-рішень, так і за допомогою окремих серверних платформ із застосуванням інкрементного та диференційного підходів до збереження даних. Такий підхід надає можливість забезпечити відновлення інформації у разі відмов обладнання, програмних збоїв або значних втрат даних при передачі. Додатково це дозволяє оптимізувати використання дискового простору завдяки збереженню лише змінених або доповнених даних між копіями. Важливим аспектом є також можливість автоматизації процесів резервного копіювання за розкладом, що зменшує вплив людського фактору та підвищує надійність збереження інформації.

3 ПРОЄКТУВАННЯ МЕРЕЖІ БІБЛІОТЕК МІСТА

3.1 Логічна структура мережі

Важливою складовою аналізу проєкту є аналіз логічної структури мережі та взаємодії її компонентів. Передбачається використання технологій VLAN для сегментації мережевого простору між адміністративними, службовими та користувацькими підмережами, що дозволить підвищити рівень інформаційної безпеки та зменшити навантаження на мережеву інфраструктуру. Для забезпечення захищеної взаємодії між філіями бібліотечної системи планується впровадження VPN-технологій, які дозволять організувати безпечні канали передачі даних через публічні мережі [16]. Також проєктом передбачено використання керованих комутаторів, маршрутизаторів корпоративного класу, серверів баз даних та систем резервного копіювання інформації.

З позиції структурного аналізу проєкту можна визначити декілька ключових функціональних підсистем, які становлять основу моделі розподіленої мережі бібліотек міста (рис. 3.1): серверну підсистему зберігання та обробки даних, комутаційну мережеву інфраструктуру, систему інформаційної безпеки, підсистему віддаленого доступу та клієнтський рівень взаємодії користувачів із ресурсами бібліотеки. Такий підхід дозволяє забезпечити модульність архітектури та спрощує подальшу модернізацію системи відповідно до зростання кількості користувачів і цифрових сервісів.

Разом із тим слід підкреслити, що фактичне впровадження описаної архітектури на даний момент відсутнє, а реалізація проєкту потребує проведення комплексного технічного планування, поетапного монтажу мережевого обладнання, налаштування серверного середовища та тестування працездатності всіх компонентів системи [17].

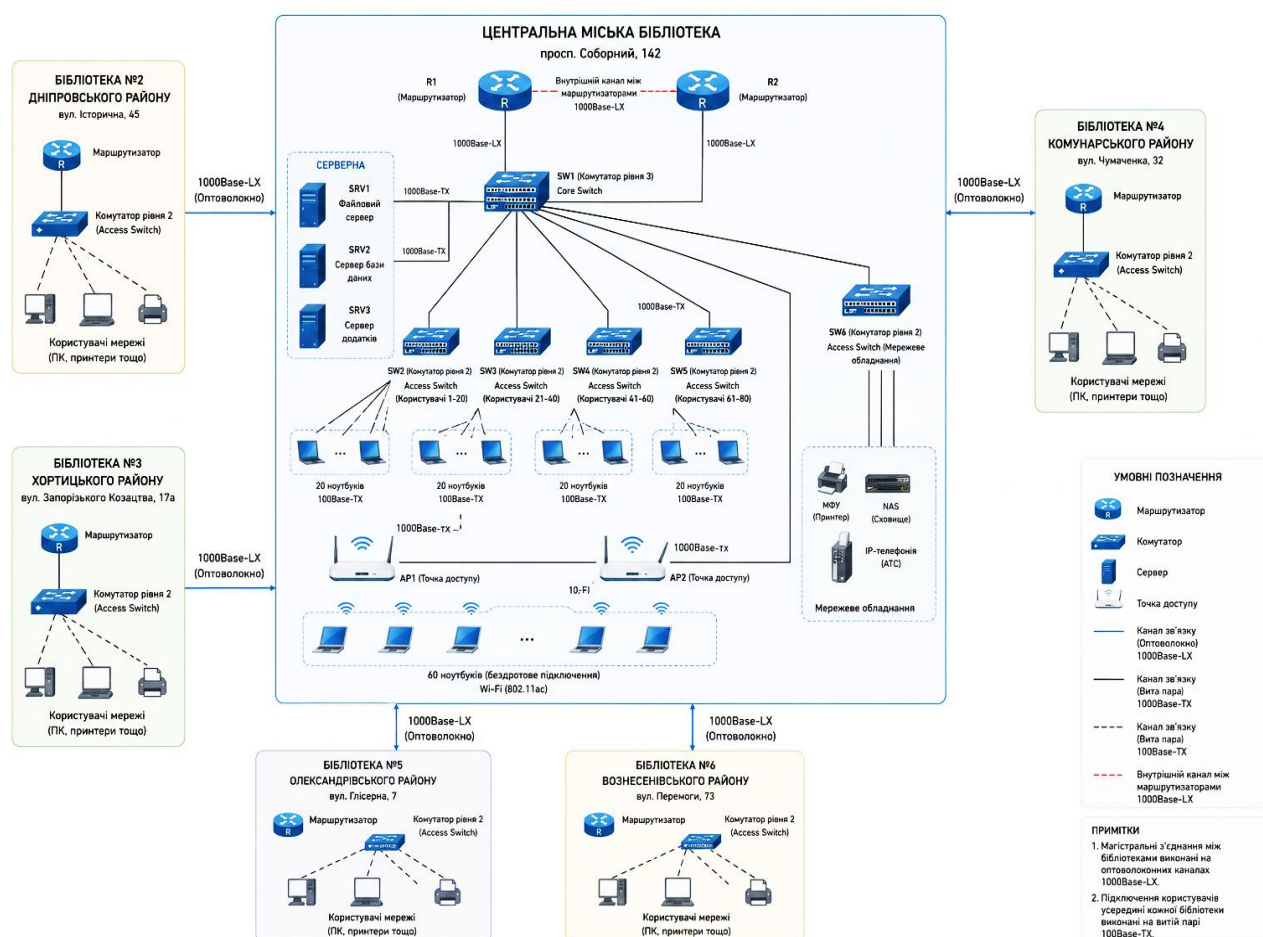


Рисунок 3.1 – Модель мережі з підключеннями

Перспективна реалізація даної мережевої інфраструктури дозволить сформувати єдиний інформаційний простір бібліотечної мережі міста, забезпечити централізоване управління ресурсами та підвищити ефективність інформаційного обслуговування користувачів.

У проєктній архітектурі передбачається активне використання технології VLAN (Virtual Local Area Network, IEEE 802.1Q) для логічного розділення єдиної фізичної мережі на окремі ізольовані сегменти VLAN (табл. 3.1):

- серверної інфраструктури;
- адміністративного персоналу;
- користувачів (читачів);
- бездротової мережі Wi-Fi;
- мережевого обладнання (management VLAN).

Таблиця 3.1 – Основні VLAN-сегменти мережі бібліотечної системи

VLAN ID	Назва	Призначення
VLAN 10	Servers	Серверна інфраструктура (бази даних, файлові та прикладні сервіси)
VLAN 20	Admin	Адміністративний персонал із розширеними правами доступу
VLAN 30	Users	Користувачі (читачі), термінали доступу та робочі станції відвідувачів
VLAN 50	WiFi	Бездротова мережа для мобільних пристроїв користувачів
VLAN 99	WiFi	Управління мережевим обладнанням (комутатори, маршрутизатори, сервери)

Кожен із зазначених сегментів виконує окрему функцію в межах єдиної інформаційної системи. Найбільш критичним є VLAN серверної інфраструктури, оскільки саме в ньому розміщуються основні інформаційні ресурси бібліотеки. VLAN управління використовується для адміністрування мережевого обладнання та має обмежений доступ лише для відповідальних осіб.

Користувацькі сегменти (Users, WiFi) мають обмежений доступ до внутрішніх ресурсів і взаємодіють із серверною частиною через визначені сервіси (наприклад, вебпортал або електронний каталог). Сегмент Librarians забезпечує роботу персоналу бібліотеки з внутрішніми системами, тоді як Admin має розширені права доступу для керування всією інфраструктурою.

Для забезпечення взаємодії між VLAN використовується міжвланова маршрутизація, яка реалізується на рівні L3-комутатора ядра мережі. При цьому застосовуються політики контролю доступу (ACL), що регламентують обмін даними між сегментами та запобігають несанкціонованому доступу. Логічна схема мережі (діаграма VLAN) наведена в додатку А.

Запропоновані політики доступу забезпечують чітке розмежування прав між різними сегментами мережі (табл. 3.2). Користувацькі VLAN мають обмежений доступ лише до необхідних сервісів, тоді як адміністративні та керуючі сегменти отримують розширені права для обслуговування інфраструктури.

Таблиця 3.2 – Політики доступу між VLAN-сегментами

Джерело VLAN	Призначення VLAN	Рівень доступу	Протоколи / сервіси	Примітка
Users	Servers	Обмежений	HTTP/HTTPS	Доступ до електронного каталогу
WiFi	Servers	Обмежений	HTTP/HTTPS	Лише публічні сервіси
Admin	Servers	Повний	SSH, RDP, SQL	Адміністрування серверів
Management	Усі VLAN	Повний	SSH, SNMP, ICMP	Керування мережевою інфраструктурою
Users	Admin	Заборонено	–	Ізоляція користувачів
WiFi	Users	Заборонено	–	Розмежування доступу
WiFi	Admin	Заборонено	–	Захист адміністративного сегмента
Users	Management	Заборонено	–	Обмеження доступу до обладнання
Admin	Users	Обмежений	HTTP/HTTPS	Моніторинг/підтримка
Servers	Users	Обмежений	TCP (сервіси)	Відповіді на запити клієнтів

Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу та підвищити загальний рівень інформаційної безпеки системи.

