

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ  
Циклова комісія (кафедра) комп'ютерної інженерії та інформаційних технологій

**КВАЛІФІКАЦІЙНА РОБОТА**  
на тему  
**ПРОЕКТУВАННЯ ТА ОПТИМІЗАЦІЯ ЛОКАЛЬНИХ  
ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ**

Виконав: студент групи 1К-21

Спеціальності 123 Комп'ютерна інженерія

Євген КОНОПЛЯСТИЙ

Керівник:

Павло РАТАЙЧУК

Черкаси 2025

# ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерна інженерія

## ЗАТВЕРДЖУЮ

Завідувач кафедри КІ та ІТ

Владислав ХОТУНОВ

(підпис)

« \_\_\_\_\_ » \_\_\_\_\_ 2024 р.

## ЗАВДАННЯ

### НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Коноплястому Євгенію Дмитровичу

1. Тема кваліфікаційної роботи «Проектування та оптимізація локальних обчислювальних мереж»

Керівник роботи Ратайчук Павло Єгорович, викладач методист

затверджені наказом закладу вищої освіти від «07» жовтня 2024 року № 68у.

2. Строк подання студентом кваліфікаційної роботи 02.06.2025

3. Вихідні дані до кваліфікаційної роботи Розробка методології проектування та оптимізації локальних обчислювальних мереж, аналіз їх продуктивності, безпеки та масштабованості.

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Дослідити основні принципи проектування локальних обчислювальних мереж, проаналізувати сучасні архітектури ЛОМ (класична модель, spine-leaf, SDN), оцінити вимоги до продуктивності, надійності та безпеки мережі, розглянути методи оптимізації мережевого трафіку та балансування навантаження, виконати практичне моделювання локальної обчислювальної мережі з урахуванням факторів продуктивності та безпеки, проаналізувати ефективність оптимізаційних заходів та надати рекомендації щодо покращення роботи мережі.

5. Дата видачі завдання 16.09.2024 р.

## КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами керівника і студента
1	Вступ	14.10.2024	
2	Розділ 1 (АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ, МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ LAN.)	9.12.2024	
3	Розділ 2 (ОПТИМІЗАЦІЯ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ)	10.03.2025	
4	Розділ 3 (МОДЕЛЮВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ)	28.04.2025	
5	Висновки	12.05.2025	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2025	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2025	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент \_\_\_\_\_  
(підпис)

Євгеній КОНОПЛЯСТИЙ

Керівник роботи \_\_\_\_\_  
(підпис)

Павло РАТАЙЧУК

## АНОТАЦІЯ

У кваліфікаційній роботі розглянуто теоретичні та практичні аспекти проектування і оптимізації локальних обчислювальних мереж (ЛОМ), які є основою функціонування сучасних інформаційних систем.

Метою дослідження є розробка ефективної моделі ЛОМ з урахуванням вимог до надійності, масштабованості, продуктивності та безпеки. Робота містить аналіз існуючих методів проектування, вибір топології, технічних засобів і програмного забезпечення для побудови мережі.

Особливу увагу приділено питанням оптимізації — мінімізації затримок, підвищенню пропускної здатності та ефективному використанню ресурсів мережі. У процесі дослідження використано методи моделювання, аналізу трафіку, розрахунку мережевих параметрів, а також засоби віртуалізації та симуляції.

На основі отриманих результатів запропоновано рекомендації щодо підвищення ефективності функціонування ЛОМ у різних типах організацій. Результати роботи можуть бути застосовані під час створення нових або модернізації існуючих мережевих інфраструктур.

## **ABSTRACT**

This qualification thesis examines the theoretical foundations and practical approaches to the design and optimization of local area networks (LANs), which serve as the core of modern information systems.

The primary objective of the study is to develop an efficient LAN model that meets key requirements such as reliability, scalability, performance, and security.

The research includes an analysis of existing design methodologies, the selection of appropriate network topologies, hardware, and software tools for network deployment.

Particular attention is given to optimization techniques aimed at reducing latency, increasing bandwidth, and improving resource utilization. The study applies methods of network modeling, traffic analysis, parameter calculation, as well as tools for virtualization and simulation.

Based on the results obtained, practical recommendations are proposed for enhancing the performance and efficiency of LANs in various organizational settings. The outcomes of the thesis can be effectively used in the development or modernization of network infrastructures.

## ЗМІСТ

Вступ.....	<b>Ошибка! Закладка не определена.</b>
Розділ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ, МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ LAN .....	<b>Ошибка! Закладка не определена.</b>
1.1. Основні технології LAN, сучасні вимоги до локальних мереж .....	<b>Ошибка! Закладка не определена.</b>
1.2. Етапи проектування локальної мережі .....	6
1.3 Розробка архітектури мережі .....	8
1.4 Вибір активного мережевого обладнання .....	10
Розділ 2. ОПТИМІЗАЦІЯ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ .....	<b>Ошибка! Закладка не определена.</b>
2.1 Методи підвищення продуктивності мережі .....	<b>Ошибка! Закладка не определена.</b>
2.2. Підвищення надійності та стійкості.....	15
2.3. Безпека LAN .....	18
2.4 Розробка логічної схеми локальної мережі .....	21
Розділ 3 МОДЕЛЮВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ	<b>Ошибка! Закладка не определена.</b>
3.1 Вибір мережевого обладнання відповідно до проєкту.	<b>Ошибка! Закладка не определена.</b>
3.3 Налаштування комутаторів та маршрутизатора .....	<b>Ошибка! Закладка не определена.</b>
3.4 Тестування з'єднання між VLAN .....	<b>Ошибка! Закладка не определена.</b>
3.5 Впровадження безпеки в сегментованій мережі: ACL та VPN .....	<b>Ошибка! Закладка не определена.</b>
3.6 Моніторинг та усунення неполадок у локальній мережі ..	<b>Ошибка! Закладка не определена.</b>
ВИСНОВКИ.....	<b>Ошибка! Закладка не определена.</b>
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....	<b>Ошибка! Закладка не определена.</b>

## ВСТУП

**Актуальність обраної теми.** У сучасному інформаційному суспільстві локальні обчислювальні мережі (ЛОМ, англ. LAN – Local Area Network) відіграють ключову роль у забезпеченні ефективної взаємодії між користувачами, обчислювальними пристроями та ресурсами організацій. З огляду на стрімкий розвиток цифрових технологій, виникає необхідність не лише створення нових мереж, а й удосконалення існуючих з метою забезпечення високої продуктивності, надійності та безпеки.

