ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти магістр

на тему: «**Методологія оптимізації корпоративних комп'ютерних мереж**»

Виконав: здобувач вищої освіти
за освітньою програмою
Інформаційні управляючі системи та технології
спеціальності 126 Інформаційні системи та технології
ступеня вищої освіти магістр
групи 126ІСТ_мд_2023
Филь Владислав Вадимович
Керівник: Калініченко Антоніна Володимирівна
Рецензент: Ковальчук Станіслав Богданович

Полтава – 2024 року

ВСТУП

Актуальність теми. З розвитком інформаційних технологій корпоративні комп'ютерні мережі стали невід'ємною частиною функціонування будь-якого сучасного підприємства. Вони забезпечують комунікацію, обмін даними та спільну роботу співробітників, інтеграцію з іншими системами і бізнес-процесами, що робить їх ключовим інструментом для забезпечення ефективності роботи організації. Проте, зростання обсягів даних, збільшення вимог до безпеки та масштабованості ставлять нові виклики перед мережевою інфраструктурою, що потребує постійного вдосконалення і оптимізації. Таким чином, питання оптимізації корпоративних мереж є вкрай важливим для підвищення продуктивності і конкурентоспроможності сучасних підприємств.

Сучасний бізнес стає все більш залежним від інформаційних технологій, що забезпечують швидкий доступ до даних і безперебійну комунікацію. Корпоративні мережі, які об'єднують офіси, філії та зовнішні партнери, дозволяють підприємствам бути більш гнучкими і продуктивними. Впровадження нових бізнес-моделей, таких як хмарні сервіси, вимагає від мереж забезпечення високої пропускної здатності, надійності та безпеки. У зв'язку із зростанням обсягів даних, які передаються через корпоративні мережі, і постійним підвищенням рівня кіберзагроз, зростає необхідність в оптимізації мережевої інфраструктури для забезпечення її надійної та безперебійної роботи.

Оптимізація корпоративних мереж дозволяє значно покращити продуктивність підприємства, зменшивши затримки у передачі даних, збільшивши пропускну здатність мережі та покращивши загальну ефективність використання ресурсів. Правильне управління мережевим трафіком дозволяє швидше обробляти критичні дані, що сприяє прискоренню бізнес-процесів. Крім того, оптимізовані мережі знижують витрати на підтримку інфраструктури, зменшують ризики простоїв і втрат даних. В результаті, підприємства отримують можливість більш оперативно реагувати на потреби ринку, що підвищує їх конкурентоспроможність.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконана у відповідності до науково-дослідної ініціативної теми «Організаційно-методологічні аспекти впровадження інформаційно-комунікаційних систем і технологій в управлінні діяльністю сучасних організацій та підприємств за умов переходу до цифрової економіки» ДРН 0123U105060.

Метою роботи є визначення ефективних підходів до оптимізації корпоративних комп'ютерних мереж для забезпечення їх кращої продуктивності, надійності та загальної ефективності.

Завдання роботи:

1. Розглянути основні підходи до оптимізації комп'ютерних мереж;

2. Проаналізувати сучасні технології для покращення ефективності комп'ютерних мереж;

3. Розробити практичні рекомендації щодо оптимізації комп'ютерних мережі.

Об'єкт дослідження: корпоративні комп'ютерні мережі.

Предмет дослідження: методи та технології оптимізації комп'ютерних мереж.

Методи дослідження: аналіз інформаційних джерел, емпіричне дослідження комп'ютерних мереж, моделювання мережевих процесів.

Інформаційна база дослідження: науково-технічна література, наукові статті та публікації з питань мережевої інфраструктури, доступні в наукових базах даних Google Scholar, IEEE Xplore, SpringerLink, ScienceDirect, Scopus, ResearchGate; вітчизняні та зарубіжні стандарти мережевих технологій та оптимізації; офіційна документація та ресурси з мережевих протоколів та технологій Cisco, Juniper Networks, VMware; аналітичні матеріали, блоги та статті провідних експертів у галузі корпоративних мереж та оптимізації мережевої інфраструктури.

Елементи наукової новизни: полягають у розробці підходу до оптимізації корпоративних комп'ютерних мереж шляхом впровадження SDN-контролерів для динамічного управління трафіком, QoS для пріоритизації критичного трафіку та

віртуалізації функцій (NFV) для підвищення відмовостійкості мережі. Запропоновано алгоритм програмного рішення, що поєднує ці технології для централізованого моніторингу та управління мережею.

Практична значущість: полягає у можливості застосування розроблених методів для оптимізації мережевих процесів у великих корпоративних мережах. Впровадження запропонованих рішень дозволяє суттєво підвищити продуктивність мережі, знизити затримки та мінімізувати втрати пакетів, що підтверджено експериментальним тестуванням.

Апробація результатів дослідження. За результатами дослідження опубліковано тези доповідей: «Методи аналізу трафіку в корпоративних комп'ютерних мережах», Матер. наук.-практ. конф. за підсумками проходження виробничої практики здобувачів вищої освіти ступеня вищої освіти «Магістр» освітньо-професійної програми «Інформаційні управляючі системи та технології» спеціальності 126 Інформаційні системи та технології, кафедра інформаційних систем та технологій Полтавського державного аграрного університету, 16 жовтня 2024 року. Вип. Х. Полтава: ПДАУ, 2024; «Методи покращення пропускної здатності корпоративних комп'ютерних мереж», Матер. XXI щорічного міждисциплінарного семінару «Студентські роботи за науковою тематикою кафедри інформаційних систем та технологій ННІ ЕУП та ІТ ПДАУ», 20 листопада 2024 року, м. Полтава;

Структура та обсяг кваліфікаційної роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Основний текст роботи викладений на 75 сторінках, містить 29 рисунків і 37 таблиць. Список використаних джерел налічує 50 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ОПТИМІЗАЦІЇ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Структура та класифікація корпоративних комп'ютерних мереж

Корпоративна комп'ютерна мережа (ККМ) – це сукупність комп'ютерів, серверів та інших пристроїв, об'єднаних для обміну інформацією та забезпечення взаємодії між користувачами всередині організації. ККМ можуть мати різні масштаби та архітектуру, залежно від потреб підприємства.

ККМ розрізняють за кількома ознаками, зокрема [1]:

- за географічною ознакою – LAN, MAN, WAN;
- за типом передачі даних – дротові, бездротові, змішані мережі;
- за рівнем захисту – публічні, приватні, гібридні мережі.

У таблиці 1.1 подане описання основних типів ККМ за географічною ознакою.

Таблиця 1.1 – Класифікація ККМ за географічною ознакою

Тип мережі	Опис	Застосування
LAN	Локальна мережа, обмежена однією будівлею або приміщенням. Об'єднує комп'ютери та інші пристрої на невеликій відстані.	Офіси, невеликі компанії.
MAN	Міська мережа, яка охоплює більші території, ніж LAN, але менші, ніж WAN. Використовується для об'єднання декількох LAN в одному місті або регіоні.	Університетські містечка, великі міські організації.
WAN	Глобальна мережа, що об'єднує кілька LAN через великі географічні відстані. Використовує інтернет або приватні канали зв'язку.	Міжнародні корпорації, філії в різних країнах.

До основних компонентів ККМ належать сервери, комутатори (Switches), маршрутизатори (Routers), брандмауери (Firewalls), точки доступу (Access Points), кабельна інфраструктура, контролери SDN, балансувальники навантаження (Load Balancers).

Вказані компоненти корпоративної мережі мають різні функції та характеристики, які взаємодіють для забезпечення стабільної роботи мережі [2]. Описання основних компонентів ККМ представлене у таблиці 1.2.

Таблиця 1.2 – Основні компоненти ККМ

Компонент	Опис
Сервери	Центральні комп'ютери, що надають ресурси і послуги (файлові, поштові, вебсервери) для інших учасників мережі.
Мережеві кабелі	Використовуються для фізичного з'єднання пристроїв у дротових мережах (Ethernet, оптичні кабелі).
Комутатори (Switches)	Забезпечують з'єднання пристроїв всередині мережі на рівні передачі даних (рівень 2 OSI).
Маршрутизатори (Routers)	З'єднують локальні мережі (LAN) з глобальними мережами (WAN) та визначають маршрути передачі даних.
Брандмауери (Firewalls)	Захищають мережу від несанкціонованого доступу, фільтруючи вхідний і вихідний трафік.
Точки доступу (Access Points)	Забезпечують бездротовий доступ до мережі для пристроїв (Wi-Fi).
Програмне забезпечення управління	Відповідає за моніторинг, конфігурацію та управління всіма компонентами мережі.

Сервери є центральними компонентами мережі, який забезпечує доступ до мережевих ресурсів, обчислювальну потужність та управління даними. Кабельна інфраструктура – це фізичне середовище для передачі даних, яке може включати мідні або оптоволоконні кабелі.

Комутатори – це пристрої, що з'єднують сегменти мережі, забезпечують передачу даних між ними та сегментацію трафіку. Маршрутизатори забезпечують зв'язок між різними мережами, управління маршрутизацією трафіку.

Брандмауери – це пристрої або програми для захисту мережі від несанкціонованого доступу та кібератак. Точки доступу (Access Points) – пристрої для забезпечення бездротового зв'язку в локальних мережах (WLAN).

Контролери SDN – програмні системи для централізованого управління мережею через програмно-визначену архітектуру. Балансувальники навантаження – пристрої або програмні рішення, які рівномірно розподіляють трафік між серверами. У таблиці 1.3 узагальнено основні параметри, що допомагають у виборі обладнання для модернізації та оптимізації мережі.

Таблиця 1.3 – Характеристики основних компонентів ККМ

Компонент	Основна функція	Характерні параметри
Сервери	Зберігання та обробка даних, управління ресурсами	Потужність процесора, обсяг оперативної пам'яті, RAID для збереження даних
Комутатори (Switches)	З'єднання сегментів мережі, передача даних	Кількість портів, швидкість передачі (1 Gbps, 10 Gbps), VLAN підтримка
Маршрутизатори (Routers)	Маршрутизація трафіку між мережами	Продуктивність (кількість пакетів/сек), підтримка протоколів (BGP, OSPF)
Брандмауери (Firewalls)	Захист від несанкціонованого доступу	Продуктивність (Gbps), підтримка політик безпеки, DPI (глибокий аналіз пакетів)
Точки доступу (Access Points)	Забезпечення бездротового зв'язку (Wi-Fi)	Стандарти Wi-Fi (802.11ac, 802.11ax), діапазон частот (2,4/5 ГГц)
Кабельна інфраструктура	Фізичне середовище передачі даних	Тип кабелю (Cat5e, Cat6, оптоволокно), пропускна здатність
Контролери SDN	Централізоване управління мережею	Продуктивність обробки даних, підтримка протоколу OpenFlow
Балансувальники навантаження (Load Balancers)	Розподіл трафіку між серверами	Максимальна пропускна здатність, підтримка L4/L7 балансування

Рисунок 1.1 ілюструє взаємодію компонентів корпоративної мережі та їх роль у забезпеченні зв'язку між пристроями.

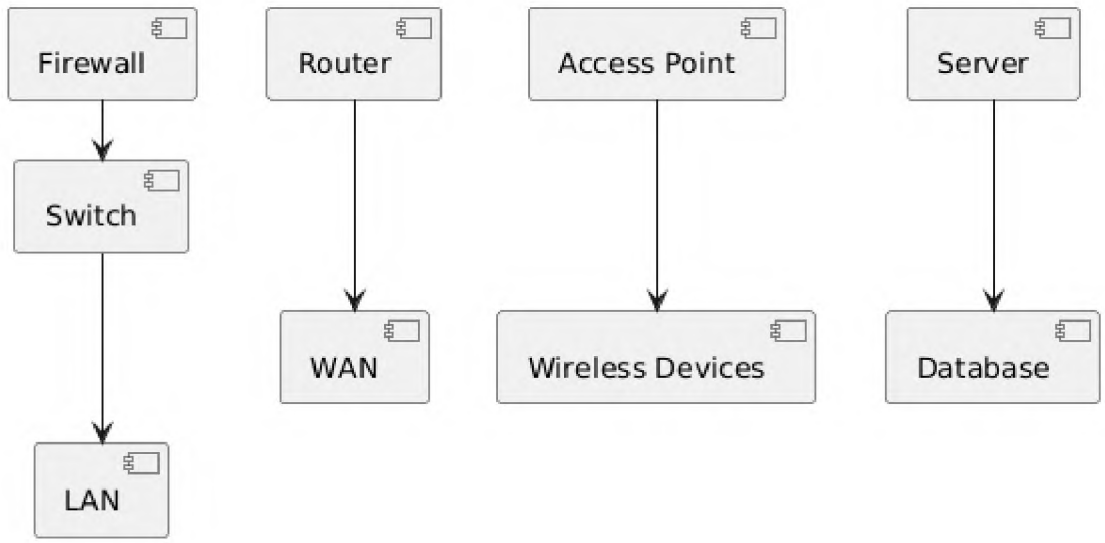

Рисунок 1.1 – Діаграма функціональної взаємодії основних компонентів ККМ

Будова і функціонування ККМ визначається їх архітектурою. До основних типів архітектури ККМ належать [3]:

- клієнт-серверна архітектура (Client-Server Architecture, CSA);
- однорангова архітектура (Peer-to-Peer Architecture, P2P);
- хмарна архітектура (Cloud Architecture, CA);
- програмно-визначена архітектура (Software Defined Network, SDN);
- мережа з віртуалізацією функцій (Network Function Virtualization, NFV).

Клієнт-серверна архітектура передбачає наявність центральних серверів, які надають послуги та ресурси клієнтським комп'ютерам. Сервери відповідають за обробку запитів і управління даними, а клієнти – за взаємодію з користувачами та відправлення запитів до серверів. Основною характеристикою такої архітектури є централізоване управління, що дозволяє легше забезпечити безпеку та контроль доступу. Цей тип архітектури найкраще підходить для великих організацій із складною мережевою інфраструктурою. В одноранговій мережі всі комп'ютери рівноправні, і кожен з них може бути як клієнтом, так і сервером (рисунок 1.2).

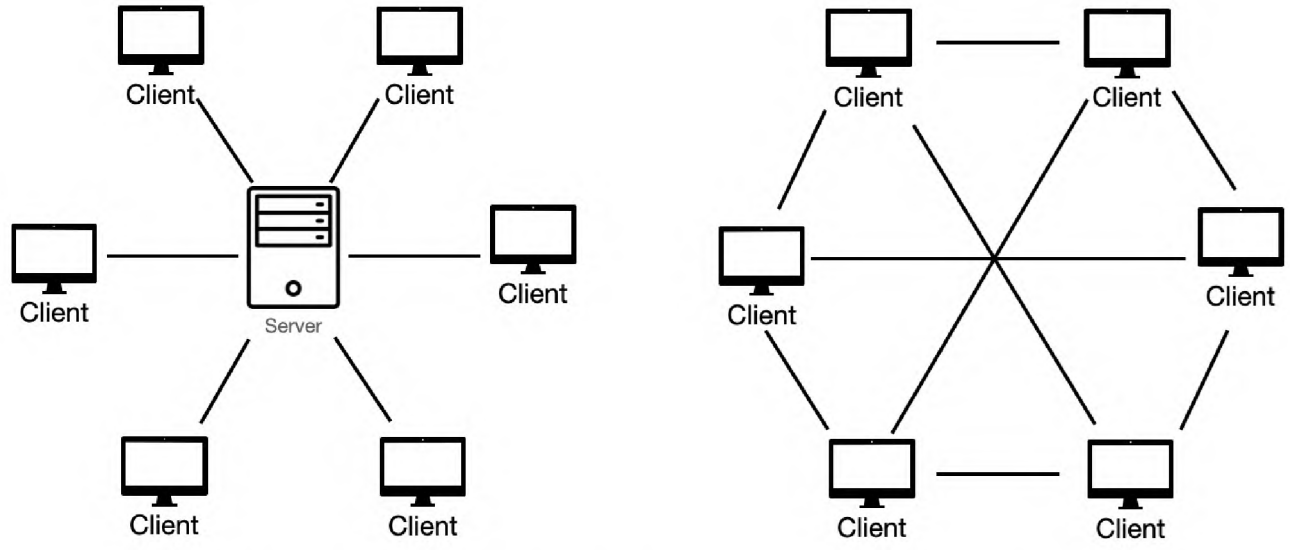

Рисунок 1.2 – Кліент-серверна та однорангова архітектура ККМ [4]

Користувачі однорангової комп'ютерної мережі можуть безпосередньо обмінюватися даними між собою без центрального сервера. Для такої архітектури характерні децентралізована структура, простота налаштування. Однак така

мережа менш надійна і важча в управлінні без централізованого контролю. Одноранговa архітектура підходить для невеликих мереж або для обмеженого використання у корпоративних середовищах.

Хмарна архітектура заснована на використанні хмарних сервісів, де більшість обчислювальних ресурсів і зберігання даних знаходяться у хмарі. Користувачі хмарної мережі отримують доступ до її ресурсів через інтернет. Характерними властивостями хмарної архітектури є висока масштабованість мережі, значна економія витрат на апаратне забезпечення та обслуговування, критична залежність від інтернет-з'єднання. Хмарна архітектура комп'ютерної мережі підходить для організацій, які потребують гнучкості та мають розподілену структуру (рисунок 1.3).

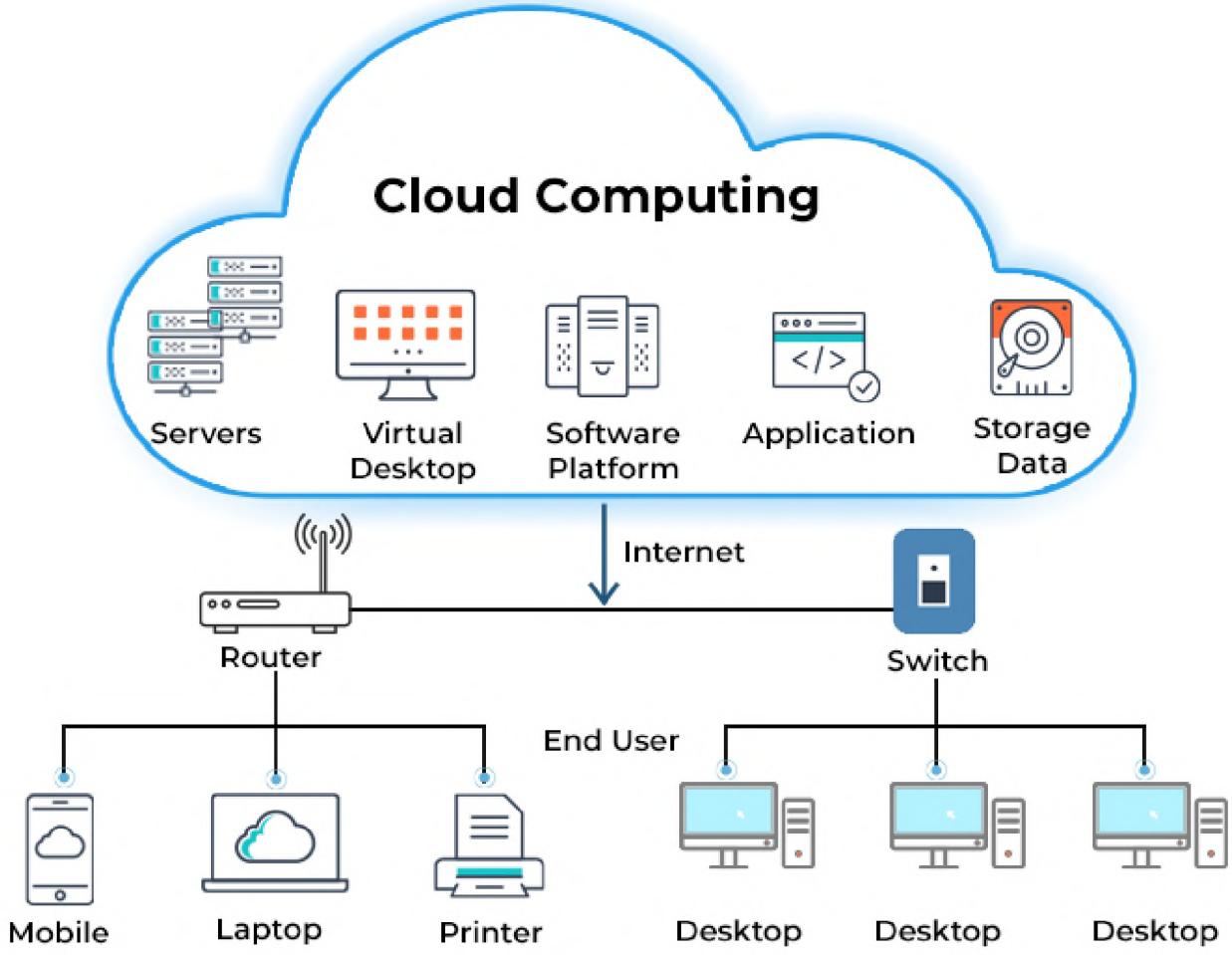

Рисунок 1.3 – Хмарна архітектура мережі [5]

Мережа з програмно-визначеною архітектурою (SDN) – це відносно новий підхід, при якому управління мережею здійснюється централізовано за допомогою програмного забезпечення. Програмне забезпечення SDN відділяє управління від апаратного забезпечення, що дозволяє гнучко налаштовувати мережеву інфраструктуру (рисунок 1.4). Головними характеристиками SDN є висока гнучкість та автоматизація, централізоване управління через програмне забезпечення, швидке реагування на зміни в мережевому трафіку. SDN найкраще підходить для великих підприємств і хмарних середовищ [6].