3.2 Мережеве обладнання та апаратна інфраструктура

Вибір мережевого та серверного обладнання для реалізації проєкту бібліотечної інформаційно-комунікаційної системи здійснюється з урахуванням вимог до продуктивності, надійності, масштабованості, вартості впровадження та подальшої експлуатації. Оскільки проєкт має централізовану архітектуру та передбачає обслуговування значної кількості користувачів і інформаційних ресурсів, до обладнання висуваються підвищені вимоги щодо стабільності роботи та підтримки сучасних мережевих технологій.

Проєктом передбачається використання наступного мережевого обладнання корпоративного класу:

- маршрутизатори (2 од.) рівня Cisco ISR або аналогічного класу (MikroTik CCR-серії або Juniper SRX), які забезпечують вихід у глобальні мережі, міжмережеву взаємодію та резервування каналів зв'язку;
- комутатор ядра (Core Layer 3 Switch), наприклад Cisco Catalyst 9500 або HPE Aruba 5400R, що забезпечує між VLAN-маршрутизацію та агрегацію трафіку;
- комутатори рівня доступу (4–5 од.), наприклад Cisco Catalyst 2960/9200 або аналогічні, які використовуються для підключення кінцевих пристроїв;
- серверна інфраструктура (3 фізичні або віртуалізовані сервери) на базі Dell PowerEdge, HPE ProLiant або Supermicro;
- бездротові точки доступу Wi-Fi (2–4 од.), наприклад Cisco Aironet або Ubiquiti UniFi;
- система резервного живлення (UPS) для забезпечення безперервної роботи критичних вузлів;
- мережеві шафи (rack 19"), патч-панелі, SFP-модулі, оптичні трансивери та структурована кабельна система (СКС).

Серверна інфраструктура проєктується як трирівнева система [5, 9]:

- файловий сервер (NAS/SAN-рівень) - для централізованого зберігання цифрових документів, архівів, резервних копій;
- сервер баз даних, який передбачає використання СУБД MySQL/PostgreSQL або Microsoft SQL Server для електронного каталогу, обліку користувачів, статистики та бібліографічних даних;
- сервер прикладних сервісів, який забезпечує роботу вебпорталу бібліотеки, систем електронного документообігу, LMS-платформ та сервісів віддаленого доступу.

При цьому файловий сервер може бути реалізований на базі Windows Server або Linux (Samba, NFS) із RAID-масивами для забезпечення відмовостійкості [18].

У якості основи мережевої інфраструктури застосовано обладнання корпоративного класу, яке підтримує функції VLAN-сегментації, маршрутизації,

VPN-з'єднань, а також централізованого адміністрування (табл. 3.3). Це дозволяє забезпечити необхідний рівень продуктивності та безпеки при обробці інформаційних потоків.

Таблиця 3.3 – Мережеве обладнання

Обладнання	Модель / Клас	Кількість	Обґрунтування вибору
Маршрутизатор	Cisco ISR 4331 / MikroTik CCR2004	2 од.	Забезпечують підключення до WAN, підтримку IPsec VPN, резервування каналів зв'язку
Комутатор ядра (L3)	Cisco Catalyst 9500 / HPE Aruba 5400R	1 од.	Виконує міжвланову маршрутизацію, агрегацію трафіку, високу продуктивність
Комутатори доступу (L2)	Cisco Catalyst 9200	4–5 од.	Підключення кінцевих пристроїв, підтримка VLAN та QoS
Точки доступу Wi-Fi	Ubiquiti UniFi 6 / Cisco Aironet	6-7 од.	Підтримка Wi-Fi 6, висока щільність клієнтів
VPN-шлюз	Fortinet FortiGate / Cisco ASA	1–2 од.	Захищені VPN-з'єднання, фільтрація трафіку
UPS	APC Smart-UPS 1500VA	2 од.	Забезпечення безперебійного живлення
Сервери	Dell PowerEdge / HPE ProLiant	3 од.	Висока продуктивність, підтримка віртуалізації

Маршрутизатори забезпечують стабільне підключення до глобальної мережі Інтернет, а також реалізацію захищених VPN-з'єднань між філіями бібліотечної системи. Використання двох пристроїв дозволяє організувати резервування каналів зв'язку та підвищити відмовостійкість системи.

Комутатор ядра (L3) відіграє ключову роль у функціонуванні мережі, оскільки виконує міжвланову маршрутизацію та забезпечує високошвидкісну обробку трафіку. Вибір саме L3-комутатора обумовлений необхідністю зменшення навантаження на маршрутизатори та підвищення ефективності роботи мережі. Комутатори рівня доступу використовуються для підключення

робочих станцій, серверів та точок доступу. Вони підтримують VLAN-сегментацію, що дозволяє реалізувати логічне розділення мережі відповідно до функціональних потреб.

Бездротова підсистема реалізується на базі точок доступу стандарту Wi-Fi 6, що забезпечує високу швидкість передачі даних та можливість одночасного підключення великої кількості користувачів. Це є критично важливим для публічних зон бібліотеки, де очікується значне навантаження.

3.3 Структурна схема мережі

У межах проєктної моделі використовується поєднання сучасних стандартів фізичного та канального рівнів:

- IEEE 802.3 (Ethernet) – базовий стандарт дротових локальних мереж;
- 100Base-TX (Fast Ethernet) – стандарт для підключення кінцевих пристроїв через виту пару Cat5e/Cat6;
- 1000Base-LX (Gigabit Ethernet over Fiber) – стандарт для магістральних оптоволоконних з'єднань між центральною бібліотекою та філіями;
- IEEE 802.11ac/ax (Wi-Fi 5/6) – стандарт, застосовується для організації бездротового доступу користувачів.

На канальному рівні моделі OSI реалізується передача Ethernet-кадрів, MAC-адресація, контроль помилок та керування доступом до середовища передачі [19]. Комутатори виконують функції навчання MAC-таблиць та фільтрації трафіку, що зменшує навантаження на мережу та підвищує її ефективність. Використання VLAN дозволяє: підвищити рівень безпеки передачі даних; обмежити в мережі ширококомовний трафік; оптимізувати загальне навантаження на мережу та спростити адміністрування всіх частин розподіленої мережі бібліотек міста.

Реалізація структурної схеми бібліотек міста починається з проектування центрального вузла, яким є вузол Центральної міської бібліотеки. Він визначається як ядро всієї інформаційно-комунікаційної системи. На цьому етапі формується фізична структура мережі, визначаються основні компоненти серверної інфраструктури, маршрутизації та рівні доступу користувачів.

У центральному сегменті мережі передбачається встановлення двох маршрутизаторів (R1 і R2), які забезпечують відмовостійкість та резервування каналів зв'язку, а також виконують функції маршрутизації внутрішнього та зовнішнього трафіку між бібліотечними підмережами і зовнішніми мережами. Між маршрутизаторами організується внутрішній канал зв'язку, що підвищує стабільність і надійність системи (рис. 3.2).