Проектування локальних мереж охоплює широкий спектр питань: вибір оптимальної топології, конфігурація обладнання, планування кабельної інфраструктури, налаштування протоколів зв'язку. Ці аспекти є критично важливими для стабільної та масштабованої роботи організації. Водночас оптимізація вже створених ЛОМ дозволяє покращити їхню ефективність, зменшити затримки передачі даних, збільшити пропускну здатність та забезпечити стійкість до збоїв або навмисних атак.

На сьогоднішній день локальні мережі використовуються практично в усіх сферах діяльності: в освітніх установах, державних органах, медичних установах, торгових та промислових підприємствах. Саме тому актуальність дослідження, присвяченого проектуванню та оптимізації ЛОМ, не викликає сумнівів. Невірне проектування чи нехтування безпековими стандартами може призвести до серйозних фінансових та репутаційних втрат.

**Метою роботи** Метою даної кваліфікаційної роботи є розробка ефективного проєкту локальної обчислювальної мережі з подальшою оптимізацією її ключових характеристик: продуктивності, надійності, безпеки та рентабельності.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- дослідити сучасні технології локальних мереж, їхні характеристики та сфери застосування;

- проаналізувати методологію проектування ЛОМ;
- обґрунтувати вибір архітектури, топології та обладнання для побудови мережі;
- вивчити методи підвищення продуктивності, безпеки та стійкості;
- змодельовати розроблену мережу за допомогою спеціалізованого програмного забезпечення;
- провести економічний аналіз проєкту;
- реалізувати та протестувати мережу на відповідність вимогам;
- створити документацію для супроводу та обслуговування ЛОМ.

**Об'єктом дослідження** є процес проектування та оптимізації локальних обчислювальних мереж.

**Предметом дослідження** виступають методи, засоби та інструменти, що використовуються для побудови ефективної інфраструктури ЛОМ.

**Практична значущість** роботи полягає в тому, що результати дослідження можуть бути застосовані для створення нових або модернізації існуючих мереж у реальних умовах: у навчальних закладах, офісних приміщеннях, лікарнях, адміністративних структурах. Запропоновані рішення є актуальними з позицій сучасних технологій і відповідають вимогам безпеки, масштабованості та енергоефективності.

**Структура роботи** включає вступ, три розділи, висновки, список використаних джерел.

## РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ, МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ LAN

### 1.1 Основні технології LAN, сучасні вимоги до локальних мереж

Локальні обчислювальні мережі (LAN — Local Area Network) є основою корпоративної інформаційної інфраструктури. Вони забезпечують ефективну передачу даних між комп'ютерами, периферійними пристроями, серверами в межах обмеженої території — офісу, установи або навчального закладу.

У XXI столітті розвиток технологій LAN відбувається стрімко. Поява нових стандартів, зростання кількості пристроїв, перехід на гігабітні швидкості й інтеграція бездротових технологій зробили локальні мережі універсальним інструментом для бізнесу, освіти, медицини, державного управління.

#### Основні технології LAN

На сьогодні найпоширенішими технологіями в реалізації локальних мереж є:

- Ethernet — дротова технологія (стандарт IEEE 802.3), яка забезпечує швидкості від 10 Мбіт/с до 100 Гбіт/с. Сучасні мережі, як правило, реалізуються на базі Gigabit Ethernet (1 Гбіт/с) або 10 Gigabit Ethernet (10 Гбіт/с).
- Wi-Fi — бездротова технологія передачі даних (стандарти IEEE 802.11n/ac/ax), яка дозволяє забезпечити мобільність та гнучкість мережевої інфраструктури без прокладання кабелів.
- Power over Ethernet (PoE) — передача живлення через Ethernet-кабель разом із даними, що дозволяє жити IP-камери, точки доступу, телефони без окремих блоків живлення.
- VLAN (Virtual LAN) — логічне розділення фізичної мережі на окремі сегменти для підвищення безпеки та організаційної структури трафіку.



Рисунок 1.1 – Приклад гібридної LAN-мережі на базі Ethernet і Wi-Fi  
 Протоколи LAN. Фундаментом будь-якої LAN є TCP/IP стек протоколів, який включає:

- IP (Internet Protocol) — визначає адресацію пристроїв у мережі. IPv4 (32-біт) є найпоширенішим, проте через вичерпання адрес дедалі частіше впроваджується IPv6 (128-біт).
- TCP (Transmission Control Protocol) — забезпечує гарантовану доставку даних.
- UDP (User Datagram Protocol) — забезпечує швидку передачу, менш надійну, але більш ефективну для відео або голосу.

Таблиця 1.1 – Порівняння IPv4 та IPv6

Параметр	IPv4	IPv6
Довжина адреси	32 біти	128 біт
Формат адреси	Десятковий (192.168.1.1)	Шістнадцятковий (fe80::1)
Кількість адрес	≈4,3 млрд	≈3,4x10 <sup>38</sup>
Безпека	Опційно (IPsec)	Вбудована

Вимоги до сучасних локальних мереж. Щоб LAN відповідала потребам організації, вона має задовольняти такі вимоги:

- Продуктивність — забезпечення необхідної пропускної здатності для всіх користувачів. Стандартом вважається використання Gigabit Ethernet, комутаторів з високою швидкістю комутації.

- Масштабованість — можливість подальшого розширення мережі без її перебудови. Забезпечується використанням керованих комутаторів, резервом портів, логічним поділом на VLAN.
- Надійність — відмовостійкість досягається через резервування каналів зв'язку, дублювання обладнання, UPS, протоколи STP/RSTP.
- Безпека — впровадження контролю доступу (802.1X), фільтрації MAC-адрес, шифрування трафіку (WPA3 для Wi-Fi), використання брандмауерів і VPN.
- Мобільність — підтримка бездротових сегментів, roaming між точками доступу.
- Управління та моніторинг — централізоване адміністрування з використанням SNMP, NetFlow, систем візуального моніторингу.