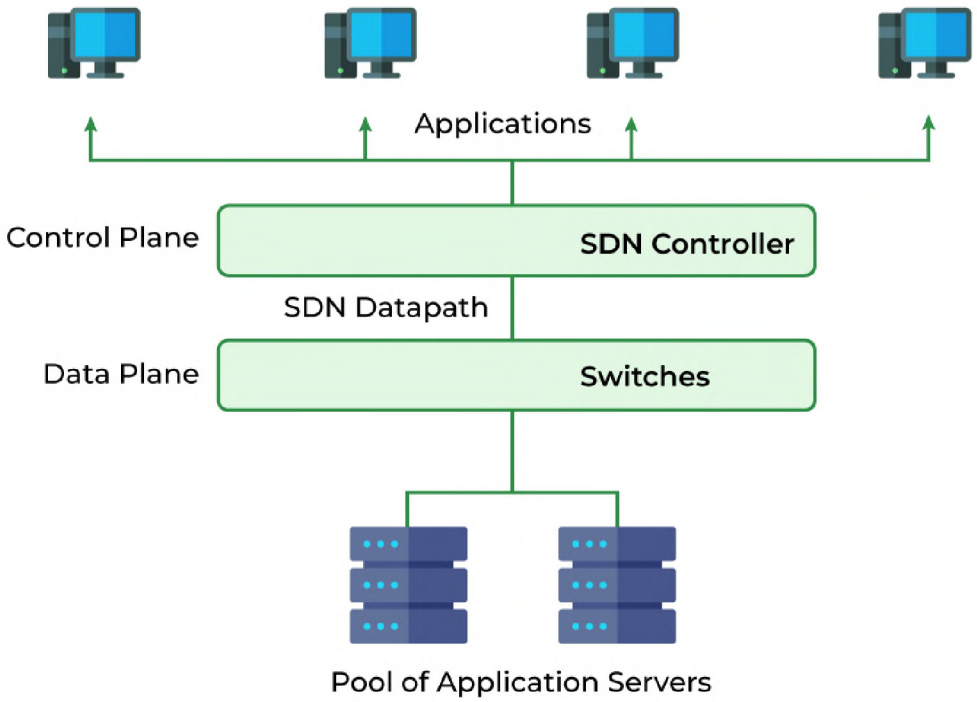

Рисунок 1.4 – Схема мережі з програмно-визначеною архітектурою (SDN) [6]

Мережа з віртуалізацією функцій (NFV) використовує віртуалізацію для виконання мережевих функцій (маршрутизація, комутація, брандмауери тощо) на стандартному апаратному забезпеченні замість спеціалізованих мережевих пристроїв [7]. Мережа NFV характеризується зменшенням витрат на апаратне забезпечення, гнучкістю у розгортанні нових функцій, високою масштабованістю. Підходить для великих організацій, які прагнуть знизити витрати на інфраструктуру (рисунок 1.5).

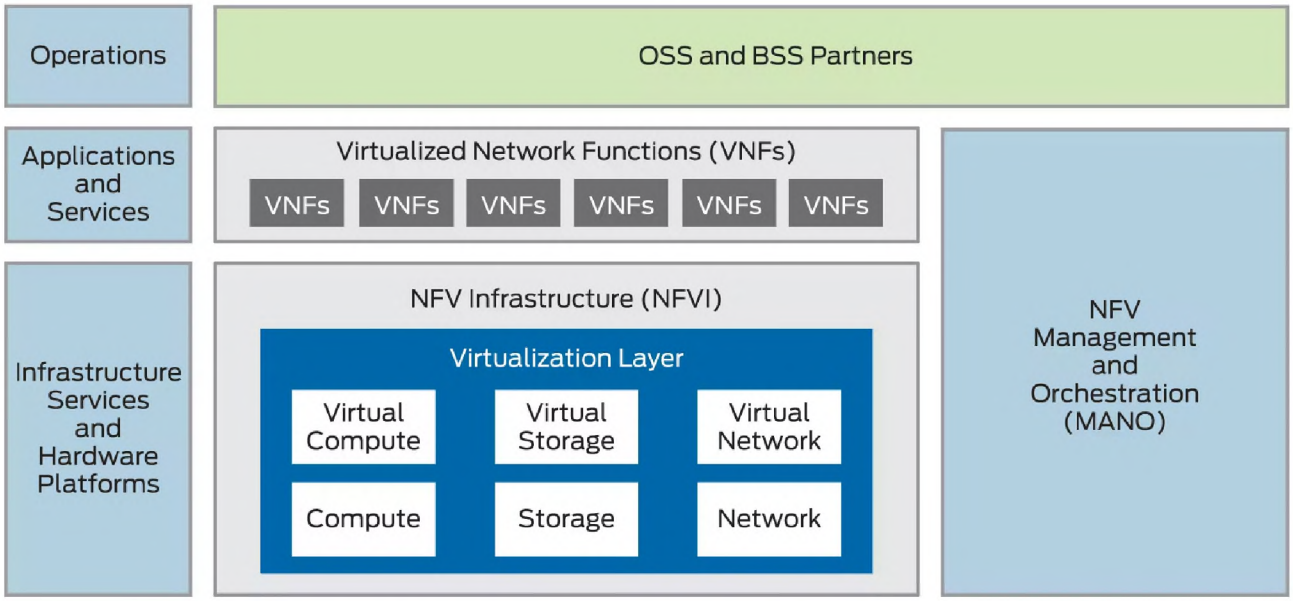

Рисунок 1.5 – Архітектура NFV-мережі [7]

Таблиця 1.4 узагальнює характеристики основних типів архітектур ККМ, їх особливості та придатність для використання у різних типах організацій.

Таблиця 1.4 – Характеристики різних типів архітектур ККМ

Архітектура	Опис	Характеристики	Використання
Клієнт-серверна	Централізоване управління з серверами, що надають ресурси і послуги клієнтам.	Централізоване управління Висока надійність Легкість у забезпеченні безпеки	Великі організації з розвиненою інфраструктурою
Одноранговa (P2P)	Всі пристрої рівноправні, кожен може бути клієнтом і сервером одночасно.	Децентралізована Простота налаштування Складно забезпечити безпеку	Невеликі мережі, робочі групи
Хмарна	Мережа, заснована на хмарних сервісах, де більшість ресурсів знаходяться у хмарі.	Висока масштабованість Зниження витрат Залежність від інтернет-з'єднання	Розподілені організації, гнучкі компанії
Програмно-визначена (SDN)	Управління мережею здійснюється централізовано за допомогою програмного забезпечення.	Централізоване управління Гнучкість та автоматизація Швидка адаптація до змін	Великі підприємства, хмарні середовища
Віртуалізація функцій (NFV)	Використання віртуалізації для виконання мережевих функцій на стандартному обладнанні.	Зниження витрат на апаратне забезпечення Масштабованість Гнучкість у розгортанні функцій	Великі організації, оптимізація інфраструктури

Існуючі архітектури комп'ютерних мереж можуть бути скомбіновані залежно від потреб підприємства, що дозволяє створювати гібридні корпоративні мережі для забезпечення їх оптимальної продуктивності та надійності.

1.2 Характеристики корпоративних комп'ютерних мереж

Головна мета корпоративної мережі – забезпечення безперебійного обміну даними між різними підрозділами підприємства, доступ до інтернету та захист інформації від зовнішніх і внутрішніх загроз. Корпоративна мережа підприємства зазвичай включає в себе декілька основних компонентів, таких як сервери, маршрутизатори, комутатори, брандмауери та точки доступу [8]. Основні характеристики ККМ наведені у таблиці 1.5.

Таблиця 1.5 – Основні характеристики типової корпоративної мережі

Компонент мережі	Опис	Технічні характеристики
Сервери	Центральні вузли мережі, що надають послуги для користувачів і пристроїв.	Процесор Intel Xeon, 64 GB RAM, 10 TB HDD, RAID 5.
Маршрутизатори	Забезпечують маршрутизацію трафіку між локальними мережами та інтернетом.	Підтримка протоколів OSPF, BGP; пропускна здатність до 10 Gbps.
Комутатори	Забезпечують комутацію даних між пристроями в локальній мережі.	Layer 2/3 комутатори з підтримкою VLAN, 24 порти, 1 Gbps на порт.
Брандмауери	Захищають мережу від зовнішніх загроз, фільтруючи трафік.	Підтримка VPN, IDS/IPS, пропускна здатність до 1 Gbps.
Точки доступу Wi-Fi	Забезпечують бездротовий доступ до мережі для мобільних пристроїв.	Підтримка стандартів Wi-Fi 6, покриття до 300 метрів, 2.4/5 GHz.

Архітектура ККМ підприємства зазвичай базується на багаторівневій моделі, яка включає ядро мережі (core), розподільний рівень (distribution) та рівень доступу (access). Така структура дозволяє ефективно керувати трафіком і забезпечувати високий рівень відмовостійкості [9]. Діаграма на рисунку 1.6 ілюструє багаторівневу архітектуру корпоративної мережі.

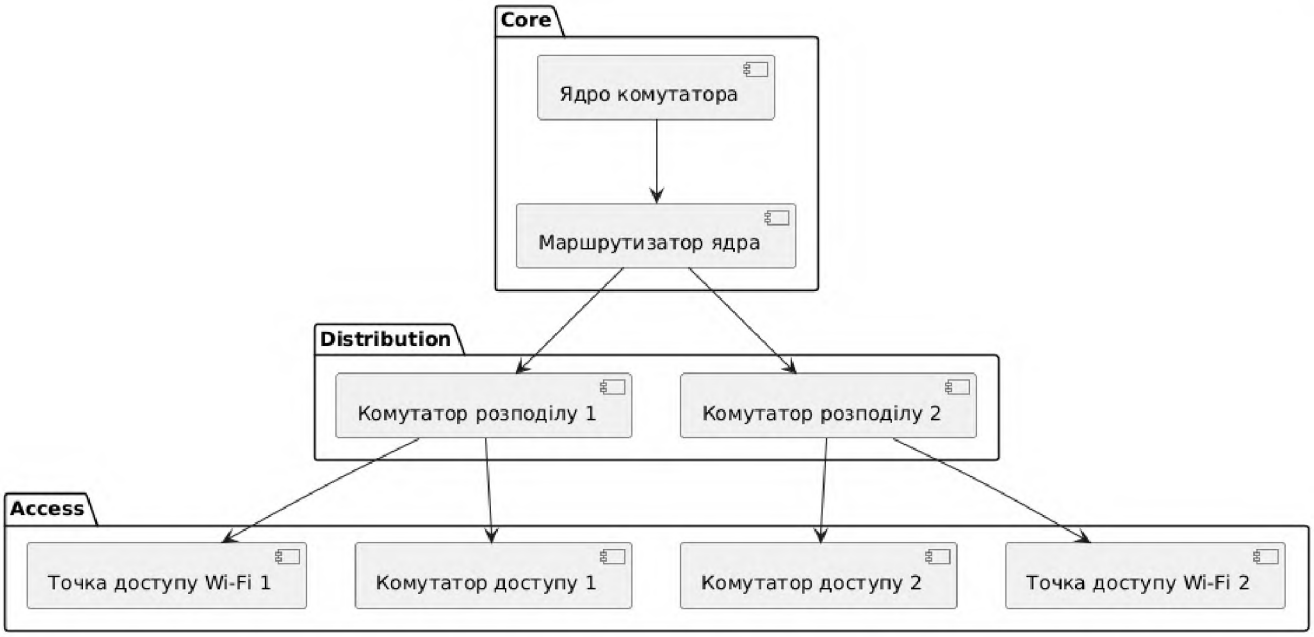

Рисунок 1.6 – Типова архітектура ККМ

Корпоративні мережі зазвичай використовують різні протоколи для забезпечення надійного з'єднання, маршрутизації та безпеки (таблиця 1.6).

Таблиця 1.6 – Основні протоколи ККМ [10]

Протокол	Опис	Використання в мережі підприємства
Протоколи маршрутизації		
OSPF (Open Shortest Path First)	Динамічний протокол маршрутизації, який обирає найкоротший шлях.	Використовується для внутрішньої маршрутизації між підмережами.
BGP (Border Gateway Protocol)	Протокол зовнішньої маршрутизації, що керує обміном між автономними системами.	Забезпечує маршрутизацію між мережею підприємства та інтернетом.
Протоколи безпеки		
IPsec	Протокол шифрування трафіку для забезпечення безпеки передачі даних.	Використовується для забезпечення безпечних VPN-з'єднань.
SSL/TLS	Протокол захисту з'єднань на рівні прикладного шару.	Використовується для захищених вебз'єднань та внутрішніх систем.
Протоколи управління мережею		
SNMP (Simple Network Management Protocol)	Протокол управління мережею для моніторингу та збору даних про стан пристроїв.	Використовується для моніторингу мережевих пристроїв та управління ними.
NetFlow	Протокол для збору інформації про потоки трафіку.	Дозволяє аналізувати трафік у реальному часі для оптимізації мережі.

Діаграма на рисунку 1.7 показує основні протоколи, які використовуються в корпоративній мережі підприємства для маршрутизації, забезпечення безпеки та управління мережею.

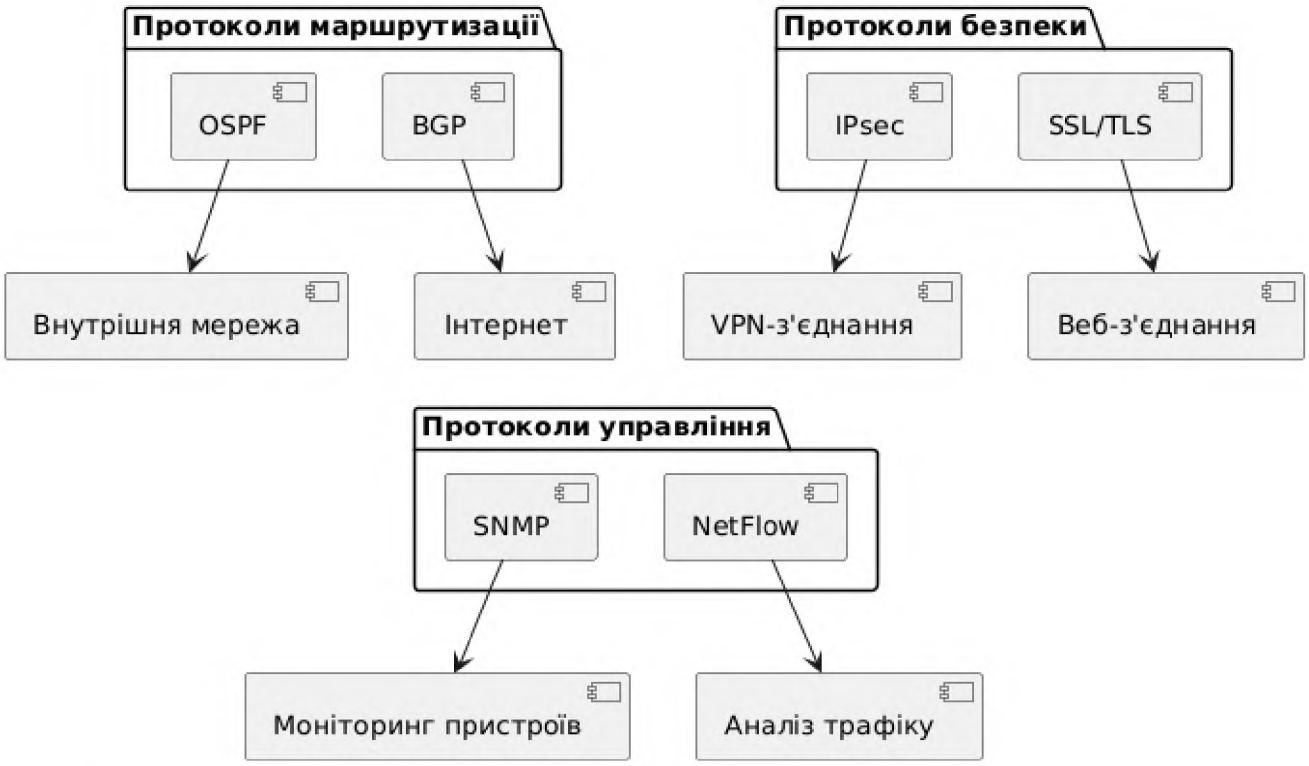

Рисунок 1.7 – Протоколи, що використовуються в мережі підприємства

Таким чином, корпоративна мережа підприємства будується на основі багаторівневої архітектури з використанням сучасних протоколів маршрутизації, безпеки та управління, що забезпечує надійність, безпеку та ефективність її роботи.

1.3 Методи оптимізації комп'ютерних мереж

Сучасні корпоративні мережі постійно розвиваються, тому існує багато методів, спрямованих на їх оптимізацію. Наукова література та інші інформаційні джерела висвітлюють як класичні підходи до оптимізації мереж, так і сучасні методи, що спираються на нові технології, такі як віртуалізація, SDN та QoS [11].

Теоретичні підходи до оптимізації ККМ, які описані у літературі, в основному зосереджуються на різних методах управління трафіком, масштабованості та безпеці (таблиця 1.7).

Таблиця 1.7 – Критичний аналіз теоретичних підходів до оптимізації

Теоретичний підхід	Критичний аналіз
Класичні моделі оптимізації	Добре працюють для статичних та стабільних мереж, але мають обмеження щодо масштабованості та гнучкості.
Сучасні моделі на основі SDN	Пропонують гнучкість та централізоване управління, проте потребують високих початкових інвестицій і нових знань.
Алгоритми балансування трафіку	Класичні алгоритми не враховують поточні навантаження, тоді як сучасні дозволяють динамічно реагувати на зміни.
Мережеве планування на основі віртуалізації	Забезпечує високу ефективність та оптимальне використання ресурсів, але потребує нових підходів до безпеки.