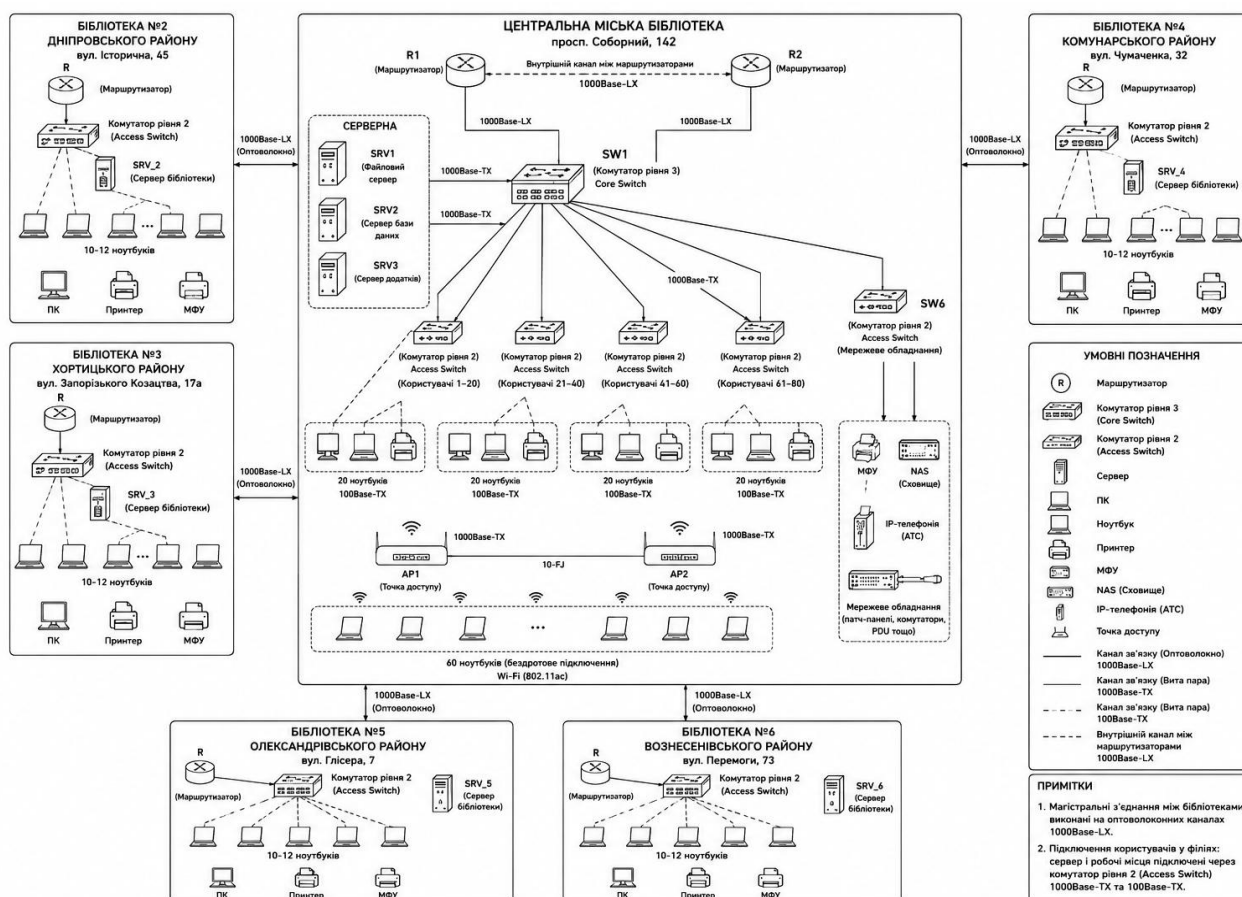


Рисунок 3.2 – Структурна схема мережі

Саме через впровадження core-рівня, який представлений центральним комутатором, здійснюється агрегація всього мережевого трафіку, підключення

серверної інфраструктури та розподіл даних до нижчих рівнів мережі. До серверного сегмента відносяться файловий сервер, сервер баз даних та сервер додатків, які забезпечують функціонування електронних каталогів, цифрових архівів та автоматизованих бібліотечних сервісів.

Далі реалізується рівень розподілу та доступу, який включає комутатори доступу, що об'єднують користувацькі пристрої в логічні сегменти мережі. На цьому рівні відбувається підключення робочих станцій бібліотекарів та користувачів, організованих у групи відповідно до структурних підрозділів (21–40, 41–60 тощо). Така сегментація дозволяє ефективно керувати навантаженням і підвищує рівень безпеки. Паралельно впроваджується бездротова підсистема, що базується на точках доступу Wi-Fi, які забезпечують підключення мобільних пристроїв, ноутбуків та інших клієнтів у читальних залах [20]. Також інтегрується додаткове мережеве обладнання, зокрема принтери, NAS-сховища та IP-телефонія, що формує єдину цифрову інфраструктуру бібліотеки [21].

Завершальним етапом реалізації є інтеграція філій бібліотек різних районів міста, які підключаються до центрального вузла через оптоволоконні канали зв'язку (1000Base-LX). На цьому рівні формується єдина міська бібліотечна мережа, у якій центральна бібліотека виконує роль керуючого та координаційного центру, забезпечуючи централізоване управління ресурсами, обмін даними та стабільне функціонування всієї системи.

4 НАЛАШТУВАННЯ МЕРЕЖ І МІЖМЕРЕЖЕВИХ З'ЄДНАНЬ

4.1 Поетапне впровадження VLAN у мережі бібліотечної системи

У межах даного проєкту технологія VLAN (IEEE 802.1Q) використовується як базовий механізм логічної сегментації мережі центральної бібліотеки та її філій. Основною метою впровадження VLAN є розділення мережевого трафіку між різними категоріями користувачів та сервісів,

підвищення рівня інформаційної безпеки, зменшення широкомовного трафіку та спрощення адміністрування мережевої інфраструктури.

Враховуючи структуру мережі, доцільно виконати сегментацію за функціональним принципом. На першому етапі здійснюється аналіз усіх вузлів мережі центральної бібліотеки та районних філій.

У центральній бібліотеці присутні:

- серверна інфраструктура;
- робочі станції співробітників;
- бездротова мережа Wi-Fi;
- IP-телефонія;
- мережеві пристрої;
- периферійне обладнання.

Для кожної категорії створюється окрема VLAN (табл.4.1).

Таблиця 4.1 – VLAN мережі

VLAN	Призначення	ID VLAN	IP-підмережа
ADMIN	Адміністрація	10	192.168.10.0/24
USERS	Користувачі бібліотеки	20	192.168.20.0/24
WIFI	Бездротова мережа	30	192.168.30.0/24
SERVERS	Серверна інфраструктура	40	192.168.40.0/24
VOICE	IP-телефонія	50	192.168.50.0/24
MGMT	Керування обладнанням	99	192.168.99.0/24

Для передачі декількох VLAN між комутаторами використовується стандарт IEEE 802.1Q. Для цього магістральні канали trunk необхідно налаштувати між:

- SW1 ↔ SW2;
- SW1 ↔ SW3;
- SW1 ↔ SW4;
- SW1 ↔ SW5;
- SW1 ↔ SW6;
- SW1 ↔ маршрутизаторами R1/R2.

Наводимо приклад конфігурації Cisco IOS:

```
enable
configure terminal
vlan 10
    name ADMIN
vlan 20
    name USERS
vlan 30
    name WIFI
vlan 40
    name SERVERS
vlan 50
    name VOICE
vlan 99
    name MANAGEMENT
exit
```

При цьому інтерфейси між комутаторами переводяться у режим trunk:

```
interface GigabitEthernet0/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan 10,20,30,40,50,99
interface GigabitEthernet0/2
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan 10,20,30,40,50,99
```

Порти для користувачів налаштовуються як access-порти:

```
interface range FastEthernet0/1-20
    switchport mode access
    switchport access vlan 20
    spanning-tree portfast
```

Порти для адміністрації:

```
interface range FastEthernet0/21-24
    switchport mode access
    switchport access vlan 10
    spanning-tree portfast
```

Підключення серверів:

```
interface GigabitEthernet0/10
  switchport mode access
  switchport access vlan 40
```

Підключення IP-телефонії:

```
interface FastEthernet0/30
  switchport mode access
  switchport access vlan 20
  switchport voice vlan 50
```

Точки доступу AP1 та AP2 повинні передавати трафік VLAN 30:

```
interface GigabitEthernet0/15
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 30
```

Оскільки в центральній бібліотеці використовується комутатор рівня L3 (SW1), міжвланова маршрутизація може виконуватись без окремого маршрутизатора. Увімкнення маршрутизації: `ip routing`

Створення SVI-інтерфейсів:

```
interface vlan 10
  ip address 192.168.10.1 255.255.255.0
  no shutdown
interface vlan 20
  ip address 192.168.20.1 255.255.255.0
  no shutdown
interface vlan 30
  ip address 192.168.30.1 255.255.255.0
  no shutdown
interface vlan 40
  ip address 192.168.40.1 255.255.255.0
  no shutdown
interface vlan 50
  ip address 192.168.50.1 255.255.255.0
  no shutdown
```

```
interface vlan 99
  ip address 192.168.99.1 255.255.255.0
  no shutdown
```

Для підвищення безпеки необхідно:

- вимкнути невикористовувані порти;
- обмежити список дозволених VLAN;
- використовувати окрему VLAN керування;
- активувати Port Security;
- використовувати DHCP Snooping;
- активувати Dynamic ARP Inspection.

Приклад вимкнення невикористаних портів:

```
interface range FastEthernet0/40-48
  shutdown
```

Приклад Port Security:

```
interface FastEthernet0/5
  switchport mode access
  switchport port-security
  switchport port-security maximum 2
  switchport port-security violation restrict
  switchport port-security mac-address sticky
```

У кожній районній бібліотеці створюються локальні VLAN:

- VLAN 20 – користувачі;
- VLAN 99 – керування.

Приклад для access-комутатора філії:

```
vlan 20
  name USERS
```

```
vlan 99
  name MANAGEMENT
```

Налаштування uplink-порту:

```
interface GigabitEthernet0/1
  switchport trunk encapsulation dot1q
```

```
switchport mode trunk
switchport trunk allowed vlan 20,99
```

Після завершення конфігурації виконується тестування.

Перевірка VLAN: `show vlan brief`

Перевірка trunk: `show interfaces trunk`

Перевірка маршрутизації: `show ip route`

Після впровадження VLAN у мережі бібліотечної системи буде досягнуто:

- логічне розділення трафіку;
- підвищення інформаційної безпеки;
- ізоляція серверного сегмента;
- зменшення широкомовного навантаження;
- підвищення продуктивності мережі;
- централізоване адміністрування;
- можливість масштабування мережі;
- підтримка IP-телефонії та Wi-Fi;
- підготовка інфраструктури до впровадження VPN та QoS.

Налаштування комутаторів у проєктованій бібліотечній мережі є одним із ключових етапів формування її логічної структури, оскільки саме на рівні комутації реалізуються механізми сегментації трафіку, керування доступом та забезпечення ефективної взаємодії між окремими підрозділами системи. Основна увага приділяється впровадженню технології VLAN відповідно до стандарту IEEE 802.1Q, конфігурації trunk-з'єднань між комутаторами для передачі трафіку кількох VLAN через один фізичний канал, а також налаштуванню access-портів для підключення кінцевих пристроїв.