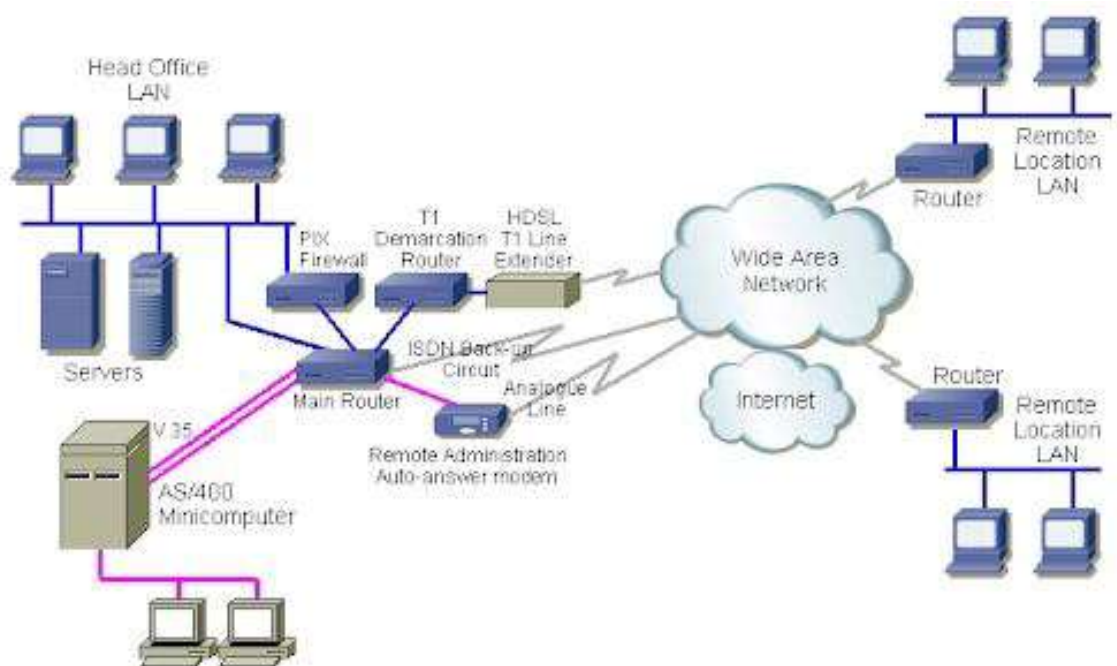


Рисунок 1.2 – Модель сучасної LAN

Таким чином, сучасні локальні мережі — це комплексне поєднання технологій, протоколів та архітектур, які мають бути правильно спроектовані та адаптовані до потреб установи. Висока швидкість, масштабованість, стабільність і безпека є ключовими критеріями ефективності LAN у XXI

столітті.

## **1.2 Етапи проектування локальної мережі**

Проектування локальної мережі — це системний процес, який складається з декількох послідовних етапів. Кожен з них відіграє важливу роль у забезпеченні ефективності, надійності та масштабованості майбутньої IT-інфраструктури. Від правильного проходження кожного етапу залежить успішність реалізації проєкту в цілому.

Першим і ключовим кроком є

### **1. Збір вимог.**

Цей етап включає аналіз потреб організації або установи. З'ясовується кількість майбутніх користувачів, типи пристроїв (ПК, ноутбуки, принтери, сервери, IP-телефони), обсяг трафіку, типові сценарії використання мережі (офісна робота, доступ до баз даних, відеонагляд, VoIP-зв'язок тощо). Також враховується фізичне розміщення робочих місць і план приміщення. Важливо визначити й майбутні вимоги: передбачуване розширення, збільшення трафіку або підключення нових підрозділів.

### **2. Аналіз існуючої інфраструктури.**

Якщо проєкт розробляється для модернізації чинної мережі, виконується аудит наявного обладнання, кабельної інфраструктури, комутації, серверного парку. Виявляються вузькі місця, слабкі точки, зони з надмірним навантаженням, вразливості безпеки. За результатами формується звіт із пропозиціями щодо збереження, оновлення або демонтажу елементів мережі.

### **3. Визначення топології та зонування.**

На цьому етапі обирається логічна та фізична топологія мережі (зірка, дерево, гібридна структура), визначаються точки підключення, мережеві сегменти (VLAN), принципи зонування (користувацька зона, серверна зона, DMZ). Планується розміщення активного мережевого обладнання (комутаторів, маршрутизаторів, точок доступу).

#### 4. Розробка технічного завдання (ТЗ).

Формується офіційний документ, який включає перелік вимог до мережі, технічні параметри, обсяги трафіку, типи кабельних ліній (UTP, FTP, оптоволокно), рівень безпеки, резервування, інтерфейси обладнання, кількість портів. У ТЗ закладається базовий обсяг інвестицій, терміни реалізації, очікувані результати. Документ погоджується між зацікавленими сторонами — замовником, ІТ-відділом, підрядником.

#### 5. Вибір стандартів та технологій.

На основі вимог і ТЗ обираються стандарти Ethernet (Fast/Gigabit/10G), протоколи передачі, IP-адресація (IPv4 або IPv6), засоби шифрування, методи автентифікації. Також визначається доцільність використання технологій типу PoE, VLAN, VPN.

#### 6. Підготовка схематичних креслень.

Розробляється план мережі — схема розташування кабелів, обладнання, комутаційних панелей, трасування. Ці креслення використовуються монтажниками та системними адміністраторами на етапах реалізації та обслуговування.

#### 7. Узгодження бюджету і матеріалів.

На завершальному етапі проектування готується кошторис, який враховує витрати на обладнання, кабелі, засоби кріплення, програмне забезпечення, монтаж, налаштування та навчання персоналу. Після затвердження починається етап реалізації.

Таким чином, етапи проектування локальної мережі є багаторівневим процесом, що включає технічний, економічний, організаційний і логістичний компоненти. Лише системний підхід гарантує отримання ефективної, стабільної та безпечної ІТ-інфраструктури, що відповідатиме потребам установи.



Рисунок 1.3 – Основні етапи проектування локальної мережі у вигляді блок-схеми

### 1.3 Розробка архітектури мережі

При проектуванні локальних мереж важливо обрати відповідну топологію — логічну або фізичну структуру з'єднання вузлів. Вибір залежить від кількості користувачів, потреб у продуктивності, надійності, бюджету та вимог

до масштабованості. Топологія визначає, як пристрої зв'язуються між собою, передають дані та реагують на відмови.

До основних типів топологій належать:

#### 1. Зіркоподібна топологія (Star Topology)

Усі пристрої підключаються до центрального комутатора (switch) або концентратора (hub).

Переваги: легкість у діагностиці та локалізації несправностей, відмова одного вузла не впливає на всю мережу, просте розширення.

Недоліки: центральна точка — критичний елемент (у разі її відмови мережа виходить з ладу), потребує багато кабельної продукції.

#### 2. Шинна топологія (Bus Topology)

Усі вузли підключаються до одного загального кабелю (шини).