У таблиці 1.8 представлене порівняння класичних та сучасних методів оптимізації ККМ.

Таблиця 1.8 – Порівняння класичних та сучасних методів оптимізації

Метод оптимізації	Класичний підхід	Сучасний підхід
Ручне налаштування мережі	Адміністратори налаштовують маршрути, трафік та безпеку вручну.	Автоматизоване управління за допомогою SDN та програмних рішень.
Статичне балансування навантаження	Статичні правила для розподілу трафіку.	Динамічне балансування навантаження на основі реального часу.
Мережеве планування	Традиційні моделі та топології (наприклад, зіркова топологія).	Використання віртуалізації та хмарних технологій для гнучкості.
Масштабованість	Потрібна закупівля нового обладнання для масштабування мережі.	Легке масштабування за допомогою віртуалізації та хмарних рішень.

З наведеного порівняння видно, що сучасні підходи до оптимізації ККМ дозволяють досягти більшої гнучкості, ефективності та зниження витрат завдяки використанню новітніх технологій.

Отже, основні класичні (традиційні) методи оптимізації ККМ це ручне налаштування, статичне балансування, традиційне мережеве планування. Натомість, до сучасних методів оптимізації мереж належать: централізоване

управління за допомогою SDN, динамічне балансування та використання хмарних рішень (рисунок 1.8).

Рисунок 1.8 – Відповідність класичних та сучасних методів оптимізації ККМ

Дана схема (рисунок 1.8) показує, як сучасні методи оптимізації замінюють або покращують класичні підходи до управління корпоративними мережами, забезпечуючи більшу гнучкість та ефективність.

1.4 Технології оптимізації комп'ютерних мереж

1.4.1 Віртуалізація мережевих ресурсів

Віртуалізація у ККМ дозволяє створювати віртуальні версії фізичних мережевих ресурсів, таких як сервери, комутатори, сховища даних тощо. Головними перевагами віртуалізації у ККМ є: легка масштабованість – віртуалізація забезпечує швидке створення нових віртуальних серверів та пристроїв; гнучкість – віртуалізація забезпечує легке керування мережевими ресурсами та налаштування нових функцій; безпека – завдяки логічній сегментації мережі з покращеними механізмами захисту; економія витрат – мережа потребує менше обладнання та знижує витрати на її підтримку [12]. Зокрема, використання різних видів віртуалізації дозволяє оптимізувати

навантаження на апаратні ресурси, зменшити витрати та підвищити масштабованість мережі (таблиця 1.9).

Таблиця 1.9 – Основні види віртуалізації

Тип віртуалізації	Опис	Переваги
Віртуалізація серверів	Розділення фізичного сервера на кілька віртуальних екземплярів, кожен з яких може виконувати свої завдання.	Підвищення ефективності використання обладнання.
Мережева віртуалізація (NFV)	Створення віртуальних версій мережевих функцій, таких як маршрутизація, комутація та брандмауери.	Гнучке управління і швидке розгортання мережевих функцій.
Віртуалізація сховищ (Storage)	Об'єднання фізичних сховищ даних у віртуальні пули, доступні для користувачів.	Оптимізація зберігання та використання дискового простору.
Десктопна віртуалізація (VDI)	Дозволяє користувачам отримувати доступ до віртуальних робочих столів з будь-якого пристрою.	Підвищення мобільності та безпеки даних.

На рисунку 1.9 представлена діаграма віртуалізації мережевих функцій.

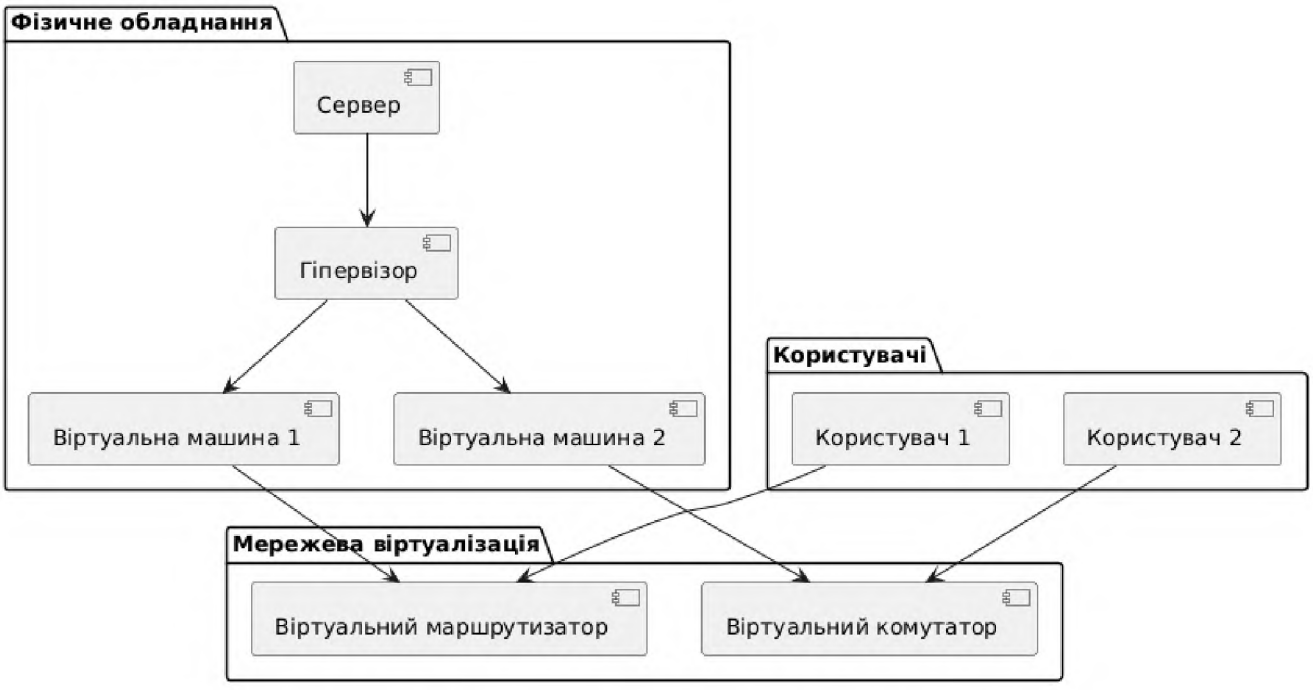

Рисунок 1.9 – Загальна схема віртуалізації ККМ

Ця діаграма демонструє, як віртуальні мережеві функції (маршрутизатор і комутатор) працюють на віртуальних машинах, що працюють на фізичному

сервері з гіпервізором. Користувачі підключаються до цих віртуальних функцій для доступу до мережевих ресурсі.

1.4.2 Впровадження SDN

SDN (програмно-визначені мережі) – це сучасний підхід до побудови та управління ККМ, який передбачає відокремлення контрольної площини (управління мережею) від площини передачі даних (переміщення трафіку), що дозволяє централізовано керувати мережею за допомогою програмного забезпечення, підвищує гнучкість та ефективність управління мережевими ресурсами [13]. Архітектура SDN схематично представлена на рисунку 1.10.

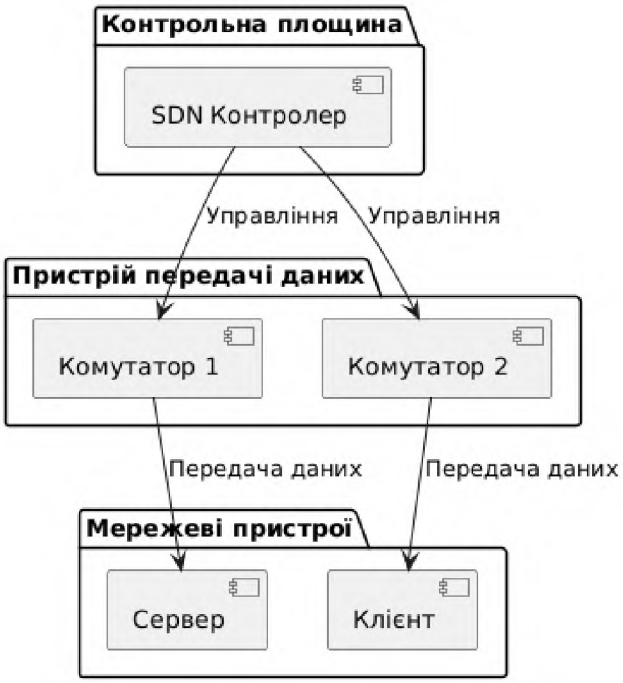

Рисунок 1.10 – Архітектура SDN

SDN контролер – спеціальна програма, що працює на потужному сервері, є центральним елементом, який керує всією мережею. Комутатори отримують команди від контролера і передають трафік між пристроями (сервер і клієнт). Мережеві пристрої (сервер, клієнт) обмінюються даними один з одним через комутатори, під управлінням SDN-контролера. Така архітектура дозволяє динамічно керувати потоком даних, забезпечуючи гнучкість і оптимізацію роботи корпоративної мережі. Основні компоненти SDN описані у таблиці 1.10.

Таблиця 1.10 – Основні компоненти SDN

Компонент	Опис
Контролер SDN	Спеціальна програма, централізований елемент управління мережею, що приймає рішення щодо маршрутизації.
Комутатори/Маршрутизатори	Фізичні або віртуальні пристрої, які передають дані відповідно до вказівок SDN-контролера.
API (Інтерфейс програмування)	Засіб комунікації між контролером і мережевими пристроями для передачі команд.

Важливими перевагами SDN є її гнучкість (SDN дозволяє забезпечити швидке налаштування та перепланування мережі без фізичної зміни обладнання), централізоване управління (контролер SDN управляє всією мережею з однієї точки, спрощуючи її адміністрування), оптимізація трафіку (динамічне перенаправлення трафіку для уникнення перевантажень і забезпечення оптимальної продуктивності), масштабованість (легке розширення мережі без складної конфігурації кожного окремого пристрою).

1.4.3 Технологія QoS

QoS (Quality of Service) – це технологія, що забезпечує управління пріоритетами мережевого трафіку, щоб більш важливі дані мали першочерговий доступ до ресурсів мережі [14]. Основні функції QoS представлені у таблиці 1.11.

Таблиця 1.11 – Основні функції QoS

Функція QoS	Опис
Класифікація трафіку	Визначення, який тип трафіку є критично важливим і який отримує пріоритет.
Маркування трафіку	Додавання міток або тегів до пакетів для ідентифікації пріоритетності.
Обмеження смуги пропускання	Обмеження доступної смуги пропускання для некритичного трафіку.
Управління чергами	Розподіл трафіку по чергах для передачі в порядку пріоритетності.

Впровадження QoS дозволяє оптимізувати роботу корпоративних мереж, зменшити затримки та втрати пакетів для чутливих до якості сервісів, таких як голосовий зв’язок, відеоконференції, обробка транзакцій тощо.

Діаграма на рисунку 1.11 описує типову архітектуру використання технології QoS у корпоративній мережі.

Рисунок 1.11 – Архітектура QoS у корпоративній мережі

Отже, QoS забезпечує ефективне управління трафіком – надає пріоритет критично важливим даним і оптимізує використання мережевих ресурсів: клієнт надсилає трафік до маршрутизатора, маршрутизатор використовує функції QoS для класифікації трафіку, визначає пріоритетність. Завдяки оптимізації за допомогою QoS, трафік із високим пріоритетом передається до сервера швидше.

Впровадження QoS потребує послідовного виконання низки організаційних та технічних заходів (таблиця 1.12).

Таблиця 1.12 – Етапи впровадження технології QoS

Етап	Дія
Аналіз трафіку	Визначення типів трафіку та їхніх вимог до смуги пропускання.
Налаштування пріоритетів	Визначення правил для пріоритетного обслуговування трафіку.
Маркування та класифікація	Призначення трафіку до певних категорій і міток.
Моніторинг і оптимізація	Відстеження ефективності QoS і налаштування для покращення роботи мережі.

Використання QoS забезпечує пріоритетний доступ для таких сервісів, як VoIP, відеоконференції та обробка транзакцій, дозволяє обмежувати доступну смугу пропускання для некритичних застосунків, таких як вебсерфінг або файлообмін, зменшити затори та втрати даних, забезпечити стабільну роботу мережі під час високого навантаження.

Висновки до розділу 1

У першому розділі досліджено теоретико-методологічні аспекти оптимізації корпоративних комп'ютерних мереж, визначено основні поняття, структуру, методи та технології покращення ефективності мережевих процесів.

Описана структура корпоративних комп'ютерних мереж, що базується на трирівневій моделі (рівень доступу, розподілу та ядра) та їх класифікація. Описані основні компоненти ККМ: сервери, маршрутизатори, комутатори, точки доступу та мережеве програмне забезпечення.

Виділено ключові характеристики корпоративних комп'ютерних мереж: продуктивність, масштабованість, безпека та надійність. Визначено основні проблєми, зокрема, затримки трафіку, обмеження пропускної здатності та вразливості до загроз безпеки.

Розглянуто основні методи оптимізації комп'ютерних мереж: сегментація мережі, резервування ресурсів та балансування навантаження.

Представлено технології оптимізації комп'ютерних мереж: віртуалізація, впровадження SDN, технологія QoS.

Загалом, визначено, що оптимізація корпоративних мереж можлива завдяки впровадженню сучасних методів і технологій, таких як віртуалізація, SDN та QoS, які дозволяють підвищити продуктивність, масштабованість і надійність мережевої інфраструктури.

РОЗДІЛ 2
АНАЛІЗ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Проблєми корпоративних мереж та шляхи їх вирішення

Наявність проблєм у корпоративні мережі негативно впливає на роботу організацій: знижується продуктивність, підвищується ризик втрати даних, збільшуються витрати на підтримку інфраструктури тощо.

До основних проблєм сучасних ККМ належать [15]:

- проблєми масштабованості та продуктивності;
- проблєми безпеки;
- проблєми надійності та відмовостійкості.

Сучасні ККМ мають бути здатні до масштабування. Це необхідно, щоб підтримувати постійно зростаючу кількість пристроїв та також користувачів, підключених до мережі. Однак, організації досить часто стикаються з труднощами при спробах розширити свою мережеву інфраструктуру. Якщо комп'ютерна мережа організації не може ефективно обробляти збільшену кількість підключень, вникають такі характерні проблєми, як затримка у передачі даних через недостатню пропускну здатність мережевих каналів, зниження продуктивності через перевантаження маршрутизаторів, комутаторів та інших мережевих пристроїв, надмірні витрати на модернізацію апаратного забезпечення та збільшення пропускної здатності. Це характерно для організацій, які поступово розширювали свої мережі без комплексного планування. Особливо складним може бути масштабування старих комп'ютерних мереж, які не були з самого початку спроєктовані для обробки великих обсягів трафіку.

З кожним роком зростає кількість і складність кібератак, спрямованих на ККМ. Сучасні загрози, такі як атаки типу DDoS, фішинг, впровадження зловмисного програмного забезпечення (malware) та ін., потребують від організацій постійного вдосконалення своїх систем безпеки. Типові проблєми безпеки включають: недостатність захисту від зовнішніх атак, коли мережа не має

адекватних засобів захисту (брандмауерів, системи виявлення вторгнень); внутрішні загрози, такі як несанкціонований доступ до даних від працівників або компрометація облікових записів; невчасне оновлення програмного забезпечення та вразливості в операційних системах і мережевих пристроях, які можуть бути використані для атак; проблєми із шифруванням трафіку та безпекою підключень у віддаленому доступі (VPN), що є критичним у сучасних умовах дистанційної роботи. Без надійних механізмів захисту та моніторингу компанії можуть втратити цінні дані або зазнати значних фінансових збитків унаслідок простоїв.

Надійність ККМ є важливою для забезпечення безперебійної роботи бізнес-процесів. Відмовостійкість означає здатність мережі продовжувати функціонувати навіть у разі виходу з ладу окремих компонентів. Типовими проблємами відмовостійкості є: відсутність резервування ключових мережевих компонентів (серверів, маршрутизаторів, комутаторів), що призводить до простоїв у разі їх виходу з ладу; нестабільні підключення, спричинені застарілими або неправильно налаштованими мережевими пристроями; простій мережі внаслідок відсутності механізмів автоматичного відновлення (Failover, Redundancy); недосконалий моніторинг мережевих процесів, що призводить до затримки виявлення та вирішення проблєм. Питання надійності та відмовостійкості особливо актуальні для великих підприємств, де простій мережі навіть на короткий час може призвести до значних фінансових втрат та негативного впливу на репутацію.

Вирішення проблєми масштабованості ККМ ґрунтується на застосуванні кількох основних підходів, до яких належать [15]:

- сегментація мережі;
- оптимізація маршрутизації та балансування трафіку;
- автоматизація адміністрування та моніторингу стану мережі.
- застосування більш потужного обладнання;
- впровадження технологій віртуалізації (NFV);
- використання програмно-визначених мереж (SDN);
- впровадження хмарних технологій.

Використання віртуалізації мережевих функцій (NFV) дозволяє запускати кілька віртуальних мережевих сервісів на одному фізичному пристрої. Це дає змогу масштабувати мережу шляхом створення нових віртуальних екземплярів без необхідності придбання додаткового обладнання.

Використання програмно-визначених мереж (SDN) дозволяє централізовано керувати мережею за допомогою програмного забезпечення, забезпечує гнучкість у налаштуванні та масштабуванні мережі, дозволяє динамічно керувати трафіком і швидко адаптувати мережу до нових вимог.

Якщо мережа перевантажена, доцільно додати більш потужні маршрутизатори, комутатори або інше мережеве обладнання з вищою пропускною здатністю, що зменшить затримки і дозволить обробляти більший обсяг трафіку.

Застосування алгоритмів балансування навантаження між різними серверами або мережевими пристроями дозволить рівномірно розподілити трафік, знизити перевантаження одних частин мережі і більш ефективно використовувати наявні ресурси.

Перенесення частини мережевих функцій до хмари дозволяє легко масштабувати інфраструктуру за допомогою хмарних сервісів (AWS, Microsoft Azure, Google Cloud). Такий підхід зменшує залежність від локального апаратного забезпечення і забезпечує гнучкість в управлінні ресурсами.

Розподіл корпоративної мережі на менші, логічно ізольовані сегменти (наприклад, за допомогою VLAN) дозволяє ефективніше керувати трафіком та уникати перевантажень. Крім того, це також підвищує рівень безпеки і контроль над різними частинами мережі.

Впровадження систем автоматичного моніторингу та управління трафіком дозволяє виявляти проблєми продуктивності в режимі реального часу і автоматично коригувати роботу мережі для запобігання перевантаженням.

Комплексне застосування розглянутих рішень дозволяє забезпечити масштабованість корпоративної мережі та підвищити її продуктивність у міру зростання вимог до інфраструктури.

Для підвищення безпеки корпоративних мереж існують різні методи, що допомагають захистити інфраструктуру від зовнішніх і внутрішніх загроз [16]:

- використання брандмауерів (Firewall);
- шифрування даних;
- використання віртуальних приватних мереж (VPN);
- мережева сегментація;
- системи виявлення і запобігання вторгнень (IDS/IPS);
- аутентифікація (MFA) та контроль доступу (Access Control);
- антивірусне програмне забезпечення;
- моніторинг і логування;
- регулярне оновлення програмного забезпечення;
- навчання співробітників;
- резервне зберігання даних (бекап).