У межах проєкту передбачено створення функціонально розподіленої VLAN-структури, яка включає такі сегменти: management, servers, admin, librarians, users, Wi-Fi та VoIP. Така сегментація дозволяє логічно ізолювати різні категорії користувачів і сервісів, зменшити розмір broadcast-доменів та оптимізувати навантаження на мережеву інфраструктуру (табл. 4.2).

Таблиця 4.2 – VLAN-сегментація бібліотечної мережі

Ім'я пристрою	Порт	Підключення	Тип порту	VLAN
Switch0 (Core)	Gig0/1	RouterOffice	Trunk	10,20,30,50,99
	Fa0/1	Switch1	Trunk	10,20,30,50,99
	Fa0/2	Switch2	Trunk	10,20,30,50,99
	Fa0/3	Switch3	Trunk	10,20,30,50,99
	Fa0/4	Switch4	Trunk	10,20,30,50,99
	Fa0/5–Fa0/7	Server Farm	Access	10
Switch1 (Access)	Fa0/1	Switch0 (Core)	Trunk	10,20,30,50,99
	Fa0/2–Fa0/3	Admin PCs	Access	20
	Fa0/4–Fa0/6	Librarian PCs	Access	30
	Fa0/7–Fa0/10	User PCs	Access	30
Switch2 (Access WiFi)	Fa0/1	Switch0 (Core)	Trunk	10,20,30,50,99
	Fa0/2–Fa0/8	WiFi Access Points	Access	50
Switch3 (Access)	Fa0/1	Switch0 (Core)	Trunk	10,20,30,50,99
	Fa0/2–Fa0/10	Users (читачі)	Access	30
Switch4 (Access)	Fa0/1	Switch0 (Core)	Trunk	10,20,30,50,99
	Fa0/2–Fa0/6	Admin PCs	Access	20
	Fa0/7–Fa0/12	Librarians	Access	30

Trunk-порти до Access-комутаторів:

```

interface GigabitEthernet0/3
  description To_SW2_Admin
  switchport mode trunk
  switchport trunk allowed vlan 20,99
interface GigabitEthernet0/4
  description To_SW3_Users
  switchport mode trunk
  switchport trunk allowed vlan 30,99
interface GigabitEthernet0/5
  description To_SW4_Users
  switchport mode trunk
  switchport trunk allowed vlan 30,99
interface GigabitEthernet0/6
  description To_SW5_Users

```

```
switchport mode trunk
switchport trunk allowed vlan 30,99
```

Маршрут за замовчуванням:

```
ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

Spanning Tree (оптимізація ядра):

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10 root primary
spanning-tree vlan 20 root primary
spanning-tree vlan 30 root primary
spanning-tree vlan 50 root primary
spanning-tree vlan 99 root primary
```

Spanning Tree (оптимізація ядра):

```
ip domain-name lab.local
username admin secret Admin123
crypto key generate rsa
modulus 1024
line vty 0 4
  login local
  transport input ssh
```

Збереження конфігурації:

```
end
write memory
```

Впровадження VLAN-архітектури на рівні комутаторів забезпечує підвищення рівня інформаційної безпеки, покращує керованість мережі та спрощує її адміністрування.

Крім того, чітке логічне розділення мережі підвищує масштабованість системи та створює основу для подальшого розвитку бібліотечної інформаційної інфраструктури.

4.2 Налаштування access-комутаторів та маршрутизації

Access-рівень мережі реалізовано на комутаторах SW2–SW5 (Cisco Catalyst 2960), які виконують роль підключення кінцевих користувачів та організації доступу до VLAN-ів.

Кожен комутатор працює у режимі Layer 2, а вся міжвланова маршрутизація винесена на SW1-Core (Layer 3 switch).

У межах цього рівня реалізовано:

- сегментацію користувачів за VLAN (Admin, Users);
- централізоване управління через Management VLAN (VLAN 99);
- trunk-з'єднання з core-комутатором SW1;
- базовий захист портів (PortFast + BPDU Guard);
- SSH-доступ для адміністрування.

Наведемо приклад конфігурації access-комутаторів SW2–SW5:

```
enable
configure terminal
hostname SW2-Access-Admin
no ip domain-lookup
! --- VLAN ---
vlan 20
    name Admin
vlan 99
    name Management
! --- Uplink до SW1 (Trunk) ---
interface GigabitEthernet0/1
    description Uplink_to_SW1
    switchport mode trunk
    switchport trunk allowed vlan 20,99
    no shutdown
! --- Порти для адмін. ПК (Fa0/1 - Fa0/20) ---
interface range FastEthernet0/1 - 20
    description Admin_Workstations_VLAN20
```

```

switchport mode access
switchport access vlan 20
spanning-tree portfast
spanning-tree bpduguard enable
no shutdown
! --- Management SVI ---
interface Vlan99
  ip address 192.168.100.12 255.255.255.0
  no shutdown
ip default-gateway 192.168.100.1
enable secret cisco123
line console 0
  password cisco
  login
line vty 0 4
  password cisco
  login
service password-encryption
end
write memory

```

Маршрутизація в мережі реалізована на двох маршрутизаторах R1 і R2, які забезпечують взаємодію між ядром (SW1-Core), віддаленими сегментами (Library-сайти) та резервування шляхів передачі даних.

Для динамічного обміну маршрутами використовується протокол OSPF (Area 0), що забезпечує швидку конвергенцію та автоматичне відновлення зв'язності у разі відмови одного з каналів.

Резервування реалізовано за рахунок:

- двох незалежних uplink-з'єднань між SW1 та R1/R2;
- міжмаршрутизаторського лінку R1 ↔ R2;
- налаштування вартості (OSPF cost) для пріоритизації основного маршруту.

Наведемо конфігурацію маршрутизаторів R1 та R2, які забезпечують динамічну маршрутизацію в мережі, обмін маршрутами між сегментами та резервування основних каналів зв'язку. Для цього використовується протокол OSPF (Area 0), що дозволяє автоматично оновлювати маршрути у разі змін у топології.

Конфігураційні налаштування маршрутизатора R1:

```
enable
configure terminal
hostname R1
no ip domain-lookup
! === Інтерфейси ===
interface GigabitEthernet0/0
    description To_SW1-Core
    ip address 10.0.0.1 255.255.255.252
    no shutdown
interface GigabitEthernet0/1
    description To_R2_Backup_Link
    ip address 10.0.1.1 255.255.255.252
    no shutdown
interface GigabitEthernet0/2
    description To_Library2
    ip address 10.10.2.1 255.255.255.252
    no shutdown
interface GigabitEthernet0/3
    description To_Library3
    ip address 10.10.3.1 255.255.255.252
    no shutdown
! === OSPF ===
router ospf 1
    router-id 1.1.1.1
    network 10.0.0.0 0.0.0.3 area 0
    network 10.0.1.0 0.0.0.3 area 0
    network 10.10.2.0 0.0.0.3 area 0
    network 10.10.3.0 0.0.0.3 area 0
! === Резервування (пріоритет основного каналу) ===
interface GigabitEthernet0/0
```

```

ip ospf cost 10
interface GigabitEthernet0/1
ip ospf cost 20
end
write memory

```

4.3 Додаткові налаштування безпечних підключень

Далі наведемо додаткові налаштування для безпечних підключень, а саме конфігурацію списків контролю доступу (ACL), які використовуються для обмеження доступу користувачів із VLAN 30 (Users) до серверної мережі VLAN 10 (Servers). ACL реалізуються на SW1-Core (Layer 3 switch), оскільки саме він виконує міжвланову маршрутизацію.

Основною метою є забезпечення:

- контролю доступу користувачів до серверів;
- дозволу тільки необхідних сервісів HTTP/HTTPS або DNS;
- повну ізоляцію небажаного трафіку.

ACL: Users → Servers (VLAN 30 → VLAN 10)

```

enable
configure terminal
ip access-list extended USERS_TO_SERVERS
! --- Дозволити необхідні сервіси (приклад: DNS, HTTP, HTTPS)
---
permit udp 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 53
permit tcp 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 80
permit tcp 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 443
! --- Заборонити весь інший доступ до серверів ---
deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
! --- Дозволити інший трафік (до інших мереж) ---
permit ip 192.168.30.0 0.0.0.255 any

```

ACL застосовується на інтерфейсі VLAN 30 (вхідний трафік від користувачів). Застосування ACL на SW1-Core:

```
interface Vlan30
  ip access-group USERS_TO_SERVERS in
```

Захист мережевого access-рівня від підроблених DHCP-серверів, несанкціонованого доступу та різноманітних атак канального рівня є однією з найважливіших складових забезпечення інформаційної безпеки сучасної комп'ютерної мережі. Оскільки саме на рівні доступу до мережі здійснюється безпосереднє підключення користувацьких пристроїв, робочих станцій, ноутбуків, мережевих принтерів та іншого кінцевого обладнання, виникає необхідність впровадження додаткових механізмів контролю та захисту мережевої інфраструктури. У мережі для підвищення рівня безпеки реалізовано технології DHCP Snooping та Port Security, які забезпечують контроль за підключенням пристроїв і дозволяють ефективно протидіяти загрозам на канальному рівні моделі OSI (Layer 2).