Переваги: простота реалізації, економічність (мінімум кабелів).

Недоліки: складність в ізоляції помилок, можливі колізії сигналів, погано масштабується.

3. Кільцева топологія (Ring Topology) Кожен вузол з'єднаний із двома сусідніми, утворюючи кільце. Дані передаються по колу.

Переваги: відсутність колізій при використанні маркерної передачі, чіткий контроль трафіку.

Недоліки: відмова одного вузла може зупинити всю мережу (якщо немає механізмів резервування), складність у реалізації та відновленні.

#### 4. Деревоподібна топологія (Tree Topology)

Ієрархічне розгалуження з головним комутатором (root switch) та підлеглими вузлами.

Переваги: зручно для організації великих структур (кампусів, офісів), логічна побудова VLAN.

Недоліки: перевантаження магістралі може вплинути на нижчі рівні, складність у фізичній реалізації.

#### 5. Повнозв'язна топологія (Mesh Topology)

Кожен вузол підключений до всіх інших. Використовується у критичних

системах.

Переваги: найвища надійність та відмовостійкість, відсутність «єдиної точки відмови».

Недоліки: висока вартість, складність конфігурації та адміністрування.

6. Гібридна топологія. Поєднує кілька типів — наприклад, зірку з кільцем. Найпоширеніший варіант у сучасних мережах. Переваги: гнучкість і адаптивність до будь-яких умов, можливість локалізувати збої в окремих сегментах без впливу на всю мережу.

Таблиця 1.2 – Порівняльна характеристика топологій локальних мереж

Тип топології	Надійність	Масштабованість	Вартість	Коментар
Зірка	Висока	Середня	Середня	Найпопулярніша в офісах
Шина	Низька	Низька	Низька	Застаріла, майже не використовується
Кільце	Середня	Низька	Середня	Потребує точності в налаштуваннях
Дерево	Середня	Висока	Висока	Добре підходить до великих мереж
Повнов'язна	Дуже висока	Низька	Дуже висока	Лише в критичних системах
Гібридна	Висока	Висока	Змінна	Гнучкий підхід до мережевого проектування

#### 1.4 Вибір активного мережевого обладнання

Активне мережеве обладнання є серцевиною будь-якої локальної мережі, оскільки забезпечує маршрутизацію, комутацію, передачу та обробку даних. До активних компонентів відносять маршрутизатори (routers), комутатори (switches), точки доступу (access points), мережеві екрани (firewalls) та інше обладнання, яке потребує живлення та бере участь у перенаправленні трафіку.

При виборі активного обладнання важливо враховувати кілька ключових параметрів:

1. Продуктивність і пропускну здатність. Для офісних і навчальних мереж стандартом де-факто є Gigabit Ethernet (1 Гбіт/с). Для серверних кімнат або мереж із великим обсягом трафіку обирають 10 Гбіт/с або навіть 40–100 Гбіт/с

інтерфейси. Комутатори повинні підтримувати необхідну швидкість передачі без зниження продуктивності при повному навантаженні.

2. Кількість портів і тип інтерфейсів. Обирається залежно від кількості користувачів. Найчастіше використовуються 8-, 16-, 24- або 48-портові комутатори. Для зв'язку між сегментами застосовуються аплінки (uplink) з підтримкою SFP/SFP+ (оптоволокну).

3. Підтримка керованості (managed/unmanaged). Керовані комутатори (L2/L3 managed switch) дозволяють налаштовувати VLAN, QoS, протоколи STP, SNMP, IGMP, що важливо для великих мереж. Некеровані пристрої (unmanaged) — дешевші, але менш гнучкі й не підходять для корпоративних задач.

4. Рівень пристрою в моделі OSI.

- Комутатори рівня 2 (L2) — працюють із MAC-адресами.
- Комутатори рівня 3 (L3) — підтримують маршрутизацію між VLAN, що дозволяє гнучке розділення підмереж.
- Маршрутизатори — здійснюють IP-маршрутизацію, підключення до інтернету, реалізують політики NAT, DHCP, VPN.

5. Підтримка PoE (Power over Ethernet). Дозволяє жити IP-телефони, точки доступу, відеокамери через той самий Ethernet-кабель. Важливо враховувати потужність на порт (15,4 Вт — PoE, 30 Вт — PoE+, 60/90 Вт — PoE++).

6. Надійність і резервування. У професійних моделях передбачена підтримка резервного живлення (RPS), подвійних вентиляторів, гарячої заміни модулів. Протоколи STP/RSTP/MSTP забезпечують петльову стійкість.

7. Підтримка протоколів безпеки. Наявність ACL, 802.1X, DoS-захисту, фільтрації портів і захисту від DHCP-spoofing.

Таблиця 1.3 – Порівняння моделей активного обладнання для офісної LAN

Модель	Тип пристрою	Кількість портів	Швидкість	Керованість	PoE	Сфера використання
TP-Link TL-SG1016D	Комутатор	16	10/100/1000 Мбіт/с	Некерований	Ні	Бюджетні офіси, невеликі мережі
Cisco CBS250-24T-4	Керований комутатор	24+4 uplink SFP	Gigabit Ethernet	Керований (L2)	Ні	Малі та середні офіси, з підтримкою VLAN
MikroTik CRS328-24P-4S+RM	Керований комутатор	24 RJ45 + 4 SFP+	Gigabit + 10Gbps uplink	Керований (L3)	Так (PoE+)	Вимогливі офіси, середній бізнес, IP-телефонія
Ubiquiti UniFi USW-24-POE	Комутатор	24	Gigabit Ethernet	Керований	Так	Установи з Wi-Fi AP, IP-камерами, телефоном
Cisco ISR 4331	Маршрутизатор	2+ WAN, 3 LAN	До 1000 Мбіт/с	Керований	Ні	Центральний шлюз з розширеними функціями безпеки
MikroTik hEX S	Маршрутизатор	5	Gigabit + SFP	Керований	Ні	Малий офіс або філія

При виборі обладнання також доцільно враховувати бренд (Cisco, TP-Link, MikroTik, D-Link, Ubiquiti), підтримку гарантії, простоту налаштування, оновлення ПЗ та наявність локальної технічної підтримки.

Грамотний вибір активного мережевого обладнання — запорука стабільності, гнучкості та безпеки майбутньої локальної мережі.