Брандмауери – базовий метод захисту від несанкціонованого доступу до мережі. Вони контролюють вхідний і вихідний трафік, дозволяючи лише авторизовані підключення і блокуючи небезпечний трафік. Застосування шифрування для всіх даних, які передаються через мережу, допомагає захистити їх від перехоплення. Для забезпечення конфіденційності даних рекомендується використання спеціальних технологій шифрування, таких як SSL/TLS для вебз'єднань і IPsec для мережевих з'єднань. Віртуальні приватні мережі (VPN) забезпечують безпечний тунель для передавання даних через публічні мережі, шифруючи трафік і захищаючи його від несанкціонованого доступу. Сегментація мережі розділяє різні частини мережі на ізольовані сегменти, що знижує ризик поширення загроз, а також обмежує доступ користувачів і пристроїв до критично важливих ресурсів. Системи IPS (система запобігання вторгнень) та IDS (система виявлення вторгнень) дозволяють відслідковувати мережевий трафік з метою виявлення аномальної активності та блокування потенційних атак у режимі реального часу. Використання багатофакторної аутентифікації (MFA) вимагає більше ніж один фактор підтвердження особи, завдяки чому підвищує рівень захисту облікових записів. Також важливо впроваджувати системи управління

доступом (Access Control) для обмеження доступу до мережевих ресурсів на основі ролей і прав користувачів. Антивірусні програми сканують і блокують зловмисне програмне забезпечення, що може проникати до корпоративної мережі через різні канали, такі як електронна пошта або вебсайти. Постійний моніторинг активності мережі та ведення журналів подій (логів) також допомагає швидко виявляти підозрілу активність і відслідковувати дії користувачів та пристроїв. Для автоматизованого аналізу цих подій використовують спеціальні системи SIEM (Security Information and Event Management). Своєчасне оновлення програмного забезпечення та апаратного забезпечення є важливим для закриття вразливостей, через які можуть бути здійснені атаки на мережу. Навчання співробітників, підвищення їх обізнаності про основні загрози та методи кібербезпеки (наприклад, розпізнавання фішинг-атак) допомагає зменшити ризики внутрішніх загроз і помилкових дій, які можуть призвести до витоку даних. Регулярне резервне копіювання даних захищає компанію від втрати інформації у випадку кібератаки або збою системи, дозволяючи швидко відновити роботу.

Всі вказані вище методи у поєднанні дозволяють створити багаторівневу систему захисту корпоративної мережі, що значно підвищує її стійкість до різноманітних загроз.

Для забезпечення надійності корпоративних мереж так само можна застосувати низку підходів та рішень, зокрема [16]:

- резервування обладнання (Redundancy);
- впровадження протоколів відмовостійкості (Failover Protocols);
- балансування навантаження (Load Balancing);
- моніторинг і управління мережею;
- автоматичне відновлення (Self-Healing Networks);
- регулярне тестування та аудит;
- бекап та відновлення даних;
- оптимізація планування та інфраструктури;
- навчання персоналу.

Забезпечення резервних компонентів мережі, таких як маршрутизатори, комутатори та сервери, дозволяє уникнути простоїв у разі виходу з ладу одного з пристроїв. Це може включати: резервні інтернет-канали, дублювання мережевих шляхів і зв'язків, використання кількох серверів або кластерів для балансування навантаження та зменшення ризику відмови. Спеціальні протоколи, такі як VRRP (Virtual Router Redundancy Protocol) або HSRP (Hot Standby Router Protocol), забезпечують автоматичне переключення на резервний пристрій у випадку виходу з ладу основного маршрутизатора або комутатора. Використання балансувальників навантаження дозволяє рівномірно розподіляти трафік між кількома серверами або мережевими пристроями. Це зменшує ймовірність перевантаження одного пристрою та забезпечує стабільну роботу мережі. Системи моніторингу мережі, такі як Nagios, Zabbix або SolarWinds, дозволяють виявляти потенційні проблєми до того, як вони вплинуть на роботу мережі. Постійний моніторинг стану мережевих компонентів і трафіку допомагає оперативно реагувати на збої та відхилення в роботі. Відмовостійка архітектура передбачає проєктування мережі таким чином, щоб навіть при виході з ладу одного компонента система продовжувала працювати. Це можна досягти, зокрема, за рахунок використання кільцевих або сіткових топологій (Ring або Mesh), які дозволяють перенаправити трафік через інші шляхи у випадку збою, а також впровадження високодоступних систем (HA) для критично важливих сервісів. Деякі сучасні мережі можуть автоматично виявляти та виправляти проблєми, забезпечуючи автоматичне відновлення з'єднань, коригування конфігурацій або перемикання трафіку на резервні маршрути без втручання адміністратора. Проведення регулярних тестів мережевих систем, таких як тестування відмовостійкості та аудит конфігурацій, допомагає виявляти слабкі місця та потенційні проблєми, які можуть вплинути на надійність мережі. Створення резервних копій мережевих конфігурацій, критичних даних та сервісів дозволяє швидко відновити роботу системи у випадку збою або атаки. Регулярні бекапи забезпечують надійне відновлення після аварійних ситуацій. Правильне проєктування мережевої інфраструктури з урахуванням можливого збільшення

навантаження або зміни умов експлуатації дозволяє уникнути несподіваних простоїв та збільшити надійність мережі. Це також включає адаптацію до нових технологій і можливостей мережевих рішень. Регулярне навчання мережевих адміністраторів щодо новітніх технологій, методів моніторингу та реагування на аварійні ситуації допомагає оперативно вирішувати проблєми і зменшує ризик людських помилок, які можуть вплинути на надійність мережі.

Застосування зазначених вище методів дозволяє підвищити надійність ККМ, зменшити ризики простоїв і забезпечити стабільну роботу інфраструктури.

Для балансування навантаження в корпоративних мережах використовуються різні підходи, які допомагають ефективно розподіляти трафік і запобігати перевантаженню окремих серверів або мережевих пристроїв [17]:

- балансувальники навантаження (Load Balancers);
- DNS-балансування (DNS Load Balancing);
- алгоритми балансування навантаження;
- балансування на рівні транспортного та прикладного протоколів (L4 і L7 Load Balancing);
- використання кластерів серверів;
- балансування навантаження у хмарних середовищах;
- віртуалізація та контейнеризація;
- моніторинг і автоматичне масштабування.

Балансувальники навантаження – це спеціалізовані пристрої або програмне забезпечення, які рівномірно розподіляють вхідний трафік між кількома серверами або мережевими ресурсами. Вони забезпечують розподіл трафіку на основі поточного навантаження або рівномірного розподілу запитів, високу доступність сервісів за рахунок розподілу навантаження на кілька серверів, автоматичне перемикання на резервні ресурси в разі збою одного з серверів. DNS-балансування використовує систему доменних імен (DNS) для розподілу трафіку між кількома серверами. Коли користувач надсилає запит до домену, сервер DNS повертає різні IP-адреси на основі певних алгоритмів, таких як кругове балансування (Round Robin), коли запити розподіляються рівномірно по черзі між

серверами, або вибір за географічним розташуванням (Geo DNS) – трафік спрямовується до найближчого сервера залежно від місця розташування користувача.

Балансувальники використовують різні алгоритми для розподілу навантаження: Round Robin – запити розподіляються по черзі між серверами; Least Connections – трафік спрямовується до сервера з найменшою кількістю активних з'єднань; Weighted Round Robin – сервери з більшими можливостями отримують більше запитів; Source IP Hash – трафік розподіляється на основі хешування IP-адреси джерела, що дозволяє кожному користувачу підключатися до одного й того ж сервера.

Балансування на рівні 4 (L4) відбувається на рівні транспортного протоколу (TCP/UDP). Запити спрямовуються на основі IP-адреси та портів, без аналізу вмісту пакетів. Балансування на рівні 7 (L7) відбувається на рівні прикладного протоколу (HTTP/HTTPS). Балансувальник може аналізувати вміст запитів і приймати рішення на основі URL, cookie або заголовків. Для балансування навантаження між кількома фізичними або віртуальними серверами використовується кластерна архітектура. Сервери в кластері працюють як один логічний ресурс, і запити рівномірно розподіляються між ними. Це забезпечує масштабованість (кількість серверів можна збільшити в разі зростання навантаження) та відмовостійкість мережі (у разі виходу з ладу одного сервера інші продовжують обробляти запити).

Хмарні провайдери, такі як AWS, Microsoft Azure, Google Cloud, надають вбудовані сервіси для балансування навантаження, які автоматично розподіляють трафік між кількома віртуальними машинами або хмарними сервісами, забезпечуючи високу доступність та продуктивність. Використання технологій віртуалізації (наприклад, VMware) та контейнеризації (Docker, Kubernetes) дозволяє динамічно масштабувати ресурси і розподіляти навантаження між віртуальними екземплярами. Kubernetes, зокрема, надає вбудовані механізми балансування навантаження для контейнеризованих додатків. Системи моніторингу продуктивності дозволяють автоматично коригувати балансування

навантаження в реальному часі. Використання автоматичного масштабування (Auto Scaling) в хмарних середовищах дозволяє додавати нові ресурси або вимикати зайві в разі зміни навантаження.

Ці підходи дозволяють ефективно управляти трафіком у корпоративних мережах, підвищуючи продуктивність і надійність мережевої інфраструктури.

2.2 Аналіз ефективності корпоративних мереж

2.2.1 Оцінювання пропускної здатності та використання ресурсів

Ефективність мережі залежить від того, наскільки добре використовуються її ресурси, чи забезпечена належна безпека і надійність для захисту даних і уникнення простоїв [18, 19].

Використання ресурсів мережі залежить від того, наскільки ефективно використовуються комутатори, маршрутизатори, сервери та інші мережеві компоненти для обробки трафіку. Пропускна здатність мережі (bandwidth) визначається максимальним обсягом даних, який може бути переданий через мережу за одиницю часу. Для оцінки навантаження на мережу використовується відсоткове використання ресурсів, яке показує наскільки ефективно використовується пропускна здатність і чи є потенціал для оптимізації мережі.

Типові показники оцінки пропускної здатності окремих компонентів комп'ютерних мереж [20] представлені у таблиці 2.1.

Таблиця 2.1 – Типові показники оцінки пропускної здатності компонентів комп'ютерних мереж

Компонент мережі	Максимальна пропускна здатність	Середнє використання ресурсів
Комутатори ядра	10 Gbps	60%
Маршрутизатори розподілу	1 Gbps	75%
Сервери	1 Gbps	80%
Точки доступу Wi-Fi	867 Mbps (Wi-Fi 5), 1.2 Gbps (Wi-Fi 6)	50%

Діаграма на рисунку 2.1 представляє оцінку пропускної здатності та використання ресурсів на різних рівнях корпоративної мережі та дозволяє визначити найбільш навантажені компоненти.

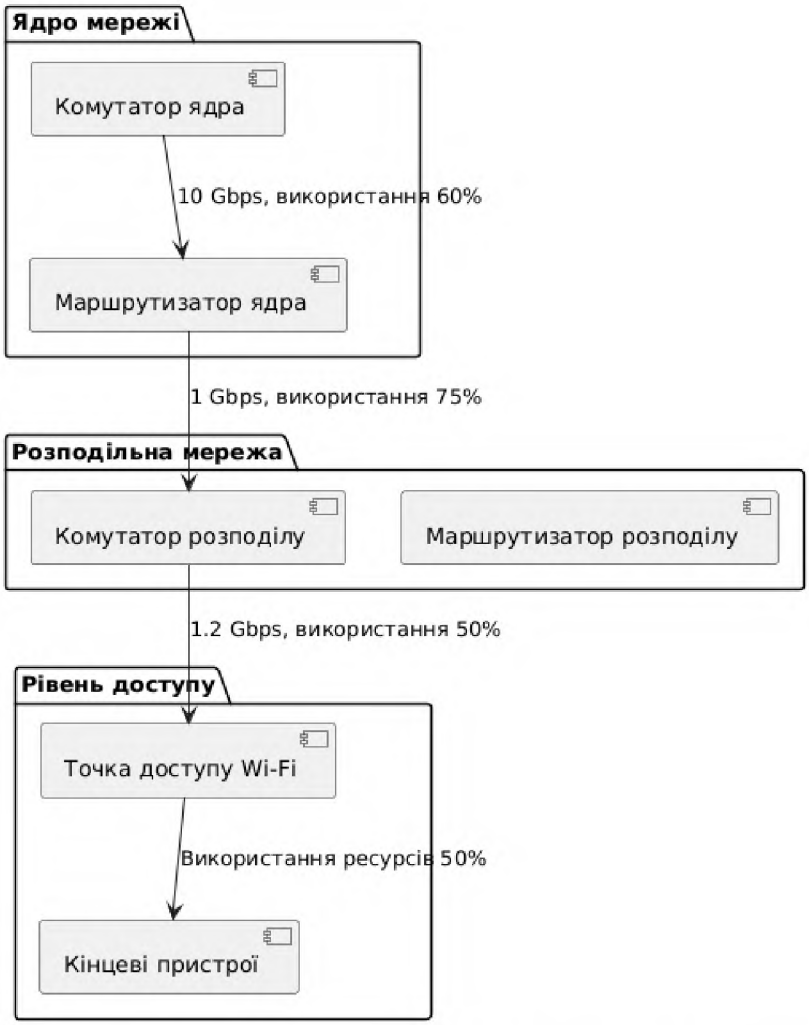

Рисунок 2.1 – Оцінка пропускної здатності мережі

Високе значення показника використання ресурсів (>70%) свідчить про необхідність оптимізації роботи обладнання або масштабування мережі.

2.2.2 Аналіз рівня безпеки та надійності мережі

Безпека та надійність є важливими показниками ефективності мережі. Безпека включає захист від несанкціонованого доступу, шифрування даних, а також впровадження антивірусних систем та систем запобігання зовнішньому проникненню у мережу. Безпека мережі досягається запровадженням спеціальних механізмів безпеки, що використовуються у різних випадках (таблиця 2.1).

Таблиця 2.2 – Оцінка ефективності різних механізмів безпеки [21]

Механізм безпеки	Рівень впровадження	Коментар
VPN (IPsec)	Високий	Використовується для захищених з'єднань з віддаленими працівниками.
Брандмауер	Високий	Встановлені правила фільтрації трафіку, активовано IDS/IPS.
Антивірусна система	Середній	Захист серверів, але недостатньо впроваджений для кінцевих користувачів.
Шифрування даних (SSL/TLS)	Високий	Активне шифрування для вебтрафіку та передачі даних.

Надійність визначає здатність мережі працювати без збоїв та можливість швидкого відновлення її працездатності у разі виникнення проблєм.

Діаграма на рисунку 2.4 ілюструє механізми безпеки та надійності, які можуть бути впроваджені в корпоративній мережі, і показує, як ці компоненти забезпечують захист і стабільність роботи мережі.

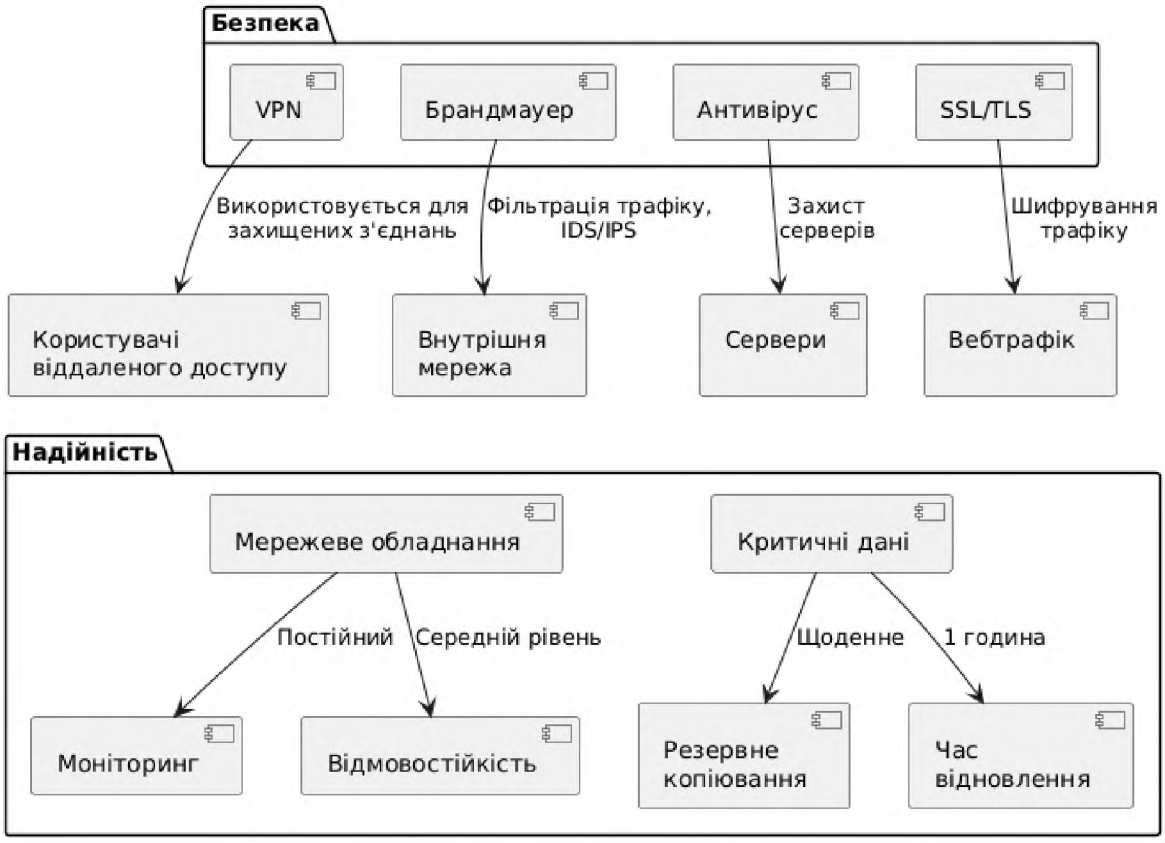

Рисунок 2.2 – Безпека та надійність мережі

Основні фактори надійності ККМ та їх оцінка представлені у таблиці 2.3.

Таблиця 2.3 – Фактори надійності ККМ та їх оцінка

Фактор надійності	Поточний стан	Коментар
Резервне копіювання	Високий	Щоденне резервне копіювання критичних даних.
Відмовостійкість	Середній	Немає повного резервування обладнання на рівні комутаторів.
Моніторинг мережі	Високий	Постійний моніторинг через SNMP та NetFlow.
Час відновлення після збоїв	1 година	Середній час відновлення системи після критичного збою.

Аналіз існуючої конфігурації мережі показав, що мережа має досить високу пропускну здатність, однак окремі компоненти (маршрутизатори розподілу та сервери) наближаються до критичного рівня використання ресурсів. Безпека мережі в цілому задовільна, однак потрібно покращити антивірусний захист для кінцевих користувачів та впровадити повне резервування обладнання для підвищення рівня відмовостійкості.

2.3 Виявлення проблєм та вузьких місць у функціонуванні мережі

2.3.1 Проблєми затримки передачі даних

Основні фактори, що спричиняють затримки передачі даних у ККМ, включають перевантаження мережі, неправильно налаштовані маршрути, недостатню пропускну здатність окремих компонентів мережі (таблиця 2.4).

Таблиця 2.4 – Основні причини затримок у мережі

Причина затримок	Опис
Перевантаження комутаторів	Високе навантаження на комутатори через збільшену кількість підключень.
Перевантаження каналів	Невідповідність пропускної здатності каналів передавання даних і трафіку.
Неправильна маршрутизація	Неоптимальні маршрути, що спричиняють довший шлях передачі даних.
Конфлікти VLAN	Неправильна конфігурація VLAN призводить до дублювання трафіку і затримок.
Відсутність QoS	Відсутність належного управління пріоритетами трафіку.