Технологія DHCP Snooping виконує функцію моніторингу та фільтрації DHCP-повідомлень, що передаються мережею. Її основним призначенням є захист від появи несанкціонованих DHCP-серверів, які можуть видавати користувачам некоректні мережеві параметри, перенаправляти трафік через зловмисні вузли або створювати умови для реалізації атак типу «людина посередині» (Man-in-the-Middle). Під час роботи DHCP Snooping усі порти комутатора поділяються на довірені та недовірені. Передача DHCP-відповідей дозволяється лише через довірені порти, що підключені до легітимного DHCP-сервера або центрального комутатора мережі. У даному проєкті таким пристроєм виступає SW1-Core, через який здійснюється централізована видача IP-адрес та інших мережевих параметрів. Завдяки цьому користувачі отримують коректні налаштування мережі виключно з авторизованого джерела, а спроби запуску сторонніх DHCP-серверів автоматично блокуються.

DHCP Snooping:

```
ip dhcp snooping
ip dhcp snooping vlan 20,30,50
interface g0/1
```

```
ip dhcp snooping trust
```

Додатковим елементом захисту є технологія Port Security, яка забезпечує контроль доступу до фізичних портів комутаторів. Вона дозволяє обмежити кількість допустимих MAC-адрес на кожному порту та прив'язати конкретний порт до визначених мережевих пристроїв. У разі підключення невідомого обладнання або перевищення встановленого ліміту MAC-адрес комутатор може виконати заздалегідь визначені дії, такі як блокування порту, генерація повідомлення про порушення або реєстрація події у журналі безпеки. Використання Port Security значно знижує ризик підключення сторонніх користувачів до мережі та перешкоджає несанкціонованому доступу до інформаційних ресурсів.

Крім того, застосування Port Security дозволяє ефективно протидіяти атакам типу MAC Flooding, під час яких зловмисник надсилає велику кількість підблених MAC-адрес з метою переповнення таблиці комутації пристрою. У результаті такої атаки комутатор може перейти в режим ширококомовної передачі кадрів, що створює можливість перехоплення мережевого трафіку. Обмеження кількості дозволених MAC-адрес та автоматичне блокування підозрілої активності усувають дану загрозу та підвищують рівень захищеності мережі.

Port Security:

```
interface range fa0/1-20
  switchport port-security
  switchport port-security maximum 2
  switchport port-security mac-address sticky
  switchport port-security violation restrict
```

Таким чином, спільне використання механізмів DHCP Snooping та Port Security забезпечує комплексний захист access-рівня мережі, підвищує надійність функціонування мережевої інфраструктури, мінімізує ризик несанкціонованого доступу та сприяє підтриманню стабільної й безпечної роботи всієї корпоративної мережі бібліотечної системи.

4.4 Налаштування VPN IPSec

Наведемо структурну схему побудови захищеної корпоративної VPN-мережі на основі технології IPSec для об'єднання центральної міської бібліотеки та п'яти віддалених бібліотек районів у єдину інформаційно-комунікаційну систему. Архітектура побудована за принципом «hub-and-spoke», де центральна міська бібліотека виконує роль головного вузла, а районні бібліотеки виступають віддаленими філіями, що підключаються через Інтернет із використанням зашифрованих тунелів IPSec VPN (рис. 4.1).

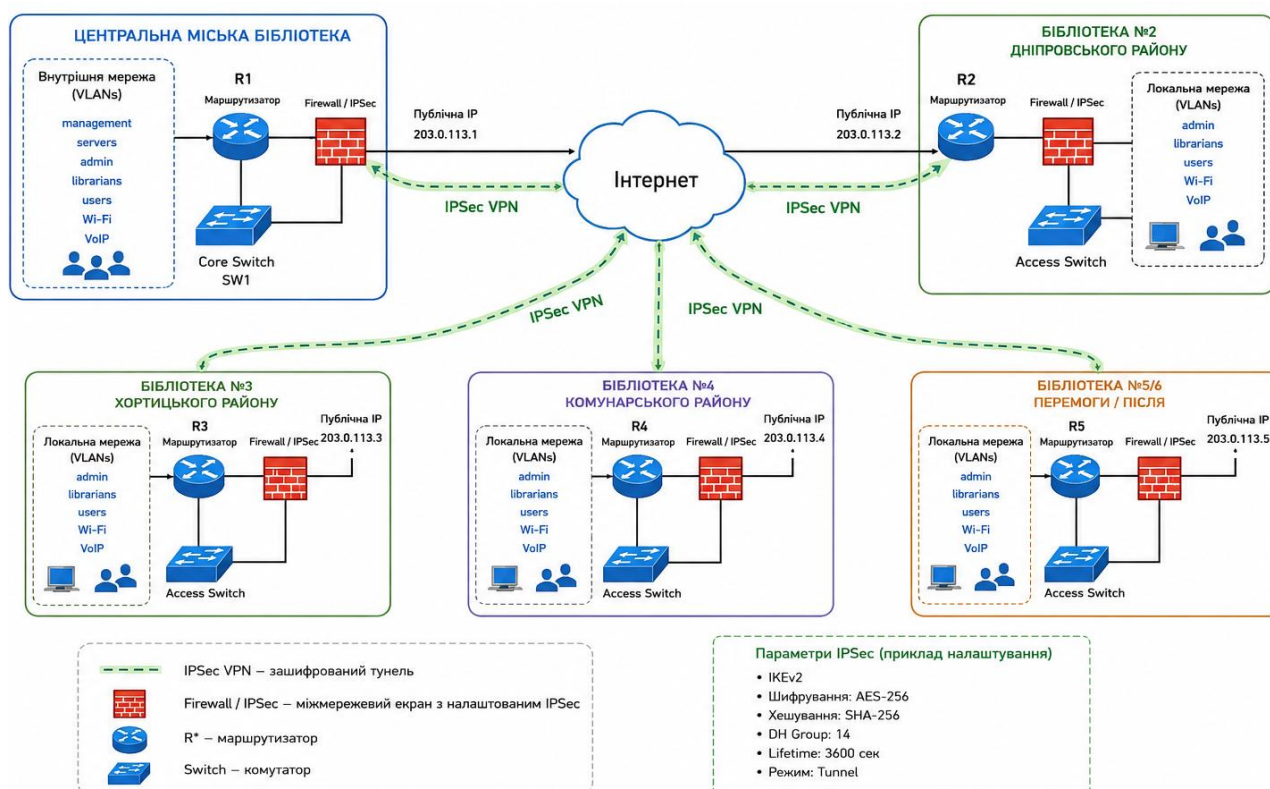


Рисунок 4.1 – Налаштування IPSec VPN

У центральній бібліотеці мережеву інфраструктуру сформовано на основі маршрутизатора R1, який забезпечує маршрутизацію між внутрішніми VLAN та зовнішнім каналом зв'язку. До маршрутизатора підключено міжмережевий екран (Firewall/IPSec), що виконує функції фільтрації трафіку та встановлення

VPN-з'єднань. Внутрішня мережа організована за допомогою комутатора Core Switch (SW1) і поділена на логічні сегменти VLAN: management, servers, admin, librarians, users, Wi-Fi та VoIP, що дозволяє сегментувати трафік, підвищити рівень безпеки та оптимізувати керування ресурсами.

Віддалені бібліотеки (№2–№5/6) мають аналогічну базову структуру, що включає маршрутизатор (R2–R5), міжмережевий екран з підтримкою IPSec та access switch для підключення кінцевих пристроїв. Кожна філія також організовує локальні VLAN-сегменти (admin, librarians, users, Wi-Fi, VoIP), що забезпечує уніфіковану модель побудови мережі в усіх підрозділах. Для кожного віддаленого вузла призначено унікальну публічну IP-адресу (203.0.113.1–203.0.113.5), яка використовується як точка ініціалізації VPN-тунелю.

Нижче наведено набір конфігураційних налаштувань і команд для реалізації IPSec VPN між центральною бібліотекою та філіями (як у твоїй схемі). Я подаю це у вигляді логічної структури: R1 (центр) ↔ R2/R3/R4/R5 (філії).

IP-адресація обладнання на схемі:

- R1 (центральна): 203.0.113.1;
- R2 (філія): 203.0.113.2;
- R3: 203.0.113.3;
- R4: 203.0.113.4;
- R5: 203.0.113.5.

Внутрішні мережі:

- Central LAN: 10.0.0.0/16;
- Branch LAN: 10.1.0.0/16 (кожна філія своя підмережа).

Зв'язок між центральною бібліотекою та філіями реалізовано через Інтернет із застосуванням IPSec VPN-тунелів, що забезпечують конфіденційність, цілісність та автентифікацію переданих даних.

Тунелі формуються між міжмережевими екранами кожного вузла, утворюючи зашифровані канали передачі інформації. На схемі також наведено параметри IPSec-конфігурації: використання IKEv2 як протоколу обміну ключами, алгоритму шифрування AES-256, хешування SHA-256, групи Діффі-

Геллмана DH Group 14, часу життя сеансу (Lifetime) 3600 секунд та режиму Tunnel, що є типовим для site-to-site VPN.