## РОЗДІЛ 2 ОПТИМІЗАЦІЯ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

### 2.1 Методи підвищення продуктивності мережі

Продуктивність локальної обчислювальної мережі (ЛОМ) є одним із ключових критеріїв її ефективності. Під продуктивністю зазвичай розуміють сукупність таких параметрів, як пропускна здатність, час затримки, частота втрат пакетів, швидкість з'єднання та здатність витримувати навантаження. У процесі проектування та оптимізації ЛОМ необхідно враховувати технічні й логічні чинники, що впливають на швидкодію мережі, та застосовувати відповідні методи підвищення її продуктивності.

Основні напрями оптимізації

Підвищення продуктивності мережі може досягатися шляхом:

1. Оптимального вибору мережевого обладнання (комутатори, маршрутизатори, точки доступу) з урахуванням гігабітної та 10-гігабітної пропускної здатності;
2. Сегментування трафіку за допомогою VLAN, що дозволяє знизити рівень широкомовного трафіку (broadcast) та локалізувати навантаження;
3. Використання QoS (Quality of Service) для пріоритетної передачі критичних даних (VoIP, відео, бізнес-додатки);
4. Актуалізації кабельної інфраструктури – застосування кабелів категорії Cat5e/Cat6 або оптоволокна для магістральних ліній;
5. Побудови ієрархічної архітектури мережі з виділенням рівнів доступу, дистрибуції та ядра (Core – Distribution – Access);
6. Зменшення затримок через розміщення серверів ближче до користувачів (Edge computing);
7. Впровадження мережевих протоколів керування трафіком – наприклад, LACP (Link Aggregation) або протоколів маршрутизації;
8. Постійного моніторингу продуктивності за допомогою SNMP, NetFlow, Zabbix, PRTG тощо.

Приклади технічних рішень:

- Вибір обладнання з великим буфером та швидкими ASIC

У комутаторах рівня доступу варто використовувати пристрої з великим обсягом оперативної пам'яті та високопродуктивними процесорами. Наприклад, моделі Cisco Catalyst, MikroTik CRS або Ubiquiti EdgeSwitch мають можливість обробляти великий трафік без втрат.

- Реалізація VLAN

Розділення трафіку на логічні мережі дозволяє мінімізувати навантаження на кожен сегмент. Наприклад, створення окремих VLAN для: адміністративного персоналу, бухгалтерії, гостьової мережі, камер відеоспостереження.

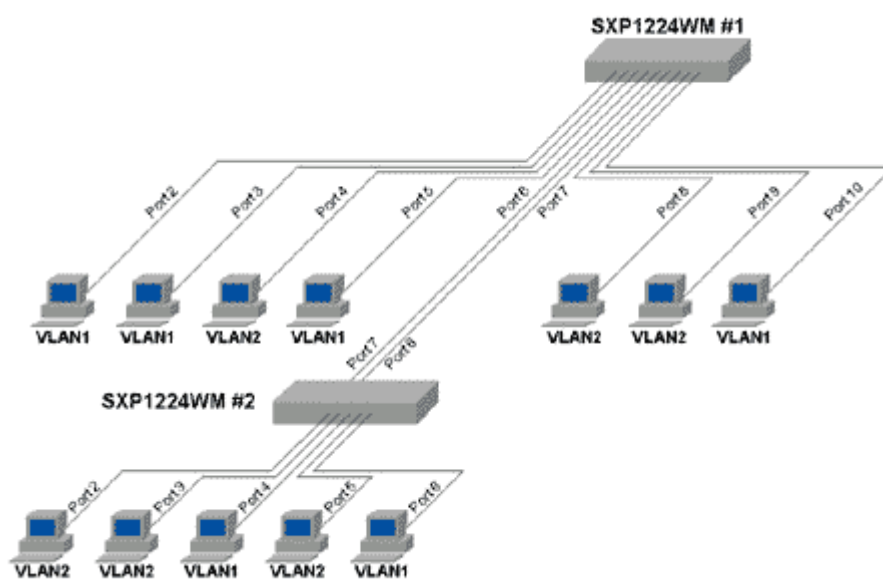


Рисунок 2.1 – Схема VLAN

- QoS та пріоритет трафіку

Quality of Service дозволяє виділити пріоритети: клас “voice” – найвищий пріоритет для VoIP, клас “video” – для відеоконференцій, клас “best effort” – для загального трафіку, клас “bulk” – для некритичних завантажень (наприклад, оновлень системи).

Налаштування QoS можливе як на комутаторах L3, так і на маршрутизаторах з CLI/GUI-інтерфейсом.

- Впровадження агрегованих лінків (Link Aggregation)

Ця технологія дозволяє об'єднати кілька фізичних ліній зв'язку між комутаторами в єдину логічну, що підвищує сумарну пропускну здатність і відмовостійкість.

Вплив на практичну реалізацію

Застосування перелічених методів дозволяє:

- зменшити кількість вузьких місць у мережі;
- уникати перевантаження в години пік;
- підвищити якість обслуговування критично важливих сервісів;
- забезпечити плавну роботу при масштабуванні;
- мінімізувати втрати пакетів та покращити користувацький досвід.

Таблиця 2.1 – Порівняння ефективності методів підвищення продуктивності

Метод	Вплив на пропускну здатність	Складність впровадження	Додаткові витрати
Використання VLAN	Високий	Середня	Мінімальні
QoS	Середній	Висока	Мінімальні
Агрегація каналів (LACP)	Високий	Висока	Середні
Оптоволокно в магістралях	Дуже високий	Середня	Високі
Обладнання з великим буфером	Середній	Низька	Середні

Таким чином, підвищення продуктивності ЛОМ є результатом комплексного підходу — поєднання правильного вибору обладнання, логічного проектування, інтелектуального керування трафіком і використання сучасних протоколів оптимізації. Реалізація цих методів забезпечує ефективну, стабільну та масштабовану роботу корпоративної мережі.

## 2.2. Підвищення надійності та стійкості

Надійність та відмовостійкість локальної обчислювальної мережі (ЛОМ) є критично важливими параметрами для забезпечення безперервності бізнес-процесів. У сучасних умовах мережа повинна залишатися працездатною навіть у разі відмови окремих елементів або підвищеного навантаження. Порушення доступу до даних, збій у маршрутизації або втрата зв'язку можуть призвести до значних фінансових і часових втрат.