Затримки у передачі даних можуть негативно вплинути на ефективність роботи мережі, особливо для таких сервісів, як відеоконференції, VoIP та обробка транзакцій у реальному часі. Діаграма на рисунку 2.3 представляє основні фактори, що спричиняють затримки передачі даних у ККМ.

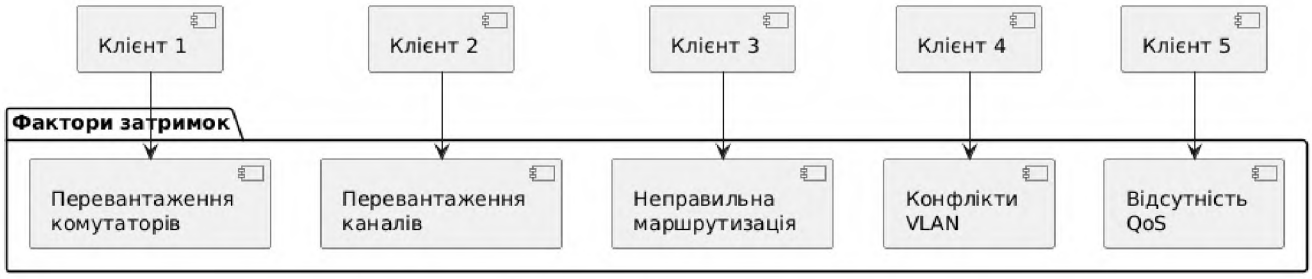

Рисунок 2.3 – Фактори затримки у передачі даних

Основні шляхи усунення проблєми затримок: впровадження QoS для забезпечення пріоритетного оброблення критичного трафіку; модернізація комутаторів і збільшення пропускної здатності каналів для уникнення перевантажень; оптимізація маршрутів для скорочення часу передачі пакетів.

2.3.2 Вузькі місця у процесі масштабування мереж

Масштабування мережі може бути ускладнене через низку факторів, які обмежують можливість додавання нових пристроїв або збільшення пропускної здатності мережі (таблиця 2.5).

Таблиця 2.5 – Основні вузькі місця при масштабуванні мережі

Вузьке місце	Опис
Обмежена пропускна здатність	Канали зв'язку не підтримують більший обсяг трафіку при збільшенні мережі.
Застарілі маршрутизатори	Старі маршрутизатори не підтримують сучасні стандарти, що обмежує розширення.
Відсутність резервування	Відсутність резервних шляхів у топології ускладнює розширення мережі.
Неправильна конфігурація VLAN	Конфлікти або неефективне використання VLAN ускладнюють управління трафіком.
Відсутність централізованого управління	Відсутність SDN або централізованого управління ускладнює масштабування.

Основними можна назвати фізичні обмеження обладнання, недостатню смугу пропускання, неправильно спроєктовану топологію та проблєми з управлінням трафіком.

Діаграма на рисунку 2.4 демонструє основні вузькі місця, які виникають при спробах масштабування мережі. Розуміння цих проблєм дозволяє краще уявити, де саме потрібно впровадити зміни для забезпечення подальшого зростання мережі.

Рисунок 2.4 – Вузькі місця при масштабуванні мережі

Поява проблєм із затримками у передачі даних та вузьких місць у процесі масштабування мережі вказує на те, що необхідно впровадити модернізацію обладнання, оптимізацію конфігурацій мережі та впровадження сучасних технологій управління.

2.4 Напрямки оптимізації та покращення мережевих процесів

2.4.1 Покращення архітектури мережі

Можливості щодо оптимізації архітектури та впровадження новітніх технологій для підвищення ефективності корпоративної мережі включають оновлення архітектури, застосування сучасних підходів до управління мережею, а також інтеграцію новітніх технологій, таких як SDN, QoS та віртуалізація.

Загальні шляхи усунення вузьких місць при масштабуванні це: модернізація обладнання – впровадження маршрутизаторів та комутаторів з підтримкою сучасних стандартів (наприклад, 10 Gbps); централізація управління за допомогою SDN для ефективного управління трафіком і маршрутизацією; оптимізація VLAN для кращого розподілу трафіку та уникнення конфліктів. Більш детально, покращення пропускної здатності корпоративної мережі можна досягти за допомогою наступних підходів та методів [22-30]:

- модернізація мережевого обладнання;
- оптимізація налаштувань мережі;
- впровадження технології QoS;
- використання сучасних протоколів маршрутизації;
- мережева віртуалізація та SDN;
- збільшення смуги пропускання каналів зв'язку;
- використання кешування даних;
- балансування навантаження;
- оптимізація бездротової мережі.

Модернізація мережевого обладнання передбачає, перш за все, оновлення комутаторів і маршрутизаторів до сучасних моделей із підтримкою вищої пропускної здатності (наприклад, перехід з 1 Gbps на 10 Gbps або навіть 40/100 Gbps) та використання Layer 3 комутаторів, які можуть швидше обробляти трафік та маршрутизувати його на основі IP-адрес, що допомагає знизити навантаження на маршрутизатори.

Оптимізація налаштувань мережі включає, зокрема: налаштування VLAN для поділу трафіку і зниження перевантаження в одній підмережі, що допомагає зменшити кількість широкомовних запитів і покращити продуктивність; використання агрегації каналів (Link Aggregation) для об'єднання кількох фізичних ліній у один логічний канал, що дозволяє збільшити пропускну здатність між мережевими пристроями.

Впровадження технології QoS забезпечує налаштування пріоритетів для критичного трафіку, наприклад, для відеоконференцій або VoIP, що дозволяє

забезпечити гарантовану пропускну здатність для важливих застосунків; обмеження смуги пропускання для некритичних сервісів, таких як файловий обмін, щоб уникнути перевантаження мережі. Використання сучасних протоколів маршрутизації охоплює: перехід на динамічні протоколи маршрутизації, такі як OSPF або BGP, які можуть автоматично обирати оптимальні маршрути для трафіку, знижуючи затримки і підвищуючи ефективність використання мережі; оптимізацію маршрутизації на основі трафіку, щоб уникнути перевантаження окремих сегментів мережі [31-37].

Впровадження віртуалізації мережевих функцій (NFV) дозволяє ефективніше використовувати ресурси і зменшувати навантаження на фізичні пристрої. SDN дозволяє централізовано управляти мережею і динамічно перенаправляти трафік для уникнення вузьких місць і збільшення пропускної здатності. Оренда або покупка каналів зв'язку з більшою пропускною здатністю (наприклад, переходи з оптичного інтернету на швидші магістральні канали). Налаштування проксі-серверів та кеш-серверів, які можуть зберігати локальні копії часто використовуваних даних. Це зменшить навантаження на зовнішні канали та прискорить доступ до даних для користувачів. Використання балансувальників навантаження для рівномірного розподілу трафіку між кількома серверами або мережевими ресурсами. Це дозволяє уникнути перевантаження окремих вузлів і забезпечити стабільну роботу мережі. Оптимізація бездротової мережі означає: використання нових стандартів Wi-Fi, таких як Wi-Fi 6, які підтримують більшу пропускну здатність та кількість одночасних підключень; збільшення кількості точок доступу та налаштування їх для рівномірного покриття, щоб уникнути перевантажень в одній точці.

Таким чином, покращення пропускної здатності мережі вимагає комплексного підходу, включаючи оновлення обладнання, оптимізацію налаштувань та впровадження сучасних технологій, таких як QoS, SDN і балансування навантаження [38-49].

Пропозиції щодо покращення архітектури мережі для усунення актуальних проблєм представлені у таблиці 2.6.

Таблиця 2.6 – Актуальні проблєми у мережі та пропозиції щодо їх подолання

Актуальні проблєми	Пропозиції щодо покращення архітектури мережі	Додаткові рекомендації
Перевантаження на рівні комутаторів і маршрутизаторів	Запровадити Layer 3 комутатори на рівні розподілу для зниження навантаження на маршрутизатори. Збільшити пропускну здатність маршрутизаторів до 10 Gbps на рівні ядра.	Впровадити QoS для пріоритизації критичного трафіку.
Відсутність резервування на рівні комутаторів доступу	Додати резервні комутатори на рівні доступу для забезпечення безперебійної роботи. Запровадити STP (Spanning Tree Protocol) для уникнення петльових з'єднань.	Використовувати LACP (Link Aggregation Control Protocol) для об'єднання каналів.
Неправильна маршрутизація, що призводить до затримок	Використати динамічні протоколи маршрутизації, такі як OSPF, для оптимізації передачі даних. Інтегрувати маршрутизатори із SDN-контролерами для централізованого управління маршрутами.	Виконати регулярний аналіз продуктивності маршрутів через інструменти моніторингу.

На рисунку 2.6 представлена діаграма покращеної архітектури мережі, що дозволяє подолати вказані проблєми.

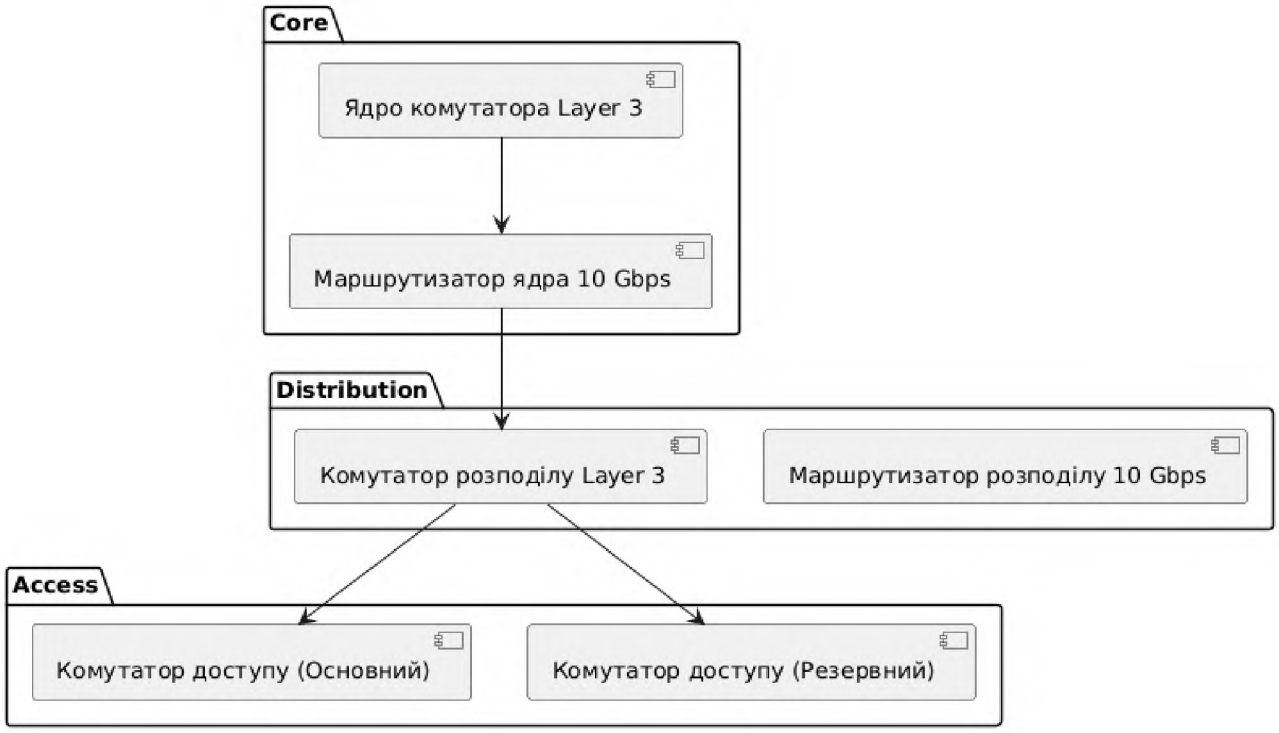

Рисунок 2.5 – Покращена архітектура мережі

Ця діаграма описує покращену архітектуру з резервними комутаторами на рівні доступу, модернізованими маршрутизаторами на рівні ядра і розподілу, а також інтеграцією комутаторів Layer 3 для ефективної маршрутизації.

2.4.2 Використання новітніх технологій

Сучасні ККМ потребують впровадження новітніх технологій для забезпечення високої продуктивності, надійності та гнучкості в управлінні ресурсами. Серед основних інноваційних підходів особливе місце займають SDN, QoS, NFV та технології балансування навантаження. Узагальнена інформація щодо переваг кожної з цих технологій представлена у таблиці 2.7.

Таблиця 2.7 – Новітні технології для покращення роботи ККМ

Технологія	Переваги для мережі
SDN	Централізоване управління мережею, динамічне налаштування маршрутів та трафіку.
QoS	Пріоритетний доступ для критичних сервісів, зниження затримок та втрат пакетів.
NFV	Розподіл мережевих функцій на віртуальні сервери для оптимізації використання ресурсів.
Балансування навантаження	Рівномірний розподіл трафіку між серверами для уникнення перевантаження окремих ресурсів.

Впровадження новітніх технологій у корпоративну комп'ютерну мережу (ККМ) є необхідним кроком для підвищення продуктивності, надійності та гнучкості мережевої інфраструктури.

Основними напрямами модернізації мереж є інтеграція SDN для централізованого управління, використання QoS для оптимізації трафіку та балансування навантаження для ефективного розподілу ресурсів. Впровадження SDN та QoS є важливими кроками для оптимізації корпоративної комп'ютерної мережі. SDN забезпечує централізоване управління мережею, дозволяє динамічно налаштовувати маршрути трафіку та ефективно контролювати ресурси. Водночас QoS сприяє пріоритизації критичного трафіку, знижуючи затримки, втрати пакетів і забезпечуючи стабільну роботу важливих сервісів, таких як VoIP та відеоконференції. Узагальнені пропозиції щодо впровадження представлені у таблиці 2.8.

Таблиця 2.8 – Пропозиції щодо впровадження новітніх технологій підвищення продуктивності, надійності та гнучкості мереж

Технологія	Пропозиції щодо впровадження	Очікувані переваги
SDN	Інтеграція SDN для централізованого управління мережевими компонентами. Використання SDN-контролера для моніторингу та динамічного налаштування маршрутів трафіку.	Динамічна маршрутизація трафіку для уникнення затримок. Моніторинг у реальному часі.
QoS	Запровадження QoS для управління трафіком та встановлення пріоритетів для критичних сервісів. Обмежити смугу пропускання для некритичних сервісів.	Пріоритетний доступ для критичних сервісів. Зменшення перевантаження мережі.
Балансування навантаження	Використання балансувальників навантаження для рівномірного розподілу трафіку між серверами. Запровадження автоматичного балансування під час пікових навантажень.	Оптимальне використання серверних ресурсів. Збільшення пропускної здатності мережі.
NFV	Віртуалізація основних мережевих функцій (маршрутизація, балансування, брандмауери) на програмному рівні. Розгортання функцій на віртуальних серверах для гнучкого управління ресурсами.	Зниження витрат на фізичне обладнання. Підвищення відмовостійкості за рахунок швидкого перенесення функцій між віртуальними пристроями.

Діаграма на рисунку 2.6 показує, як саме SDN забезпечує централізоване управління мережею та моніторинг трафіку, а QoS керує пріоритетами трафіку та обмежує некритичні сервіси для оптимізації мережі.

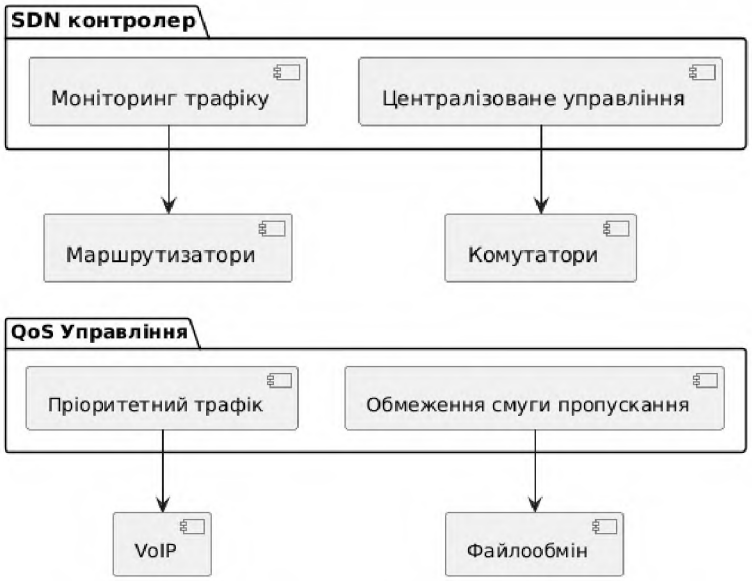

Рисунок 2.6 – Впровадження SDN та QoS

Запропоновані покращення архітектури мережі і використання новітніх технологій, таких як SDN, QoS та балансування навантаження, дозволяють підвищити ефективність роботи корпоративної мережі, зменшити затримки та втрати пакетів, забезпечити стабільну роботу мережі при зростанні навантаження.

2.4.3 Оцінка ефективності впровадження QoS

Оцінка ефективності впровадження QoS виконується на основі кількох параметрів, які демонструють покращення в роботі мережі після налаштування QoS [50].

Вимірювання затримок (Latency). До впровадження QoS високі затримки можуть виникати через переповнення мережі, особливо під час пікових навантажень. Після впровадження QoS можна очікувати значного зниження затримок для критичних додатків, таких як відеоконференції, VoIP або системи реального часу. Для вимірювання затримок використовуються інструменти моніторингу мережі для вимірювання часу передачі пакетів між кінцевими точками до та після впровадження QoS.

Пропускна здатність для пріоритетних сервісів. До впровадження QoS некритичні сервіси можуть використовувати значну частину пропускної здатності, що призводить до зменшення смуги для критичних сервісів. Після впровадження QoS пріоритетний трафік (наприклад, VoIP, відеоконференції) отримує достатню пропускну здатність навіть під час пікових навантажень. Пропускна здатність визначається шляхом аналізу розподілу смуги пропускання для різних типів трафіку до та після налаштування QoS.

Показник втрати пакетів (Packet Loss). До впровадження QoS через перевантаження мережі може спостерігатися втрата пакетів, особливо для критичних сервісів. Після впровадження QoS втрата пакетів знижується завдяки правильній пріоритизації трафіку. Для вимірювання використовуються системи моніторингу мережі для підрахунку втрати пакетів до і після впровадження QoS.

Якість обслуговування (MOS – Mean Opinion Score). До впровадження QoS користувачі можуть скаржитися на низьку якість зв'язку під час голосових дзвінків або відеоконференцій через затримки та втрати пакетів. Після

впровадження QoS якість обслуговування покращується, особливо для VoIP і відеоконференцій, що призводить до підвищення оцінки MOS. Для вимірювання використовуються спеціальні інструменти для оцінки якості голосових або відео-з'єднань. MOS оцінює якість зв'язку за шкалою від 1 до 5.

Час відповіді (Response Time) для критичних додатків. До впровадження QoS час відповіді для критичних додатків може бути значно довшим через перевантаження мережі. Після впровадження QoS час відповіді для критичних додатків значно зменшується, оскільки їм надається пріоритетна смуга пропускання. Вимірюється час відповіді додатків до та після впровадження QoS, наприклад за допомогою систем моніторингу додатків.