R1 (центральний маршрутизатор);

```
crypto isakmp policy 10
  encryption aes 256
  hash sha256
  authentication pre-share
  group 14
  lifetime 3600
```

Pre-shared key (для кожної філії):

```
crypto isakmp key VPN_KEY address 203.0.113.2
crypto isakmp key VPN_KEY address 203.0.113.3
crypto isakmp key VPN_KEY address 203.0.113.4
crypto isakmp key VPN_KEY address 203.0.113.5
```

R1 (окремо для кожної філії):

```
crypto map VPN-MAP 10 ipsec-isakmp
  set peer 203.0.113.2
  set transform-set TS
  match address 100
crypto map VPN-MAP 20 ipsec-isakmp
  set peer 203.0.113.3
  set transform-set TS
  match address 110
crypto map VPN-MAP 30 ipsec-isakmp
  set peer 203.0.113.4
  set transform-set TS
  match address 120
crypto map VPN-MAP 40 ipsec-isakmp
  set peer 203.0.113.5
  set transform-set TS
  match address 130
```

Маршрутизатор R1. ACL (який трафік шифрується):

```
access-list 100 permit ip 10.0.0.0 0.0.255.255 10.1.1.0
0.0.0.255
```

```

access-list 110 permit ip 10.0.0.0 0.0.255.255 10.1.2.0
0.0.0.255
access-list 120 permit ip 10.0.0.0 0.0.255.255 10.1.3.0
0.0.0.255
access-list 130 permit ip 10.0.0.0 0.0.255.255 10.1.4.0
0.0.0.255

```

Застосування crypto map на інтерфейс:

```

interface GigabitEthernet0/0
ip address 203.0.113.1 255.255.255.0
crypto map VPN-MAP

```

Налаштування філій (R2–R5) на прикладі R2 (аналогічно для інших):

```

crypto isakmp policy 10
  encryption aes 256
  hash sha256
  authentication pre-share
  group 14
  lifetime 3600
crypto isakmp key VPN_KEY address 203.0.113.1
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
  mode tunnel
crypto map VPN-MAP 10 ipsec-isakmp
  set peer 203.0.113.1
  set transform-set TS
  match address 100
access-list 100 permit ip 10.1.1.0 0.0.0.255 10.0.0.0
0.0.255.255
interface GigabitEthernet0/0
ip address 203.0.113.2 255.255.255.0
crypto map VPN-MAP

```

Таким чином, представлена архітектура забезпечує інтеграцію територіально розподілених бібліотечних підрозділів у єдину захищену мережу з централізованим управлінням та уніфікованою політикою безпеки. Використання VLAN дозволяє логічно розмежовувати внутрішні сервіси, а IPSec

VPN гарантує безпечну взаємодію між віддаленими сегментами через публічну мережу Інтернет.

Запропонована мережева модель є масштабованою, безпечною та технологічно обґрунтованою для використання в розподілених організаціях. Вона забезпечує високий рівень захисту даних завдяки IPSec, ефективну сегментацію трафіку за допомогою VLAN та централізоване адміністрування всієї інфраструктури. Такий підхід підвищує надійність обміну інформацією між бібліотеками, спрощує керування мережею та створює основу для подальшого розширення системи без суттєвої перебудови архітектури.

ВИСНОВКИ

У ході переддипломної практики успішно вирішено основні завдання проєктування, здійснено комплексний аналіз принципів побудови розподілених мережевих систем та розроблено концептуальну модель мережевої інфраструктури для об'єднання бібліотек міста в єдиний інформаційний простір. Особливу увагу приділено аналізу сучасних підходів до організації корпоративних мереж, а також ролі технологій VLAN та VPN у забезпеченні гнучкості, масштабованості та безпеки мережевих рішень.

У межах роботи розглянуто особливості логічної сегментації мережі за допомогою VLAN, що дозволяє ефективно розподіляти трафік між різними функціональними підрозділами бібліотечної системи. Також проаналізовано принципи побудови захищених каналів зв'язку на основі VPN, які забезпечують безпечну взаємодію між віддаленими бібліотечними вузлами через публічні мережі.

Розроблена архітектура розподіленої мережі передбачає централізоване управління ресурсами, оптимізацію інформаційних потоків та підвищення рівня інформаційної безпеки. Запропоноване рішення дозволяє забезпечити стабільну роботу мережевих сервісів, ефективне використання пропускної здатності каналів зв'язку та логічну ізоляцію окремих сегментів мережі.

Таким чином, можна зробити висновок, що використання технологій VLAN та VPN є доцільним та ефективним підходом при проєктуванні розподіленої мережі бібліотек міста. Реалізація запропонованої моделі сприятиме підвищенню рівня цифровізації бібліотечних послуг, покращенню якості доступу до інформаційних ресурсів та забезпеченню належного рівня захисту даних у межах єдиної інформаційної системи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Шлапик О. А., Киричек Г. Г. Моделирование распределенной сети библиотеки с использованием среды Cisco Packet Tracer // Тижень науки–2026. Факультет комп'ютерних наук і технологій : тези доповідей наук.-практ. конф., м. Запоріжжя, 13–17 квіт. 2026 р. / редкол.: В. Шаломєєв (відп. ред.). Запоріжжя : НУ «Запорізька політехніка», 2026.
2. Thavi R., Jhaveri R., Narwane V., Gardas B., Jafari Navimipour N. Role of cloud computing technology in the education sector. *Journal of Engineering, Design and Technology*, 2024. 22.1. pp. 182–213.
3. Киричек Г.Г., Тягунова М.Ю., Братчиков В.В. Система кешування даних в розгалуженій мікросервісній архітектурі *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*. 2024. Том 35 (74) №1. Ч.1. С.141-146. DOI: 10.32782/2663-5941/2024.1.1/21.
4. Zhang Y., Wang L., Liu D., Su Y., Zhu Y., Zhang X. Design of Information Security Protection System for Cloud Business System. In: *International Conference on Artificial Intelligence and Communication Technology*. Singapore: Springer Nature Singapore, 2023. P. 105-122.
5. Wood, M. J. Study of Network Design Considerations for Small Businesses. *IOARP Journal of Communication and Networks (IOARP JCN)*, 2023, 3.1. pp.38-56.
6. Киричек Г.Г., Тягунова М.Ю., Шлапик О.А. Метод децентралізованого керування комп'ютерними системами. VII Міжнародна науково-практична конференція Таврійського національного університету імені В. І. Вернадського до 175-ї річниці від дня народження Ісмаїла Гаспринського. (Київ, 31 бер. 2026). Київ, Україна, 2026.
7. Kaur L., Kaur R. A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm. *Global Transitions Proceedings*. 2021. Vol. 2(2). P. 520–529. DOI: 10.1016/j. gltp.2021.08.001.

8. Ruaya E. P., Buladaco M. V. M. Virtual local area network (vlan) network design for nemsu-administration building. *International Journal*, 2022, 11.6. pp. 294-298.
9. Balachandran S., Dominic J., Sivankalai S. Comparative Analysis of VPN and Proxy Protocols in Library Network Management. *Library of Progress-Library Science, Information Technology & Computer*, 2024, 44.3. pp. 20-28.
10. Forbacha S. C., Agwu M. J. A. Design and implementation of a secure virtual private network over an open network (Internet). *American Journal of Technology*, 2023, 2.1: pp. 1-36.
11. Ogunyanda K., Ogunyanda O. O., Familua A. D., Shongwe T., Swart T. G., Cheng L. Wi-Fi 6 Data Transmission over a Low-Voltage Power Line Channel: Implementation and Analysis. *Journal of Communications*, 2025, 20.3: 315-323. DOI: 10.12720/jcm.20.3.315-323.
12. Дира В. В. Огляд взаємодії технологій ethernet і wifi у корпоративних телекомунікаційних мережах. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, 2024. 35 (74). № 3. С. 37-44. DOI: 10.32782/2663-5941/2024.3.2/05.
13. Wu X., O'Brien D. C. Parallel transmission LiFi. *IEEE Transactions on Wireless Communications*. 2020. № 19 (10). P. 6268–6276. DOI: 10.1109/TWC.2020.3001983.
14. Киричек Г.Г., Школовий В.В. Забезпечення відмовостійкості та надійності мереж передачі даних. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*. 2026. Том 37 (76) №1. Ч.2. С.128-134. DOI: 10.32782/2663-5941/2026.1.2/17.
15. Kumar S., Singh M., Gupta A., Tiwari M., Shadab A. Designing a Secure Campus Area Network with an Advanced DNS System. In: 2025 7th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2025. P. 1051-1056.
16. Zhong M., Xie W., Yang L. The Optimization and Improvement of Campus Network Based on MSTP. In: 2023 4th International Conference on Computers and Artificial Intelligence Technology (CAIT). IEEE, 2023. P. 212-216.

17. Киричек Г.Г., Живогляд В.А., Тягунова М.Ю. Система моніторингу мереж із підтримкою передачі повідомлень. Таврійський науковий вісник. Серія: Технічні науки. 2026. №1. Ч.1. С.122-130. DOI: 10.32782/tnv-tech.2026.1.1.14.
18. Prajapati D., Bowman J., Suvarna N. Designing Real-World Multi-domain Networks. Cisco Press, 2024. 456 p.
19. Sangoleye F., Johnson J., Chavez A., Tsiropoulou E. E., Marton N. L., Hentz C. R., Yannarelli A. Networked microgrid cybersecurity architecture design guide: A new jersey transitgrid use case. Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2022. 68 p. DOI: 10.2172/1900087.
20. Tiahunova M., Kyrychek H., Bohatyrova T., Moshynets D. System and method of automatic collection of objects in the room. Paper presented at the *CEUR Workshop Proceedings*, 2021. Vol-3077. P. 174-186. URL: <https://ceur-ws.org/Vol-3077/paper10.pdf> (дата звернення: 25.04.2026).
21. Li X., Yao L. Multi VLAN reliable and efficient campus network design. In: Third International Symposium on Computer Engineering and Intelligent Communications (ISCEIC 2022). SPIE, 2023. p. 243-248.