Основні фактори, що впливають на надійність ЛОМ:

1. Наявність єдиної точки відмови (Single Point of Failure) – наприклад, один комутатор, через який проходить увесь трафік.
2. Фізичне зношення обладнання – вихід з ладу портів, блоків живлення, мережевих карт.
3. Недостатня резервованість – відсутність запасних маршрутів або дублюючих каналів.
4. Програмні збої або помилки конфігурації – що можуть призвести до зависання обладнання або відмови сервісів.
5. Людський фактор – помилки при налаштуванні, оновленні або обслуговуванні.

Основні методи підвищення надійності:

#### 1. Впровадження резервування

- Резервні канали зв'язку (Redundant Links) – створення додаткових фізичних з'єднань між критичними вузлами.
- Резервування маршрутизаторів / комутаторів – наприклад, за допомогою VRRP (Virtual Router Redundancy Protocol), HSRP або STP/RSTP.
- Дублювання джерел живлення – використання комутаторів з подвійним живленням (dual power supply).
- Встановлення ІБЖ (UPS) – для запобігання відключенням при перебоях в електроживленні.

#### 2. Протоколи відмовостійкості

- STP (Spanning Tree Protocol) – дозволяє уникнути петель у мережі, але автоматично активує резервні шляхи при відмові основного.
- LACP (Link Aggregation Control Protocol) – поєднує кілька фізичних каналів у логічний, забезпечуючи більшу пропускну здатність і резервування.
- VRRP/HSRP – автоматичне перемикання шлюзу у випадку виходу з ладу основного маршрутизатора.

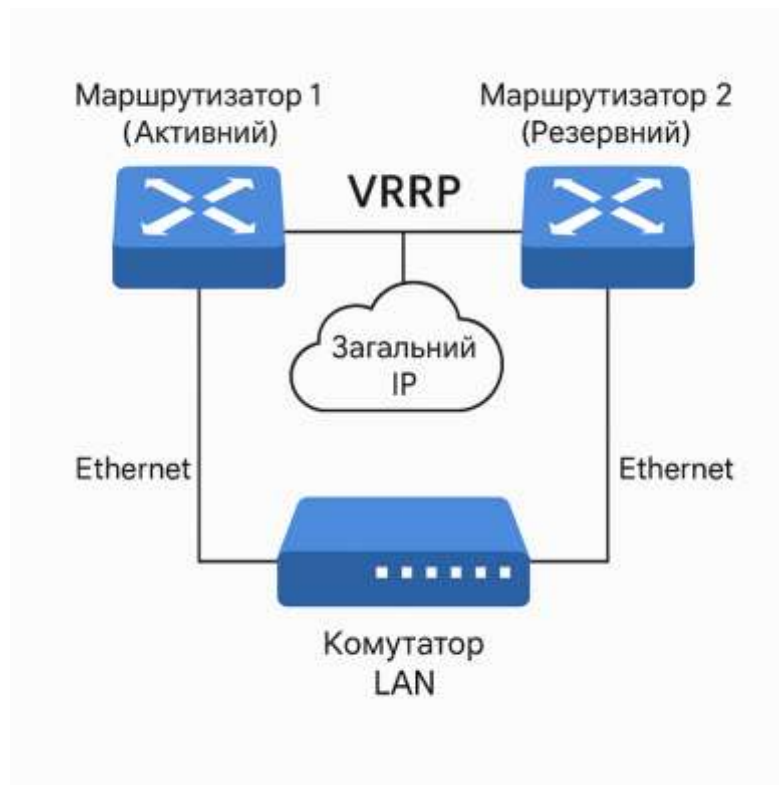


Рисунок 2.2 – Схема резервування шлюзу з використанням VRRP

#### Стратегія резервного копіювання

- Резервне копіювання конфігурацій обладнання – збереження поточних налаштувань комутаторів і маршрутизаторів.
- Автоматичне резервування даних серверів – у хмару або на окремий локальний NAS.
- Тестування відновлення після аварії (Disaster Recovery) – регулярні перевірки працездатності резервної інфраструктури.

#### Архітектурні підходи

- Ієрархічна структура мережі (3-tier design) – з поділом на рівень доступу (Access), дистрибуції (Distribution) і ядра (Core). Це дозволяє локалізувати збої й обмежити їх вплив.
- Використання L3-комутаторів на рівні Distribution — для зниження навантаження на маршрутизатори та скорочення часу маршрутизації.
- Гео-резервування — для великих компаній: резервний офіс або дата-центр у географічно іншому регіоні.

Приклад практичної реалізації:

- резервний uplink з комутатора ядра до маршрутизатора;
- реалізація STP для уникнення петель;
- UPS для ключових вузлів (сервер, маршрутизатор, комутатор);
- подвійне збереження файлів (на сервері та у хмарі);
- використання VLAN для ізоляції критичних систем.

Таблиця 2.2 – Порівняння методів підвищення надійності

Метод	Вартість впровадження	Вплив на надійність	Складність реалізації
Резервні канали	Середня	Високий	Середня
STP / RSTP	Мінімальна	Високий	Низька
VRRP / HSRP	Середня	Високий	Середня
UPS + Dual PSU	Висока	Високий	Середня
Geo-резервування	Дуже висока	Дуже Високий	Висока

Забезпечення високої надійності та відмовостійкості є основою для безперервної роботи мережі. Правильне впровадження резервування, використання протоколів захисту та постійне тестування здатності до відновлення є запорукою стійкості інформаційної інфраструктури до збоїв та аварій.

### 2.3. Безпека LAN

Захист даних у локальній обчислювальній мережі (LAN) є критично важливим компонентом інформаційної безпеки організації. Порушення конфіденційності, цілісності або доступності інформації може призвести до витоку комерційної та особистої інформації, порушення законодавства та фінансових збитків. У зв'язку з цим проектування ЛОМ повинно супроводжуватися впровадженням заходів безпеки на різних рівнях – від фізичного до прикладного.

Основні загрози локальним мережам: несанкціонований доступ до внутрішніх ресурсів, вірусні атаки та шкідливе ПЗ, перехоплення або підміна трафіку, DDoS-атаки, соціальна інженерія, вразливості у пристроях та ОС.

Методи захисту на різних рівнях:

#### 1. Фізичний рівень

- Розміщення критичного обладнання (серверів, маршрутизаторів) у закритих серверних приміщеннях;
- Захист кабельних трас від механічних пошкоджень;
- Обмеження доступу до комутаційних шаф.