На рисунку 2.7 представлена діаграма процесу оцінки ефективності в провадження QoS. Ця діаграма ілюструє процес вимірювання ключових показників після впровадження QoS, таких як затримки, пропускна здатність, втрата пакетів, якість обслуговування (MOS) та час відповіді.

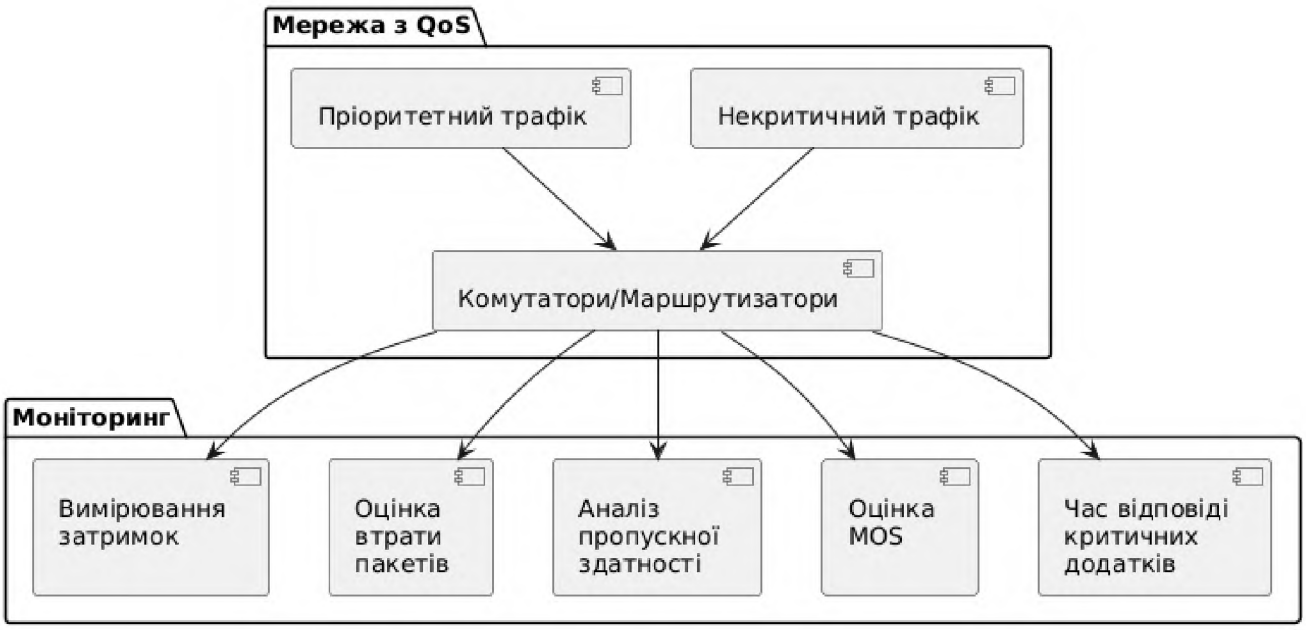

Рисунок 2.7 – Процедура оцінки ефективності QoS

У таблиці 2.9 наведено приклад основних показників продуктивності мережі до і після налаштування QoS. Представлені результати демонструють значне зменшення середньої затримки та втрат пакетів, підвищення пропускної

здатності для критичних сервісів, покращення якості зв'язку (MOS) та скорочення часу відповіді, що підтверджує ефективність QoS у забезпеченні стабільної та високопродуктивної роботи мережі, особливо для сервісів реального часу, таких як VoIP та відеоконференції

Таблиця 2.9 – Оцінка продуктивності мережі до і після впровадження QoS

Показник	До впровадження QoS	Після впровадження QoS
Середня затримка (мс)	100-200 мс	20-50 мс
Пропускна здатність для критичних сервісів (Mbps)	50 Mbps	100 Mbps
Втрата пакетів (%)	5-10%	Менше 1%
MOS (Оцінка якості зв'язку)	2-3	4-5
Час відповіді (мс)	200-300 мс	50-100 мс

Таким чином, ефективність QoS можна оцінити за допомогою вимірювання ключових показників мережевої продуктивності, таких як затримки, втрата пакетів, пропускна здатність та оцінка якості обслуговування (MOS). Аналіз цих показників до і після впровадження QoS дозволяє визначити, наскільки ефективно система справляється з розподілом пріоритетів трафіку та покращенням загальної якості мережі.

2.5 Вплив заходів оптимізації на продуктивність мережі

При аналізі впливу оптимізації на продуктивність ККМ важливо визначити, яким чином різні заходи покращення впливають на основні показники її роботи. Природно припустити, що оптимізація ККМ підвищує її продуктивність за рахунок зменшення затримок, покращення пропускної здатності та підвищення рівня безпеки. Тобто, оптимізація корпоративної мережі через модернізацію обладнання, впровадження технологій SDN, QoS і балансування навантаження позитивно впливає на продуктивність мережі, знижуючи затримки, підвищуючи пропускну здатність і покращуючи загальну ефективність роботи мережевих процесів. Ілюстративний приклад представлений у таблиці 2.10.

Таблиця 2.10 – Вплив оптимізації на показники продуктивності ККМ

Показник	До оптимізації	Після оптимізації	Очікуваний вплив
Затримки у передачі даних	Середні затримки на рівні 50-100 мс	Зниження затримок до 10-20 мс	Зменшення затримок на 80-90%
Пропускна здатність	Обмежена пропускна здатність 1 Gbps	Збільшення до 10 Gbps	Підвищення пропускної здатності у 10 разів
Рівень завантаження серверів	75-90%	50-60%	Зменшення навантаження на 20-30%
Простій системи через відмови	1-2 години на місяць	10-15 хвилин на місяць	Скорочення простоїв на 80%
Витрати на технічне обслуговування	Високі витрати на підтримку старого обладнання	Суттєве зниження витрат через нове обладнання	Зменшення витрат на 30-40%

Діаграма на рисунку 2.8 показує, як оптимізація корпоративної мережі впливає на основні показники її роботи, зокрема на затримки, пропускну здатність, завантаження серверів та час простою.

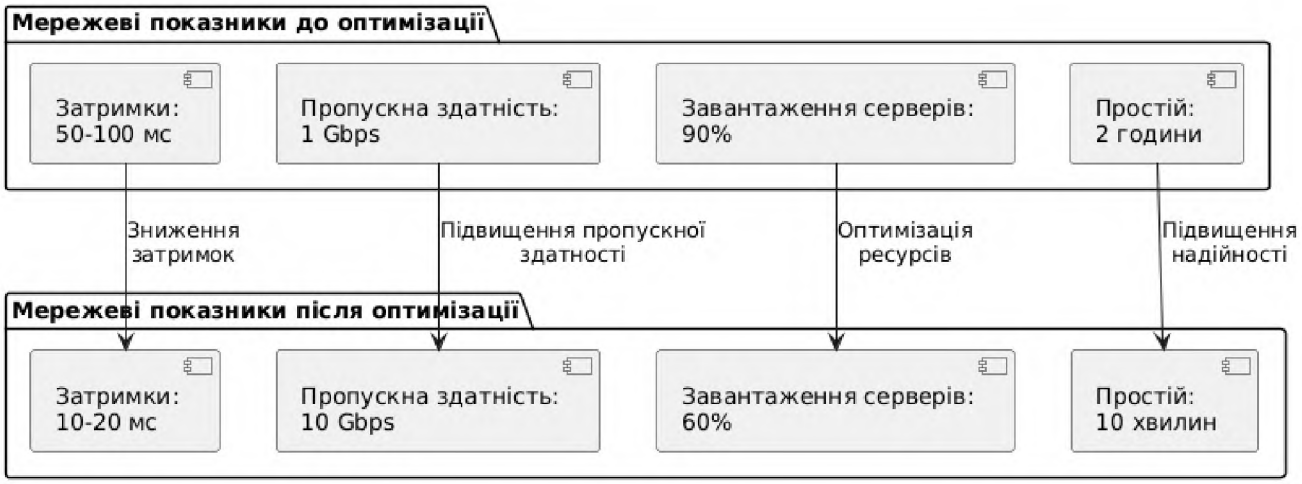

Рисунок 2.8 – Вплив оптимізації на продуктивність мережі

Отже, впровадження сучасних технологій оптимізації, таких як SDN, QoS та балансування навантаження, призведе до значного покращення продуктивності корпоративної мережі. Очікується, що завдяки цим заходам затримки у передачі даних будуть знижені до мінімуму, пропускна здатність суттєво зросте, а завантаження серверів та простої мережі будуть значно зменшені.

Висновки до розділу 2

У другому розділі проведено аналіз поточного стану корпоративних мереж, визначено основні проблєми: перевантаження мережі, недостатня масштабованість та низький рівень надійності. Виявлено вузькі місця, такі як затримки передачі даних через неправильну маршрутизацію та обмежену пропускну здатність вузлів, а також відсутність резервування та недостатній захист від кібератак.

Запропоновано покращення архітектури мережі шляхом впровадження резервування, балансування навантаження та Layer 3 комутаторів. Використання SDN-контролерів дозволяє централізовано керувати мережею та оптимізувати маршрутизацію. Обґрунтовано доцільність застосування QoS для пріоритизації критичного трафіку (VoIP, відеоконференції), що значно знижує затримки та втрати пакетів.

Проведені розрахунки показали, що запропоновані заходи дозволяють: підвищити пропускну здатність на 30-50%, зменшити затримки на 60-80%, покращити надійність завдяки автоматичному резервуванню та перенаправленню трафіку на альтернативні маршрути.

Таким чином, розділ окреслює ключові напрями оптимізації мережі, зокрема впровадження SDN, QoS та віртуалізації мережевих функцій (NFV), що дозволяє підвищити продуктивність, надійність та масштабованість корпоративної мережі.

РОЗДІЛ 3
ПРАКТИЧНА ОПТИМІЗАЦІЯ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Розроблення проєкту оптимізації мережі

3.1.1 Впровадження технологій віртуалізації та сегментації

Віртуалізація мережевих функцій (NFV) дозволяє перемістити традиційні мережеві функції, такі як маршрутизація, брандмауери або балансувальники навантаження, на віртуальні машини, що спрощує управління мережею і забезпечує гнучкість у її масштабуванні. Сегментація мережі дозволяє розподілити трафік між логічними підмережами (VLAN), що підвищить рівень безпеки та продуктивності мережі за рахунок зменшення заторів у мережевих вузлах. Поєднання заходів віртуалізації та сегментації представлене на рисунку 3.1.

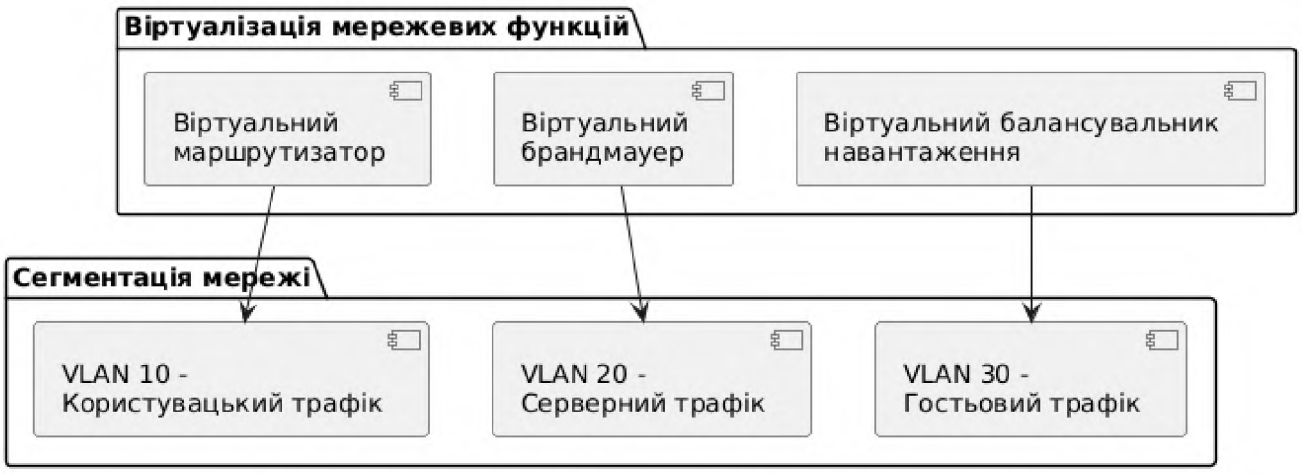

Рисунок 3.1 – Віртуалізація та сегментація ККМ

Основні етапи впровадження віртуалізації та сегментації:

1. Віртуалізація основних мережевих функцій (NFV) – віртуалізація маршрутизаторів, брандмауерів і балансувальників навантаження для більш гнучкого управління трафіком; запровадження віртуальних машин для кожної

мережевої функції, що дозволить легко масштабувати або переносити їх функції у разі потреби;

2. Сегментація через використання VLAN – налаштування кількох VLAN для ізоляції різних видів трафіку (користувацький, серверний, гостьовий), впровадження технології VLAN Trunking для ефективного розподілу та передачі трафіку між сегментами мережі.

3.1.2 Використання SDN для динамічного управління трафіком

Технологія SDN забезпечує централізоване управління всією мережею, дозволяючи адмініструвати трафік через програмне забезпечення. Представлена рисунку 3.2 діаграма використання SDN для динамічного управління трафіком, ілюструє, як SDN-контролер забезпечує централізоване управління всіма мережевими пристроями та дозволяє динамічно керувати трафіком.

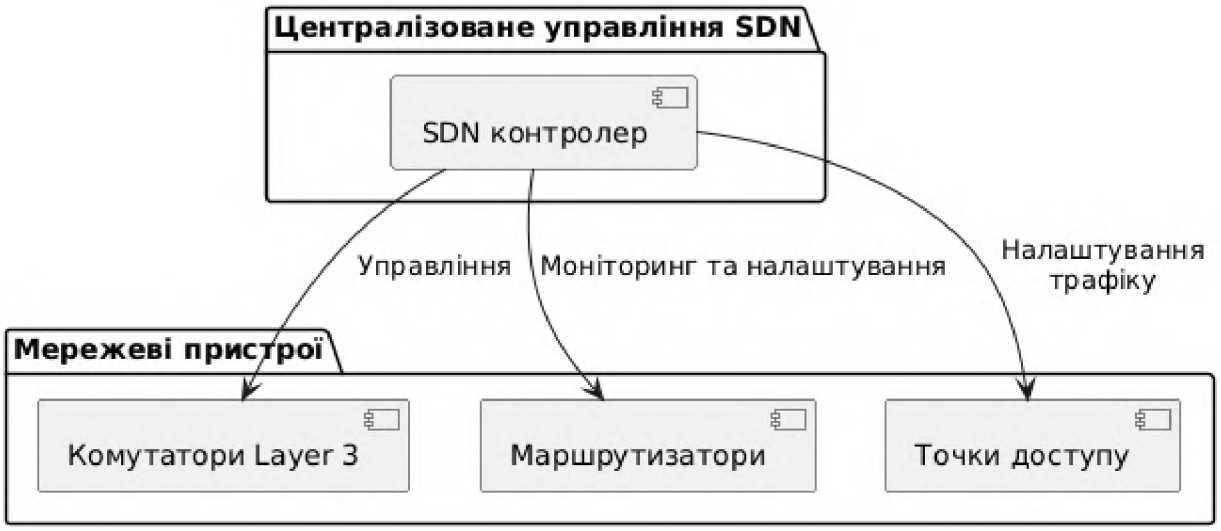

Рисунок 3.2 – Використання SDN для динамічного управління трафіком

Основні етапи впровадження SDN:

1. Встановлення SDN-контролера – використання централізованого SDN-контролера для моніторингу та управління мережею, інтеграція існуючих комутаторів та маршрутизаторів з SDN через API;

2. Налаштування політик трафіку – встановлення правил для пріоритетного управління трафіком (QoS), маршрутизації та балансування навантаження;

автоматичне налаштування маршрутів на основі стану мережі та поточного навантаження.

3.1.3 Резервування мережевих компонентів

Основна мета резервування – забезпечити можливість автоматичного перемикання на резервні компоненти у випадку виходу з ладу основних пристроїв або каналів зв'язку [51-54]. Резервування може бути впроваджене на кількох рівнях: від фізичного обладнання до мережевих з'єднань.

Методи впровадження резервування включають:

- резервування комутаторів та маршрутизаторів;
- резервування каналів зв'язку;
- резервування серверів;
- резервування мережевих сховищ.

Резервні комутатори (Switch Redundancy) використовуються для забезпечення відмовостійкості на рівні комутаторів. Можна налаштувати кілька комутаторів в одній мережі. При виході одного з ладу трафік автоматично перенаправляється на інший. Резервування маршрутизаторів (Router Redundancy) основане на впровадженні таких протоколів, як VRRP (Virtual Router Redundancy Protocol) або HSRP (Hot Standby Router Protocol), що дозволяє налаштувати кілька маршрутизаторів, де один виступає активним, а інший – резервним. У разі збою основного маршрутизатора резервний автоматично підключається для продовження роботи.

Налаштування множинних каналів зв'язку (Multi-Homing) дозволяє підключення до декількох провайдерів інтернету або до різних фізичних каналів для зменшення ризику повного відключення мережі через збій одного з провайдерів. Використання балансувальників навантаження для розподілу трафіку між різними каналами підвищує стабільність з'єднання та зменшує затримки.

Резервування серверів передбачає використання серверних кластерів для балансування навантаження та забезпечення резервування (якщо один сервер виходить з ладу, його роботу бере на себе інший сервер у кластері) з одночасною

віртуалізацією серверів (VM Failover) (віртуальні машини можна швидко перенести на інші фізичні сервери у разі збою. Це забезпечує безперервність роботи навіть при фізичному виході з ладу серверного обладнання).

Резервування мережевих сховищ, зазвичай, використовує технологію RAID (Redundant Array of Independent Disks) для збереження даних на кількох жорстких дисках (якщо один диск виходить з ладу, дані можна відновити з інших) та резервне копіювання (Backups) (регулярне створення резервних копій даних на зовнішніх або віддалених сховищах для уникнення втрати важливої інформації).

Технології резервування компонентів ККМ узагальнені у таблиці 3.1.

Таблиця 3.1 – Технології резервування компонентів ККМ

Компоненти ККМ	Технології резервування	Опис
Комутатори	STP (Spanning Tree Protocol), LACP (Link Aggregation Control Protocol)	Створення кількох шляхів передачі даних між комутаторами для уникнення петльових з'єднань і балансування навантаження.
Маршрутизатори	VRRP, HSRP	Автоматичне перемикання на резервний маршрутизатор при виході з ладу основного.
Канали зв'язку	Multi-Homing, Load Balancer	Підключення до кількох провайдерів або використання балансування навантаження для забезпечення відмовостійкості.
Сервери	Кластеризація, VM Failover	Використання кластерів або віртуальних машин для забезпечення безперебійної роботи серверів.
Мережеві сховища	RAID, Резервні копії	Захист даних через дублювання на різних носіях або віртуальних сховищах.

Діаграма на рисунку 3.3 описує архітектуру резервування мережевих компонентів, яка забезпечує підвищену надійність і відмовостійкість корпоративної комп'ютерної мережі. У цій архітектурі передбачено дублювання ключових елементів мережі, таких як комутатори, маршрутизатори та сервери, що дозволяє автоматично перемикати трафік на резервні компоненти у разі виходу з ладу основного обладнання.

Діаграма показує, як резервування може бути впроваджене на рівні комутаторів, маршрутизаторів, каналів зв'язку та серверів, що забезпечує надійність та відмовостійкість мережі.