ДОДАТОК А
ЛОГІЧНА СХЕМА МЕРЕЖІ

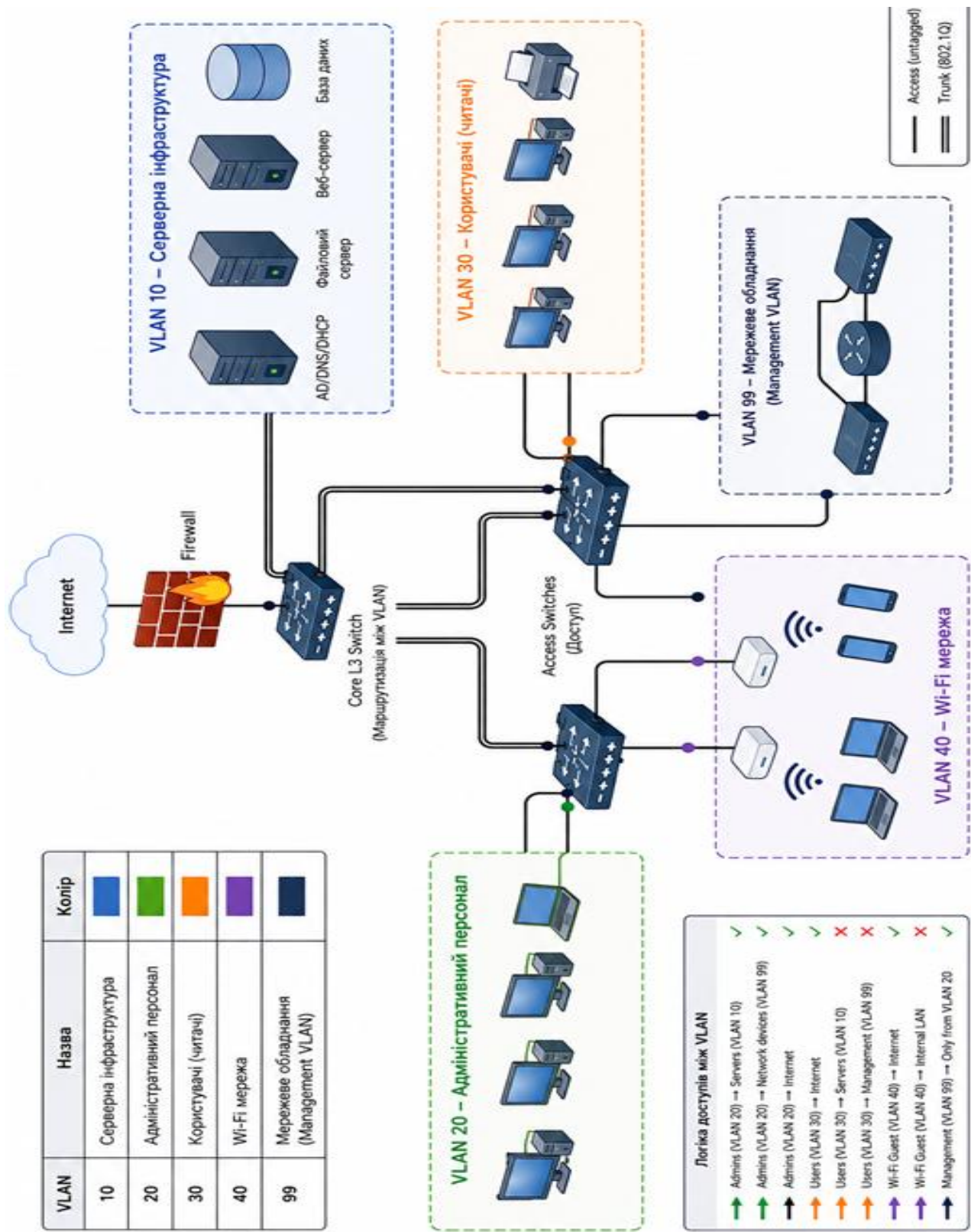


Рисунок А.1 – Логічна схема мережі

ДОДАТОК Б

СЛАЙДИ ПРЕЗЕНТАЦІЇ

Проектування розподіленої мережі бібліотек міста з використанням VLAN та VPN

Студент: Шлапик О.А.
Спеціальність: 123 Комп'ютерна інженерія
Керівник: доцент Киричек Г.Г.
2026 рік

Рисунок Б.1 – Слайд 1

Актуальність теми

Актуальність теми обумовлена активною цифровізацією бібліотечної сфери та зростанням потреби у швидкому доступі до електронних ресурсів і онлайн-сервісів.

Сучасні бібліотеки потребують інтеграції в єдину інформаційно-комунікаційну систему, оскільки існуючі рішення часто працюють розрізнено та не забезпечують ефективного обміну даними.

Впровадження розподіленої мережі дозволяє організувати централізоване управління ресурсами та підвищити продуктивність роботи.

Використання технологій VLAN і VPN забезпечує необхідний рівень безпеки та надійності передачі інформації.

Рисунок Б.2 – Слайд 2

Мета роботи, об'єкт та завдання

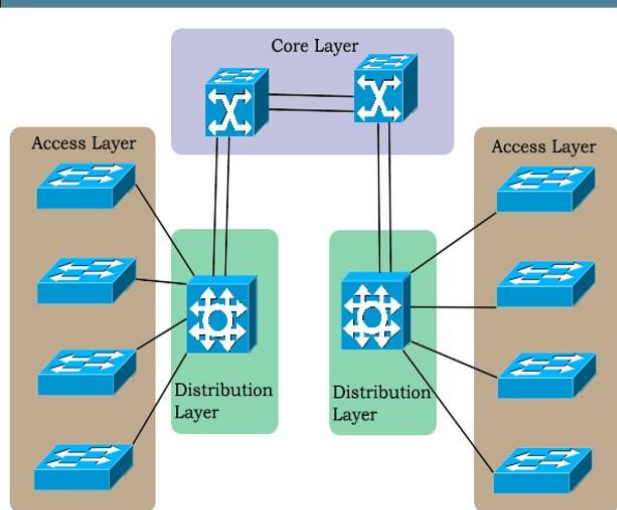
Мета роботи: проектування архітектури та впровадження принципів організації розподіленої мережі бібліотек міста з використанням технологій VLAN і VPN. Об'єктом розробки є процес проектування інформаційно-комунікаційної мережі міських бібліотек та організації розподіленої мережевої інфраструктури з використанням VLAN та VPN.

Основні завдання:

- аналіз мережевих технологій
- дослідження VLAN і VPN
- розробка архітектури мережі
- вибір обладнання
- забезпечення інформаційної безпеки

Рисунок Б.3 – Слайд 3

Архітектура мережі



- Мережа побудована за багаторівневою моделлю Core–Distribution–Access - ефективний розподіл функцій між мережевими пристроями.
- Центральний рівень (Core) відповідає за обробку та маршрутизацію трафіку, рівень розподілу (Distribution) забезпечує агрегацію та керування потоками даних, а рівень доступу (Access) відповідає за підключення кінцевих користувачів.

Рисунок Б.4 – Слайд 4

Порівняння мережевих рішень

Тип рішення	Основні характеристики	Переваги	Обмеження	Доцільність використання
Локальна мережа без сегментації	Єдина мережа без VLAN, базова маршрутизація	Простота реалізації, низька вартість	Відсутність ізоляції, складність контролю доступу, низька масштабованість	Невеликі бібліотеки
VLAN + L3 комутація	Логічне розділення мережі, маршрутизація між сегментами	Кращий контроль трафіку, підвищена безпека, гнучкість	Потребує налаштування та керованого обладнання	Міські бібліотечні мережі
MikroTik-рішення	Єдиний пристрій із функціями маршрутизації, VPN, firewall	Доступність, гнучкість налаштувань	Обмеження при великому навантаженні	Філії, невеликі вузли
Корпоративні рішення (Cisco, HPE)	Високопродуктивне обладнання з розширеними функціями	Надійність, масштабованість, централізоване управління	Висока вартість, складне адміністрування	Центральний вузол мережі
Хмарні рішення	Розміщення сервісів у віддалених дата-центрах	Гнучке масштабування, зменшення локальної інфраструктури	Залежність від інтернету, сумнівна безпека даних	Додаткові сервіси
SDN / SD-WAN	Програмно-керована мережа, централізоване управління	Гнучкість, оптимізація трафіку	Складність впровадження	Перспективний розвиток

Рисунок Б.5 – Слайд 5

Технології

Технологія	Швидкість	Середовище	Переваги	Недоліки	Альтернативи
100Base-TX	до 100 Мбіт/с	Вита пара Cat5e	Низька вартість, проста реалізація	Обмежена пропускна здатність	1000Base-T
1000Base-T	до 1 Гбіт/с	Вита пара Cat5e/Cat6	Висока швидкість, сумісність	Вища вартість обладнання	10GBase-T
1000Base-LX	до 1 Гбіт/с	Оптоволокно	Велика дальність, завадостійкість	Висока вартість інсталяції	10GBase-LR