#### 2. Мережевий рівень

- Контроль доступу за MAC-адресами – фільтрація дозволених пристроїв на комутаторах;
- Ізоляція трафіку через VLAN – розділення мережі на сегменти з різними рівнями довіри;
- ACL (Access Control Lists) – на маршрутизаторах для обмеження доступу між VLAN;
- Брандмауери (Firewall) – апаратні або програмні шлюзи для контролю вхідного та вихідного трафіку;
- VPN (Virtual Private Network) – захищене підключення зовнішніх користувачів до внутрішньої мережі.

#### 3. Прикладний рівень

- Аутентифікація користувачів (Active Directory, RADIUS, 802.1X);
- Шифрування трафіку (HTTPS, TLS, IPsec);
- Антивірусне ПЗ і антишпигунські системи;
- Моніторинг подій і логування – з використанням систем SIEM (Security Information and Event Management).

#### 4. Безпека бездротової мережі (Wi-Fi)

- Шифрування трафіку за допомогою WPA2/WPA3;
- Використання гостьової мережі для сторонніх користувачів;
- Приховування SSID або застосування MAC-фільтрації;
- Відключення WPS (через його вразливості).

Приклад практичної реалізації в рамках дипломного проєкту

У проєктованій ЛОМ буде реалізовано:

- VLAN для відокремлення мережі бухгалтерії, адміністрації, Wi-Fi, камер;
- контролю доступу до внутрішніх ресурсів через ACL;
- брандмауер на маршрутизаторі з підтримкою Stateful Inspection;
- VPN-сервер для захищеного доступу працівників ззовні;
- WPA3-захист точок доступу з гостьовим сегментом;
- SNMP-моніторинг усіх комутаторів;
- автоматичне оновлення прошивок та антивірусне ПЗ на робочих станціях.

Таблиця 2.3 – Узагальнення методів захисту в LAN

Рівень захисту	Метод/технологія	Призначення
Фізичний	Замикання серверної, шаф	Унеможливлення фізичного доступу
Канальний	MAC-фільтрація	Обмеження за адресою пристрою
Мережевий	VLAN, ACL, FIREWALL	Ізоляція та фільтрація трафіку
Транспортний	IPsec, TLS	Шифрування трафіку
Прикладний	AD, RADIUS, логування	Ідентифікація та контроль доступу
Бездротовий	WPA3, гостьовий доступ	Захист Wi-Fi від вторгнень



Рисунок 2.3 – Схема безпечної сегментованої LAN з VLAN, ACL і VPN

Таким чином, безпечна локальна мережа – це не лише наявність антивірусу чи пароля. Це комплекс заходів, що охоплюють весь шлях трафіку

— від фізичного з'єднання до прикладного рівня. Ефективна реалізація мережевої безпеки потребує планування, регулярного моніторингу, аналізу логів і адаптації до сучасних загроз.

## 2.4 Розробка логічної схеми локальної мережі

Розробка логічної схеми локальної обчислювальної мережі (ЛОМ) є критичним етапом проектування, оскільки вона визначає, як саме взаємодіють мережеві компоненти між собою на рівні протоколів, адресації та функціонального розподілу. Логічна структура не обов'язково відповідає фізичному розташуванню пристроїв, але є основою для налаштування IP-адрес, VLAN, доступу до ресурсів та безпеки.

### Основні компоненти логічної схеми

У межах розроблюваної мережі передбачаються наступні логічні елементи:

- Комутатори доступу (Access switches) — обслуговують кінцеві пристрої користувачів;
- Комутатори рівня дистрибуції (Distribution switches) — об'єднують сегменти мережі та реалізують маршрутизацію між VLAN;
- Маршрутизатор з VPN — забезпечує вихід в Інтернет і захищений віддалений доступ;
- Сервери — розташовані в окремому VLAN, ізольовані від користувацького трафіку;
- Wi-Fi точки доступу — підключені до VLAN гостьового трафіку;
- IP-камери — в окремому VLAN, доступ до яких дозволений лише адміністраторам.

### Логічна структура VLAN

Розділення мережі на VLAN дозволяє:

- ізолювати різні підрозділи;
- зменшити широкомовний трафік (broadcast domain);
- підвищити безпеку і керованість.

Таблиця 2.4 – Запропонована структура VLAN

VLAN ID	Назва сегменту	Призначення
VLAN 10	Адміністрація	Робочі станції керівників і бухгалтерії
VLAN 20	Співробітники	Загальні робочі місця
VLAN 30	Гостьовий Wi-Fi	Відокремлений доступ до Інтернету
VLAN 40	Сервери	Локальні файлові/базові сервери
VLAN 50	Камери відеоспостереження	Доступ лише для адміністраторів

Для спрощення адміністрування обрана статична схема підмереж за VLAN.

Наприклад:

- VLAN 10: 192.168.10.0/24
- VLAN 20: 192.168.20.0/24
- VLAN 30: 192.168.30.0/24
- VLAN 40: 192.168.40.0/24
- VLAN 50: 192.168.50.0/24

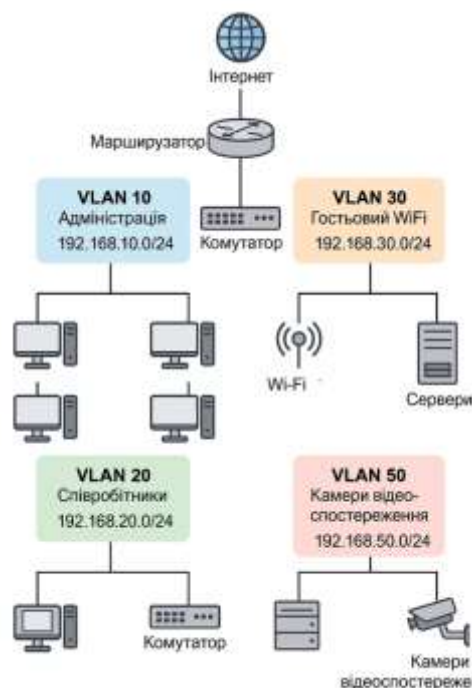


Рисунок 2.4 – Логічна схема мережі з VLAN, маршрутизатором і комутаторами DHCP та DNS

Для VLAN 20 та 30 буде реалізовано автоматичну роздачу IP-адрес через DHCP. DNS-сервери – зовнішні (Google DNS: 8.8.8.8, 8.8.4.4), дублюються в

маршрутизаторі. Сервер у VLAN 40 також може бути резервним DNS у внутрішній мережі.

ACL і правила доступу У маршрутизаторі будуть налаштовані ACL (Access Control Lists): VLAN 30 (гості) не мають доступу до VLAN 10, 20, 40, VLAN 50 доступний лише з VLAN 10 (адміністрація), доступ між VLAN 10 ↔ VLAN 40 дозволений (керівництво ↔ сервери).