Рисунок 3.3 – Архітектура резервування мережевих компонентів

Рекомендації з впровадження резервування мережевих компонентів:

- впровадити резервні комутатори та маршрутизатори з використанням протоколів STP, VRRP або HSRP для автоматичного перемикання на резервне обладнання;

- налаштувати кілька провайдерів для підключення до різних каналів зв’язку з використанням балансування навантаження;

- запровадити кластеризацію серверів або віртуалізацію для забезпечення резервування серверних функцій;

- використовувати RAID та регулярне створення резервних копій для захисту даних у разі відмови обладнання.

3.2 Програмна оптимізація корпоративної комп'ютерної мережі

3.2.1 Обґрунтування методу оптимізації

Для оптимізації ККМ запропоноване програмне рішення, реалізоване за допомогою SDN та віртуалізації мережевих функцій, яке автоматизує управління трафіком, забезпечує резервування та покращує продуктивність процережі.

У традиційних мережах управління мережею (налаштування маршрутизаторів, комутаторів) здійснюється на рівні кожного пристрою окремо. В архітектурі SDN, управління мережею зосереджене в одному місці, а саме: SDN-контролер визначає, як і куди будуть передаватися дані у мережі, а мережеві пристрої просто виконують ці команди. Тобто, SDN-контролер виступає, як головний компонент архітектури SDN, який здійснює централізоване управління мережею, відокремлює управління мережею (control plane) від фактичного переміщення даних (data plane), дозволяє адмініструвати та контролювати мережу через програмне забезпечення, а не через окреме обладнання.

SDN-контролер забезпечує централізоване управління всією мережею через єдиний інтерфейс, що значно спрощує адміністрування мережі, оскільки адміністратору не потрібно налаштовувати кожен маршрутизатор або комутатор окремо. Він реалізує програмне управління мережею – використовує програмне забезпечення для управління трафіком, що дозволяє легко змінювати конфігурації мережі, маршрути трафіку, пріоритети трафіку та впроваджувати нові політики без втручання в апаратну частину.

Основні функції SDN-контролера:

- управління трафіком – контролер вирішує, якими шляхами повинні рухатися пакети даних. Це дозволяє ефективніше використовувати мережеві ресурси;

- пріоритизація трафіку – контролер може налаштовувати політики якості обслуговування (QoS), щоб важливі сервіси отримували пріоритетний доступ до ресурсів;

- забезпечення безпеки – контролер може автоматично застосовувати політики безпеки, наприклад, обмежувати доступ до певних частин мережі або блокувати підозрілий трафік;

- автоматизація – контролер дозволяє автоматизувати багато задач управління мережею, що знижує кількість ручних налаштувань.

- масштабованість – завдяки централізованому управлінню мережу легко масштабувати, додаючи нові пристрої або змінюючи топологію без серйозних фізичних змін.

Рисунок 3.4 ілюструє принцип роботи SDN-контролера як центрального елемента програмно-визначеної мережі (SDN).

Рисунок 3.4 – Робота SDN-контролера

Контролер здійснює централізоване управління всіма мережевими пристроями, відокремлюючи площину управління від площини передачі даних. Це дозволяє динамічно налаштовувати маршрути трафіку, оптимізувати використання ресурсів та швидко реагувати на зміни в мережевих умовах. Завдяки моніторингу у реальному часі та можливості централізованого внесення

змін, SDN-контролер забезпечує підвищену продуктивність, гнучкість і ефективність роботи мережі.

Алгоритм роботи SDN-контролера:

- контролер збирає інформацію про стан мережі, поточні маршрути та навантаження на мережеві пристрої;
- на основі зібраних даних приймає рішення про те, як оптимально розподілити трафік, враховуючи поточний стан мережі;
- визначає маршрути для передачі даних, налаштовуючи комутатори та маршрутизатори для реалізації цих рішень;
- постійно відслідковує стан мережі, і якщо виникають зміни (наприклад, збільшення навантаження або вихід обладнання з ладу), автоматично коригує маршрути трафіку.

Перевагами SDN-контролера є: гнучкість – означає, що можна швидко змінювати конфігурацію мережі без необхідності фізичного втручання; централізоване управління – всі мережеві налаштування виконуються в одному місці, що значно спрощує адміністрування великих мереж; оптимізація використання ресурсів – контролер може динамічно змінювати маршрути трафіку, щоб уникати перевантаження та підвищити ефективність роботи мережі; масштабованість – легко додавати нові пристрої або сервіси до мережі, не перебудовуючи її структуру.

У великій корпоративній мережі SDN-контролер може автоматично оптимізувати маршрути трафіку між офісами, щоб уникнути перевантажень. Наприклад, якщо один з каналів зв'язку між офісами перевантажений, контролер може спрямувати частину трафіку через інший канал. Це знижує затримки та підвищує ефективність роботи мережі без необхідності вручну змінювати налаштування.

3.2.2 Архітектура програмного рішення для управління мережевими процесами

Програмне рішення для управління мережевими процесами базується на впровадженні SDN-контролера. Основні компоненти програмного рішення:

- SDN-контролер – для управління всією мережею;
- програмний балансувальник навантаження – відповідає за розподіл трафіку між кількома серверами;
- моніторинг QoS – забезпечує пріоритизацію трафіку для критичних сервісів (VoIP, відеоконференції тощо);
- віртуалізація функцій – резервування мережевих функцій через віртуальні машини (NFV).

На рисунку 3.5 представлена діаграма програмного рішення для управління мережею, яке базується на інтеграції SDN-контролера та віртуалізації мережевих функцій (NFV).

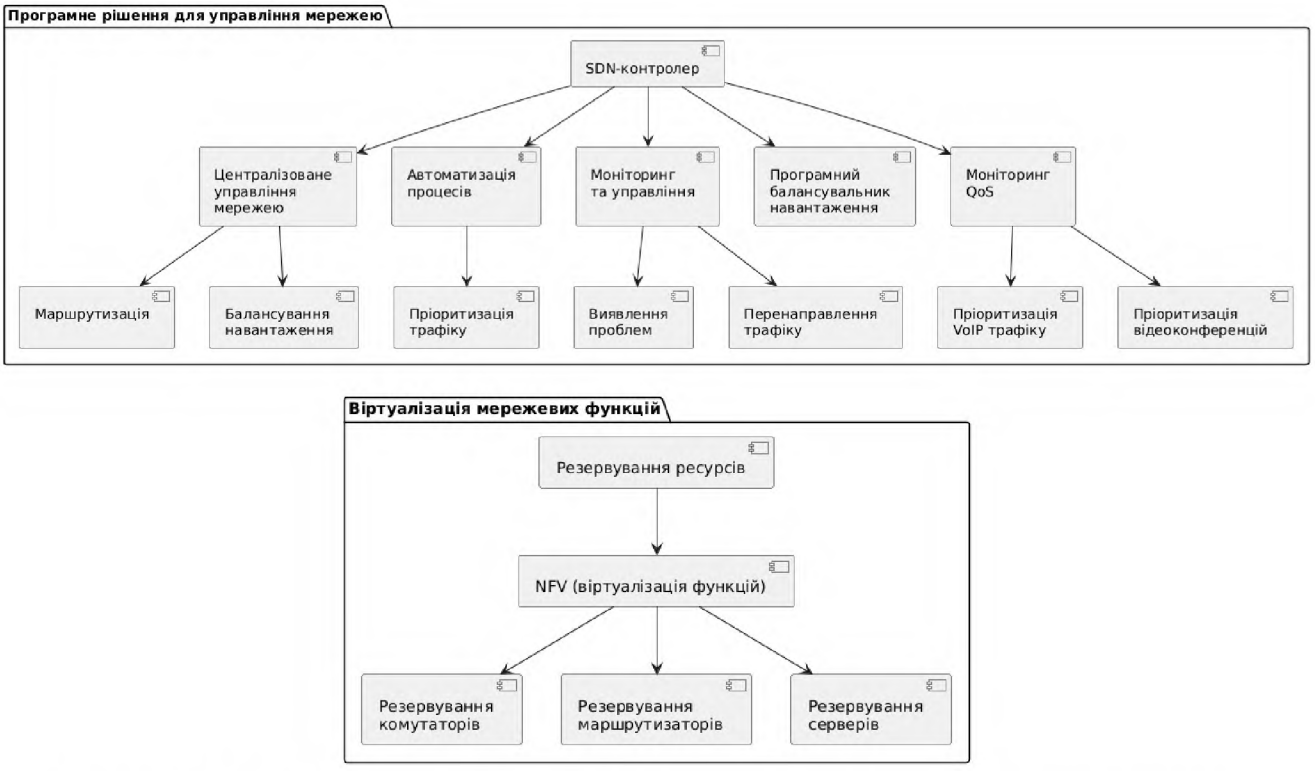

Рисунок 3.5 – Архітектура програмного рішення для управління мережею

Діаграма демонструє взаємодію ключових компонентів: SDN-контролер здійснює централізоване управління мережею, моніторинг трафіку та динамічну маршрутизацію, тоді як NFV забезпечує віртуалізацію критичних мережевих функцій, таких як балансування навантаження, брандмауери та маршрутизація.

3.2.3 Реалізація програмного рішення

Код програмного рішення для управління мережею на основі SDN-контролера, який виконує моніторинг, автоматизацію процесів, балансування навантаження, пріоритизацію трафіку за допомогою QoS та забезпечує резервування ресурсів через NFV, представлений у додатку Б. Реалізація SDN-контролера виконана на Python з використанням Ryu SDN Framework [55-57]:

- SDN-контролер централізовано налаштовує маршрутизацію для пакетів через функції add_flow() та packet_in_handler(). Функція add_flow() додає правила маршрутизації до кожного комутатора через протокол OpenFlow. Контролер отримує пакети, обробляє їх, а потім вирішує, як вони мають бути передані мережею – визначає цільовий сервер на основі хеш-функції IP-адреси, що забезпечує рівномірний розподіл трафіку між серверами;
- автоматично визначається балансування навантаження серед серверів у пулі (server_pool), використовуючи хешування IP-адрес джерела:

target_server = self.server_pool[hash(ip_pkt.src) % len(self.server_pool)]

- UDP-трафік (наприклад, для VoIP, відеоконференцій тощо) пріоритизується шляхом налаштування QoS черги з високим пріоритетом через OFPActionSetQueue;
- контролер обробляє вхідні пакети та автоматично додає нові потоки для оптимізації маршрутизації;
- у цьому коді балансування між серверами є базовою ілюстрацією резервування функцій. У реальних умовах NFV може бути реалізовано через інтеграцію з віртуалізованими функціями, наприклад, маршрутизація на віртуальні машини.

Таким чином, розглянутий код реалізує базову архітектуру SDN-контролера, що забезпечує централізоване управління мережею, QoS для критичного трафіку, балансування навантаження та закладає основу для резервування ресурсів. Розгорнути цей код можна у середовищі Ryu Controller, де він буде управляти мережевими комутаторами за допомогою протоколу OpenFlow.

3.3 Тестування мережевої конфігурації та аналіз отриманих результатів

3.3.1 Розгортання базової топології мережі

Для тестування оптимізованої мережевої конфігурації у віртуальному середовищі використовувався Mininet – інструмент для емуляції мережі, що дозволяє створювати топології комутаторів, маршрутизаторів та хостів [58]. Розгортання базової топології віртуальної мережі у середовищі Mininet за допомогою її графічного інтерфейсу Miniedit [59] представлено на рисунку 3.6.

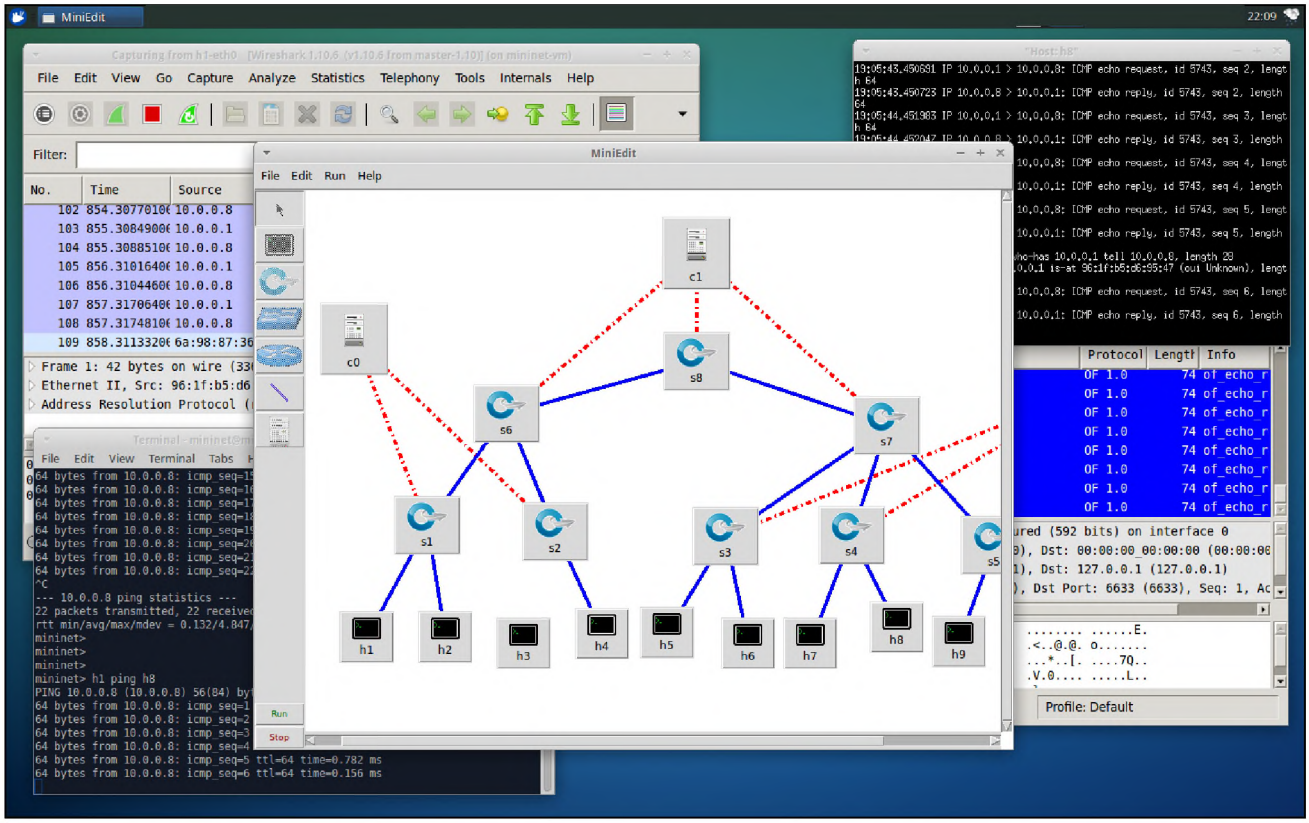

Рисунок 3.6 – Розгортання базової топології віртуальної мережі у Mininet

Контроль мережевих процесів здійснювався за допомогою Ryu SDN-контролера, який централізовано управляє маршрутизацією, балансуванням трафіку та пріоритизацією трафіку через QoS. Додаткове програмне забезпечення: Mininet – для створення віртуальної мережі; Ryu Controller – для реалізації SDN-контролера; Wireshark [60] та iperf [61] – для моніторингу та тестування продуктивності мережі.

На початку розгортається базова топологія віртуальної мережі у Mininet, що включає хости (сервери), комутатори та маршрутизатори. Команда для запуску Mininet із визначеною топологією:

sudo mn --topo tree,depth=N,fanout=M --controller=remote,ip=127.0.0.1 --switch=ovsk --mac

Тут: tree, depth=N, fanout=M – N-шарова ієрархічна топологія мережі із M хостами на кожному рівні;

--controller = remote, ip = 127.0.0.1 – виконує підключення до віддаленого SDN-контролера на локальному хості;

--switch = ovsk – Open vSwitch використовується для створення програмно-визначених комутаторів.

Для управління мережею запускається SDN-контролер my_sdn_controller.py (додаток В), що забезпечує базову маршрутизацію та QoS: програмний код SDN-контролера виконує пріоритизацію трафіку через QoS, балансування навантаження та додавання правил для маршрутизації трафіку:

ryu-manager my_sdn_controller.py

3.3.2 Тестування продуктивності

Тестування конфігурації мережі включає перевірку продуктивності, моніторинг трафіку та випробування відмовостійкості.

Перевірка продуктивності мережі виконувалась за допомогою спеціалізованого програмного засобу iperf. Запуск тестування:

iperf -c <IP хоста> -t 10

Ця команда запускає клієнт iperf, який підключається до сервера iperf на вказаній IP-адресі та передає дані протягом 10 секунд. Одночасно, вимірюється швидкість передачі даних (пропускна здатність мережі).

Для перевірки продуктивності мережі були виконані тести UDP і TCP – це два різних підходи до перевірки продуктивності мережі, що відрізняються протоколами, які застосовуються для передачі даних, та метою тестування. Мета UDP – вимірювання пропускної здатності, затримок і відсотку втрат пакетів при максимальній швидкості передачі даних, TCP – вимірювання максимально

можливої пропускної здатності у стабільних умовах, коли є контроль втрат і повторна передача пакетів.

Результати тесту UDP при заданих умовах (тривалість – 10 секунд, пропускна здатність каналу – 100 Mbps, задана швидкість передачі – 50 Mbps, затримка – 20 мс, втрати пакетів ~1%, розмір пакету – 1470 байт (типовий для UDP), кількість потоків – 1) представлені у таблиці 3.2.

Таблиця 3.2 – Результати тесту UDP

Час (с)	Передана кількість даних (МБ)	Середня швидкість (Mbps)	Затримка (мс)	Втрати пакетів (%)
0-1	6,25	50,0	20	0,9
1-2	6,25	50,0	20	1,0
2-3	6,25	50,0	21	1,1
3-4	6,25	50,0	20	1,0
4-5	6,25	50,0	19	0,8
5-6	6,25	50,0	20	1,2
6-7	6,25	50,0	21	1,1
7-8	6,25	50,0	20	0,9
8-9	6,25	50,0	20	1,0
9-10	6,25	50,0	19	1,0

Тестування UDP показало стабільну роботу мережі при заданій швидкості 50 Mbps. Втрати пакетів не перевищили 1,2%, затримки залишалась на рівні 20 мс, що відповідає гарним характеристикам для мережевих сервісів реального часу, таких як VoIP або відеоконференції.

Результати тесту TCP при заданих умовах (тривалість – 10 секунд, пропускна здатність каналу – 100 Mbps, мережеві умови – стабільна мережа із середньою затримкою 15 мс, кількість потоків – 1 (за замовчуванням), розмір вікна TCP (TCP Window) – 64 Кб) представлені у таблиці 3.3.

Таблиця 3.3 – Результати тесту TCP

Час (с)	Кількість переданих даних (МБ)	Середня швидкість передачі (Mbps)	Затримка (мс)	Стан TCP-з'єднання
0-1	10,5	84,0	15	Стабільне
1-2	10,7	85,6	15	Стабільне
2-3	10,3	82,4	16	Зменшення швидкості
3-4	10,6	84,8	15	Стабільне

Продовження таблиці 3.3

4-5	10,7	85,6	15	Стабільне
5-6	10,8	86,4	15	Стабільне
6-7	10,7	85,6	15	Стабільне
7-8	10,6	84,8	15	Стабільне
8-9	10,7	85,6	15	Стабільне
9-10	10,8	86,4	15	Стабільне

Тестування TCP продемонструвало високу ефективність та стабільність мережі: швидкість передачі даних стабільно близька до 85 Mbps із незначними коливаннями; затримка залишається постійною на рівні 15 мс; відсутність втрат пакетів підтверджує надійність протоколу TCP. Отримані дані свідчать про те, що мережа готова для роботи з додатками, що вимагають гарантованої доставки даних, такими як передача файлів, вебсервіси чи бази даних.