Стандарт	Швидкість	Частота	Переваги	Недоліки
802.11n (Wi-Fi 4)	до 600 Мбіт/с	2.4/5 ГГц	Сумісність, дешевизна	Нижча продуктивність
802.11ac (Wi-Fi 5)	до 3.5 Гбіт/с	5 ГГц	Висока швидкість	Обмежене покриття
802.11ax (Wi-Fi 6)	до 9.6 Гбіт/с	2.4/5 ГГц	Висока щільність користувачів	Вища вартість

Рисунок Б.6 – Слайд 6

Структурна схема мережі

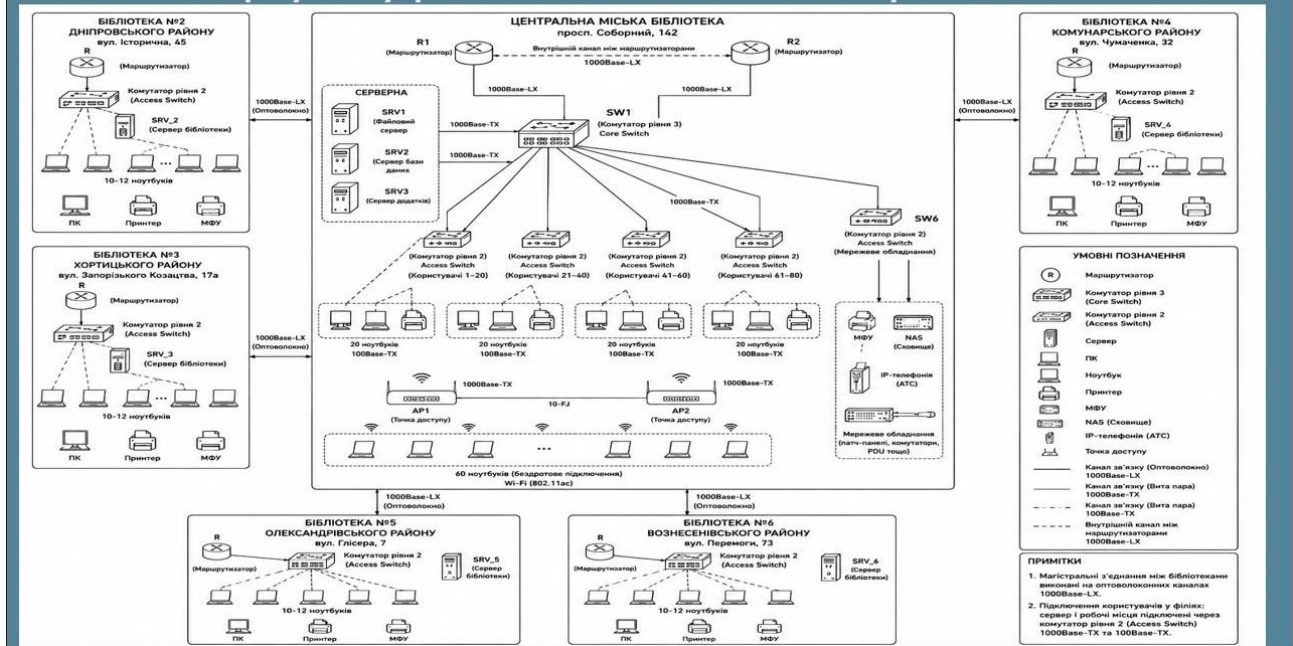


Рисунок Б.7 – Слайд 7

Мережеве обладнання

У проєкті використовується корпоративне мережеве обладнання, яке забезпечує стабільну та надійну роботу інфраструктури:

- маршрутизатори для резервування та підключення до зовнішніх мереж
- L3-комутатор для міжVLAN маршрутизації
- комутатори доступу для кінцевих пристроїв
- сервери баз даних, файлів та застосунків
- бездротові точки доступу Wi-Fi 6
- система резервного живлення (UPS)

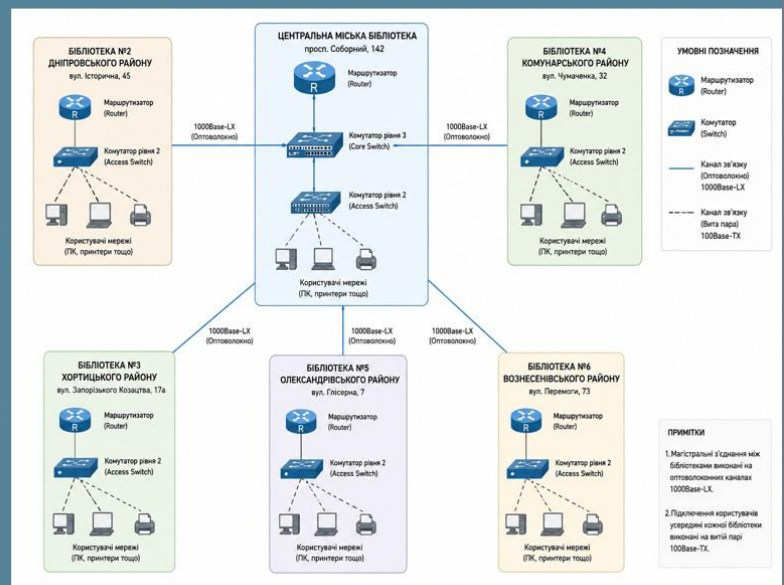


Рисунок Б.8 – Слайд 8

VLAN

- ▶ Технологія VLAN використовується для логічного розділення мережі на окремі сегменти незалежно від фізичної структури. Це дозволяє підвищити рівень інформаційної безпеки, зменшити широкомовний трафік та спростити адміністрування мережі.
- ▶ У проєкті передбачено такі VLAN:
 - VLAN серверної інфраструктури
 - VLAN адміністративного персоналу
 - VLAN користувачів
 - VLAN бездротового доступу

Рисунок Б.9 – Слайд 9

VPN

- ▶ Технологія VPN використовується для забезпечення захищеного з'єднання між центральною бібліотекою та її філіями.
- ▶ У проєкті передбачено:
 - IPsec VPN для з'єднання між філіями
 - SSL VPN для віддаленого доступу користувачів

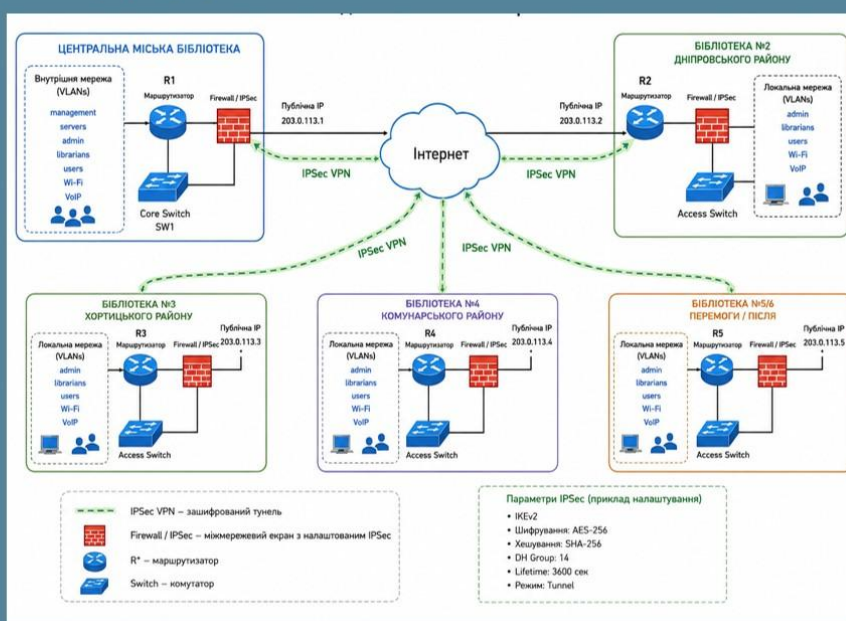


Рисунок Б.10 – Слайд 10

Висновки

- У результаті виконання роботи розроблено логічну та структурну схеми розподіленої мережі бібліотек міста з використанням сучасних мережевих технологій.
- Запропонована архітектура базується на багаторівневій моделі Core–Distribution–Access, яка забезпечує масштабованість, керованість та ефективний розподіл мережевого трафіку.
- Використання технології VLAN дозволяє логічно сегментувати мережу та підвищити рівень її безпеки, а впровадження VPN забезпечує захищений обмін даними між віддаленими підрозділами.
- Отримані результати підтверджують доцільність застосування запропонованих рішень для побудови сучасної інформаційної інфраструктури бібліотечної системи.

Рисунок Б.11 – Слайд 11

Публікації за темою роботи

1. Шлапик О. А., Киричек Г. Г. Моделирование распределенной сети библиотеки с использованием срединища Cisco Packet Tracer // Тиждень науки–2026. Факультет комп'ютерних наук і технологій : тези доповідей наук.-практ. конф., м. Запоріжжя, 13–17 квіт. 2026 р. / редкол.: В. Шаломєєв (відп. ред.). Запоріжжя : НУ «Запорізька політехніка», 2026
2. Киричек Г.Г., Тягунова М.Ю., Шлапик О.А. Метод децентралізованого керування комп'ютерними системами. VII Міжнародна науково-практична конференція Таврійського національного університету імені В. І. Вернадського до 175-ї річниці від дня народження Ісмаїла Гаспринського. (Київ, 31 бер. 2026). Київ, Україна, 2026.

Рисунок Б.12 – Слайд 12