Таблиця 2.5 – Правила доступу між VLAN

Джерело	Призначення	Доступ
VLAN 10	VLAN 40	Дозволено
VLAN 20	VLAN 40	Заборонено
VLAN 30	VLAN 10, 20, 40	Заборонено
VLAN 10	VLAN 50	Дозволено
VLAN 20	VLAN 50	Заборонено

Розроблена логічна схема забезпечує:

- поділ мережі за функціональними ознаками;
- ізоляцію критичних сегментів;
- можливість масштабування;
- централізоване управління IP-адресами та доступом;
- високий рівень безпеки завдяки VLAN та ACL.

Це є передумовою для побудови ефективної, надійної та безпечної корпоративної мережі.

## **РОЗДІЛ 3**

### **МОДЕЛЮВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ**

#### **3.1 Вибір мережевого обладнання відповідно до проєкту**

## ВИСНОВКИ

У результаті виконання дипломного проєкту було здійснено повний цикл проєктування, оптимізації та моделювання локальної обчислювальної мережі для умовного офісного середовища. Метою роботи було створення ефективної, безпечної, масштабованої та економічно обґрунтованої мережевої інфраструктури з урахуванням сучасних вимог до функціональності та надійності.

У першому розділі було проведено теоретичний аналіз принципів побудови локальних мереж, описано ключові характеристики технологій Ethernet, IP-адресації, топологій (зіркова, кільцева, гібридна тощо) та методів забезпечення масштабованості й безпеки. Також були розглянуті типи активного мережевого обладнання (комутатори, маршрутизатори, точки доступу), їх призначення та особливості вибору. Порівняльна таблиця дозволила зробити обґрунтований вибір пристроїв, найбільш придатних для реалізації в запропонованих умовах.

У другому розділі розглянуто методи оптимізації локальних мереж. Зокрема, описано технології підвищення пропускної здатності, управління трафіком, резервування (VRRP), розмежування трафіку за допомогою VLAN, впровадження списків контролю доступу (ACL) та захищених тунелів (VPN). Окрему увагу було приділено практичному проєктуванню сегментованої мережі з урахуванням безпекових вимог.

У третьому розділі було реалізовано проєкт фізичної та логічної побудови мережі у середовищі Cisco Packet Tracer. Здійснено налаштування VLAN на комутаторах, маршрутизатора з сабінтерфейсами для маршрутизації між VLAN (Router-on-a-Stick), налаштовано бездротову точку доступу, сервер і клієнтські станції. Також було перевірено зв'язність усіх сегментів мережі, проаналізовано таблиці маршрутизації, реалізовано елементи безпеки (ACL, VPN) і змодельовано типові сценарії несправностей з подальшим усуненням. Налаштування підтверджені командними виводами CLI (show vlan, show ip

interface brief, ping, тощо).

Окремий акцент було зроблено на моніторинг і діагностику, що дозволяє ефективно підтримувати працездатність мережі після впровадження. Запропоновано набір базових рекомендацій щодо резервування, безпеки, оновлення прошивок та управління трафіком.

У підсумку, виконана робота доводить доцільність застосування комбінації технологій VLAN, ACL, VPN і резервування шлюзів у локальних офісних мережах малого та середнього масштабу. Розроблена мережа має чітку структуру, гнучко масштабується, забезпечує сегментовану архітектуру з чітким поділом доступу, високою надійністю та резервуванням критичних вузлів.

Згідно з економічним аналізом, реалізація даного проєкту є доцільною та може бути втілена у реальному середовищі без надмірних витрат. Впровадження такої мережі дозволить значно покращити якість обміну даними, підвищити безпеку та забезпечити безперебійну роботу офісної IT-інфраструктури.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міхальова Н. В. Хмарні технології в інформатизації освіти: теорія і практика : монографія / Н. В. Міхальова. – Київ : Педагогічна думка, 2013. – 276 с.
2. Mell P., Grance T. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. – Gaithersburg : NIST, 2011. – 7 p. – (NIST Special Publication 800-145). URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (дата звернення: 24.04.2025).
3. Рибак О. В. Хмарні обчислення як інноваційна технологія інформатизації / О. В. Рибак // Інформаційні технології в освіті. – 2016. – № 26. – С. 137–147.
4. Трачук С. М. Основи хмарних обчислень: навч. посіб. / С. М. Трачук. – Київ : Кондор, 2020. – 196 с.
5. Кравченко І. В. Хмарні технології: моделі, переваги та ризики / І. В. Кравченко // Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – 2018. – № 31 (1319). – С. 45–52.
6. Жукова Н. О. Хмарні технології: безпека, законодавчі аспекти, нормативи / Н. О. Жукова // Інформаційне суспільство. – 2020. – № 4. – С. 12–18.
7. Amazon Web Services. AWS Well-Architected Framework. – Amazon, 2022. URL: <https://docs.aws.amazon.com/wellarchitected/latest/framework/> (дата звернення: 24.04.2025).
8. ISO/IEC 27017:2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. – Geneva : International Organization for Standardization, 2015.
9. Шарапов Д. С., Кондратюк Л. В. Cisco Packet Tracer як інструмент для моделювання хмарних мереж / Д. С. Шарапов, Л. В. Кондратюк // Системи обробки інформації. – 2021. – № 3 (165). – С. 134–139.

10. Kavis M. J. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) / Michael J. Kavis. – Indianapolis : Wiley, 2014. – 225 p.
11. Байдус О. І. Інфраструктура як сервіс: основи IaaS / О. І. Байдус // Електроніка та інформаційні технології. – 2019. – № 2. – С. 33–39.
12. Серeda П. І. Технології побудови гібридних хмарних мереж / П. І. Серeda // Збірник наукових праць Харківського університету Повітряних Сил. – 2020. – № 3 (65). – С. 86–92.
13. Cisco Systems. SD-WAN White Paper. – Cisco, 2023. URL: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-740111.html> (дата звернення: 24.04.2025).
14. Ткаченко А. В. Fog та Edge Computing: сучасні тренди у хмарних обчисленнях / А. В. Ткаченко // Наукові вісті НТУУ «КПІ». – 2021. – № 5. – С. 29–34.
15. Gartner. Magic Quadrant Cloud Infrastructure and Platform Services. – Gartner, 2023. URL: <https://www.gartner.com/en/documents/4001743> (дата звернення: 24.04.2025).