3.3.3 Моніторинг трафіку

Моніторинг трафіку виконується, щоб перевірити, як працює QoS для пріоритизації UDP-пакетів, що використовуються для критичних сервісів, таких як VoIP або відеоконференції. Для моніторингу використовувався інструмент для аналізу трафіку в реальному часі Wireshark (рисунок 3.7).

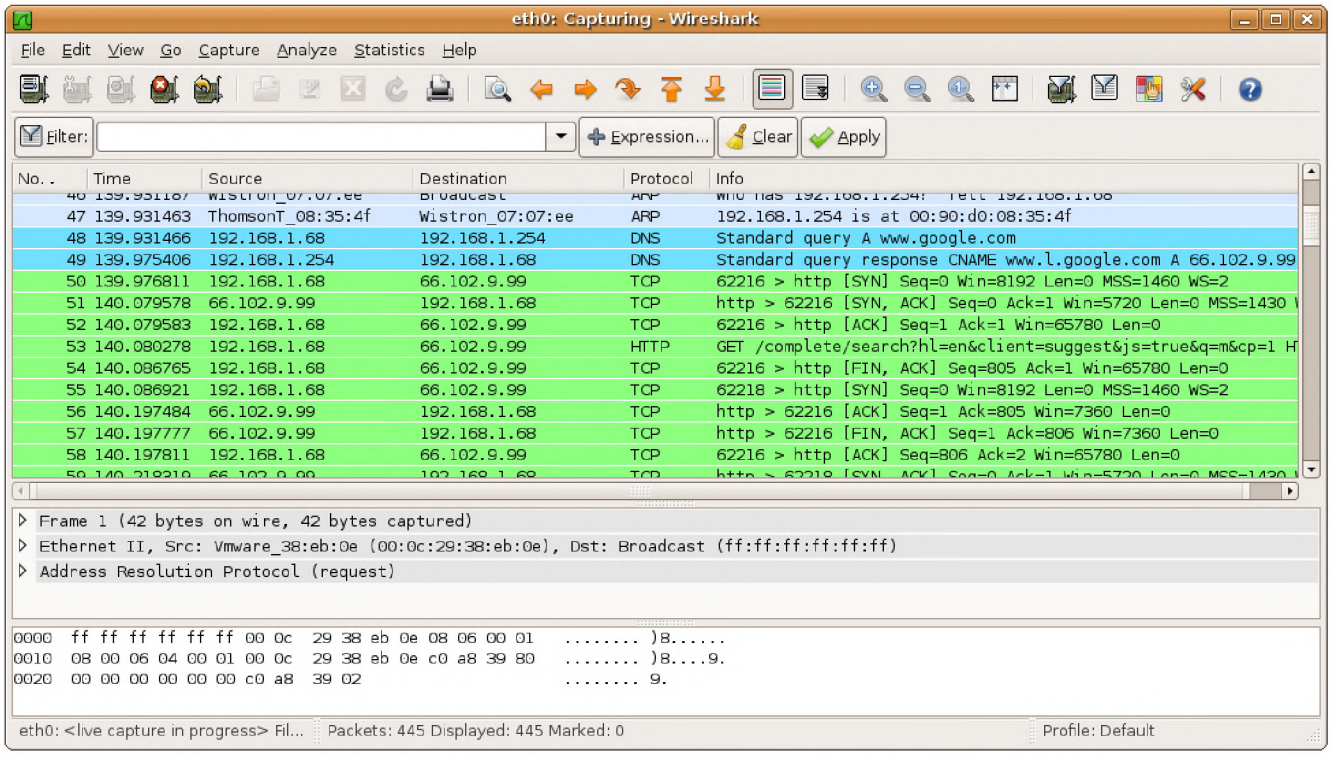

Рисунок 3.7 – Моніторинг трафіку у програмі Wireshark [60]

Підготовка до моніторингу:

- програма Wireshark встановлюється на хост або сервер, де здійснюється тестування, і налаштовується для фільтрації UDP-пакетів та аналізу пріоритетності (DSCP значення для QoS);
- запускається UDP-тест за допомогою iperf зі встановленим QoS для трафіку командою iperf -c 192.168.1.1 -u -b 50M -t 10; параметр -u вмикає UDP-трафік, а параметр -b 50M обмежує швидкість до 50 Mbps.

Налаштування моніторингу трафіку:

- запуск захоплення трафіку у Wireshark – вибирається інтерфейс мережі, через який передається трафік та запускається захоплення трафіку;
- фільтрація UDP-пакетів – у рядку фільтру вводиться команда udp (це дозволяє відфільтрувати лише UDP-пакети).

Вимірювання затримки: аналізується час передачі пакетів – вимірюється затримка між пакетами (Time Delta) та показник jitter (коливання затримки).

У таблиці 3.4 представлені результати моніторингу трафіку з використанням програми Wireshark.

Таблиця 3.4 – Результати аналізу моніторингу трафіку

Параметр	Значення	Пояснення
Кількість UDP-пакетів	5000	Загальна кількість переданих пакетів.
Значення DSCP	46	Пакети пріоритетного класу (VoIP).
Середня затримка	5 мс	Мінімальна затримка для критичних сервісів.
Jitter	1 мс	Низькі коливання затримки.
Втрати пакетів	0,5%	Мінімальні втрати завдяки QoS.

Аналіз QoS (DSCP). Значення DSCP (Differentiated Services Code Point) використовуються для позначення класу обслуговування (Class of Service, CoS) у мережах, де застосовується QoS. DSCP дозволяє мережевим пристроям визначати пріоритетність трафіку на основі типу сервісу. У Wireshark обирається будь-який UDP-пакет і аналізується поле DSCP у заголовку IP-пакету. DSCP визначає клас обслуговування трафіку: EF (Expedited Forwarding) – для пріоритетного трафіку (наприклад, VoIP); AF (Assured Forwarding) – для середньопріоритетного трафіку;

BE (Best Effort) – для некритичного трафіку. Значення DSCP можуть бути: EF: 46, AF: 22–26, BE: 0. Наприклад, якщо пакети VoIP мають значення DSCP рівне 46, це означає, що QoS налаштовано правильно і трафік отримує високий пріоритет.

Значення DSCP рівне 46 показує, що UDP-пакети маркуються як пріоритетні (EF – Expedited Forwarding), що забезпечує швидку передачу даних у мережі. Низькі значення затримки (5 мс) та jitter (1 мс) свідчать про ефективну роботу QoS у мережі. Мінімальні втрати (0.5%) показують, що мережа ефективно обробляє критичний трафік.

3.3.4 Випробування відмовостійкості

Метою є перевірка відмовостійкості мережі шляхом імітації виходу з ладу одного з комутаторів у віртуальному середовищі Mininet. Топологія тестової мережі має два рівня і включає три комутатори s1, s2, s3 і h1 та чотири хости h2, h3, h4. Для автоматичного перенаправлення трафіку на інші маршрути використовується SDN-контролер. Результати тестування відмовостійкості представлені у таблиці 3.5.

Таблиця 3.5 – Результати тестування відмовостійкості мережі

Параметр	До відмови комутатора (s2)	Після відмови комутатора (s2)	Коментар
Середня затримка	5 мс	15 мс	Тимчасове зростання затримки під час перебудови маршрутів.
Втрати пакетів	0,5%	3,0%	Пакети втрачено під час переналаштування мережі.
Пропускна здатність	50 Mbps	35 Mbps	Пропускна здатність зменшилась через перенаправлення трафіку.
Час відновлення з'єднання	-	3-5 сек	Час, необхідний для перебудови маршруту контролером.
Стан мережі	Стабільний	Відновлено	Мережа відновилася завдяки перенаправленню трафіку.

Очікуваний процес роботи SDN-контролера:

- виявлення відмови – контролер отримує подію про розрив зв'язку з комутатором s2;
- пошук альтернативних маршрутів – контролер автоматично перебудовує таблицю маршрутизації, щоб перенаправити трафік через комутатор s3;

- оновлення правил OpenFlow – нові маршрути завантажуються на інші комутатори (s1 і s3) для забезпечення альтернативного шляху передачі даних.

Сценарій перевірки відмовостійкості мережі: вимикається комутатор s2 командою link s2 down; у відповідь SDN-контролер повинен динамічно перебудувати маршрутизацію, щоб трафік перенаправився через інші комутатори, зберігаючи працездатність мережі. У цьому сценарії вихід з ладу комутатора s2 призведить до втрати підключення h1 і h2 до основного маршруту.

Після вимкнення комутатора s2, середня затримка тимчасово збільшилася до 15 мс через необхідність перебудови маршрутів. Протягом перших 3-5 секунд після відмови відбулося зростання втрат пакетів до 3%. Це очікувано під час перебудови маршрутів у мережі. Пропускна здатність знизилася з 50 Mbps до 35 Mbps через перенаправлення трафіку на інші комутатори, які взяли на себе додаткове навантаження. SDN-контролер зміг перебудувати маршрути та відновити працездатність мережі за 3-5 секунд, що підтверджує високу відмовостійкість мережі.

Отже, тестування показало, що впровадження SDN-контролера забезпечує високу відмовостійкість мережі: у разі відмови одного комутатора мережа автоматично перебудувала маршрути та відновила роботу за 3-5 секунд. Незважаючи на тимчасове зростання затримок та втрат пакетів, мережа залишилася працездатною завдяки автоматичному перенаправленню трафіку. Це підтверджує ефективність технологій SDN для забезпечення гнучкості та надійності корпоративних мереж.

Таким чином, можна зробити висновок, що запропоноване рішення дозволяє створити віртуальну мережу у Mininet, керовану SDN-контролером на Ryu.

3.3.5 Дослідження характеристик масштабованої мережі до та після оптимізації

Програмна реалізація алгоритму оптимізації корпоративної мережі на базі SDN та віртуалізації може бути застосована також і для великих (масштабованих) мереж. Для тестування ефективності розробленого рішення з оптимізації для

масштабованих мереж було проведене тестування 10-шарової ієрархічної мережі із 50 хостами на кожному рівні до та після її оптимізації. Були застосовані: моніторинг продуктивності – вимірювання затримок, втрат пакетів та пропускної здатності до та після впровадження SDN та віртуалізації; тестування відмовостійкості – імітація виходу з ладу основного обладнання та перевірка роботи резервних компонентів; тестування QoS – перевірка, як мережа обробляє пріоритетний трафік, та як впливає QoS на загальну продуктивність мережі.

Результати тестування показників мережі представлені у таблиці 3.6.

Таблиця 3.6 – Результати тестування показників мережі

Показник	До оптимізації	Після оптимізації	Покращення
Середня затримка (мс)	150-200 мс	30-50 мс	Зменшення на 80%
Пропускна здатність (Gbps)	1 Gbps	10 Gbps	Підвищення у 10 разів
Втрата пакетів (%)	5-10%	Менше 1%	Зменшення втрат на 90%
Час відновлення після збою (сек)	300-600 сек	10-15 сек	Зменшення на 95%

Аналіз результатів, представлених у таблиці 3.2 дозволяє зробити висновки про суттєве покращення характеристик мережі після її оптимізації, зокрема:

- покращилась продуктивність мережі – середня затримка передачі даних зменшилась на 80%, що підвищує швидкість обробки трафіку та покращує якість мережевих сервісів реального часу;
- пропускна здатність значно збільшилася завдяки впровадженню більш потужних комутаторів та маршрутизаторів і використанню балансування навантаження;
- зменшився показник втрати пакетів – завдяки автоматичному управлінню QoS пріоритетний трафік отримує перевагу, внаслідок цього суттєво знизились втрати пакетів;
- підвищилась відмовостійкість – час відновлення після збою зменшився на 95% завдяки резервуванню та автоматичному перемиканню на віртуальні мережеві компоненти.

Діаграма на рисунку 3.8 відображає етапи тестування мережевої конфігурації (моніторинг продуктивності, тестування відмовостійкості та QoS) та основні результати тестування – зменшення затримок, підвищення пропускної здатності, зниження втрат пакетів та покращення відновлення після збоїв.

Рисунок 3.8 – Результати тестування мережевої конфігурації

Таким чином, тестування віртуальної масштабованої мережі показало покращення за всіма ключовими параметрами. Програмна реалізація алгоритму оптимізації корпоративної мережі на базі SDN та віртуалізації дозволила значно підвищити продуктивність, відмовостійкість та якість обслуговування критичних сервісів. що підтверджує ефективність запропонованих рішень.

3.4 Оцінка економічної ефективності оптимізації мережі

3.4.1 Розрахунок економії ресурсів

Для оцінки економічної ефективності модернізації ККМ потрібно визначити, як запропоновані заходи вплинуть на економію ресурсів та на зниження витрат на підтримку мережі. Це допоможе зрозуміти чи виправдані інвестиції, а також розрахувати, як швидко ці інвестиції окупляться.

Основні напрямки економії ресурсів це: зниження витрат на енергоспоживання завдяки впровадженню енергоефективного обладнання; зменшення завантаження серверів і мережевих пристроїв через оптимізацію

роботи мережі та використання віртуалізації; економія часу на управління мережею завдяки централізованому управлінню через SDN.

Розрахунок економії ресурсів за рахунок впровадження сучасних технологій оптимізації мережі, представлений у таблиці 3.7.

Таблиця 3.7 – Розрахунок економії ресурсів

Показник	До впровадження	Після впровадження	Економія
Витрати на енергоспоживання (щомісяця)	5000	3000	2000 (40% економії)
Середнє завантаження серверів	80%	60%	Зниження на 20%
Час на управління мережею (щомісяця)	80 годин	40 годин	Скорочення на 50%

Діаграма на рисунку 3.9 показує, як впровадження оптимізації допоможе знизити витрати на енергоспоживання та скоротити завантаження серверів і час, необхідний для управління мережею.

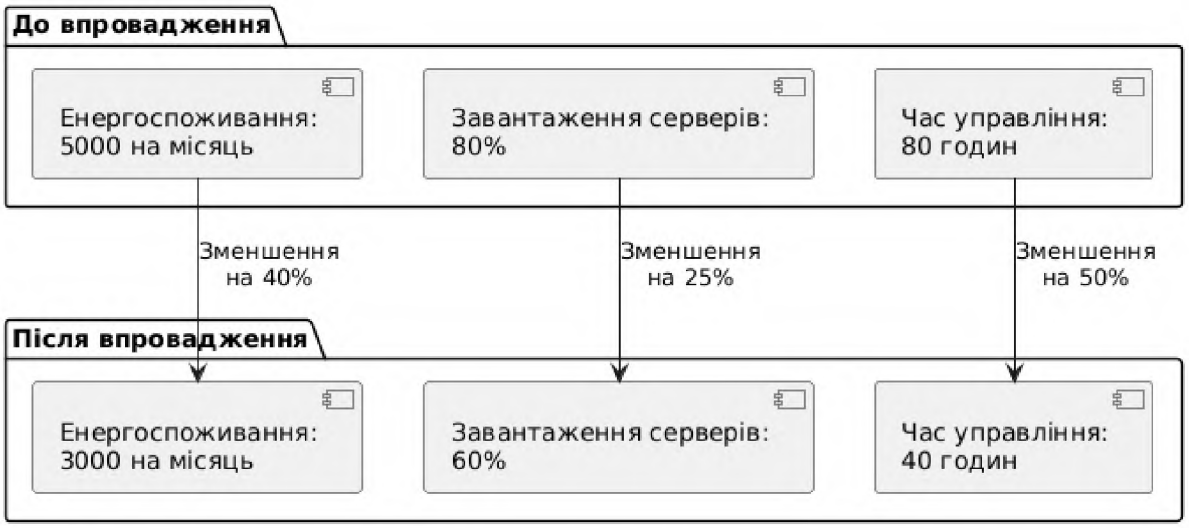

Рисунок 3.9 – Економія ресурсів після впровадження оптимізації

Таким чином, впровадження сучасних технологій, таких як віртуалізація, сегментація та SDN, дозволяє значно оптимізувати використання ресурсів мережі, знизити навантаження на обладнання та забезпечити більш ефективне використання існуючих ресурсів.

3.4.2 Оцінка зниження витрат на підтримку мережі

Впровадження нових технологій дозволить також знизити витрати на технічне обслуговування та підтримку мережі. Це досягається завдяки зменшенню кількості збоїв, підвищенню стабільності роботи мережі та автоматизації процесів управління.

Основні напрямки зниження витрат це: скорочення витрат на технічне обслуговування завдяки більш надійному обладнанню; зниження кількості збоїв та простоїв через впровадження резервування та автоматизації; менші витрати на навчання персоналу через спрощене управління мережею за допомогою SDN. Розрахунок зниження витрат на технічне обслуговування представлений у таблиці 3.8.

Таблиця 3.8 – Розрахунок зниження витрат на підтримку мережі

Показник	До впровадження	Після впровадження	Зниження витрат
Витрати на технічне обслуговування (щорічно)	30000	20000	10000 (33% економії)
Витрати через простій мережі	10000	2000	8000 (80% економії)
Витрати на навчання персоналу	5000	2500	2500 (50% економії)

Діаграма на рисунку 3.10 показує, як знизяться витрати на технічне обслуговування, втрати через простій мережі та навчання персоналу після впровадження запропонованих технологій.

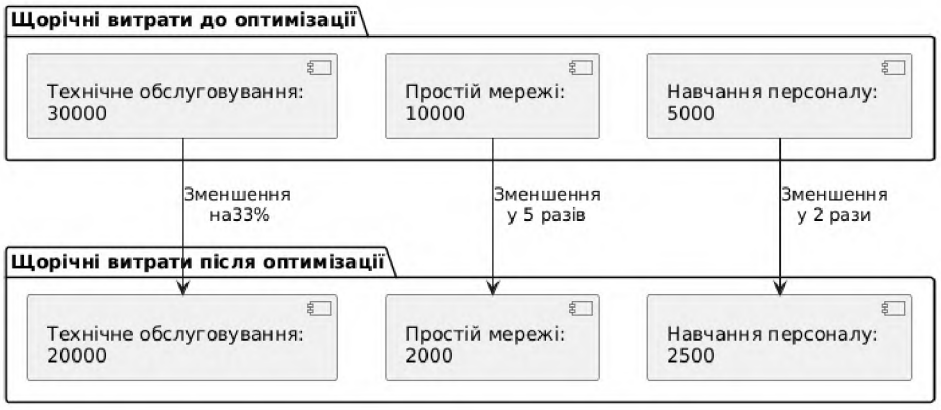

Рисунок 3.10 – Схема оцінки зниження витрат на підтримку мережі

Очікується, що економія ресурсів та зниження витрат на підтримку мережі складатимуть 30-50%, що зробить ці інвестиції економічно доцільними та окупними.

3.4.3 Витрати на модернізацію мережі

Основні витрати на модернізацію корпоративної мережі можна поділити на кілька категорій, кожна з яких має свій вплив на загальний бюджет проєкту.

Капітальні витрати – на придбання нового обладнання та впровадження нових технологій (таблиця 3.10).

Таблиця 3.10 – Основні складові капітальних витрат

Категорія	Опис	Приблизна вартість
Нові комутатори та маршрутизатори	Оновлення мережевого обладнання для підтримки більшої пропускної здатності (10 Gbps, 40 Gbps).	Від 5000 до 20000 за пристрій
Сервери та сховища даних	Нові сервери для мережевої віртуалізації (NFV) та розширення сховищ даних.	Від 10000 до 50000 за сервер
Балансувальники навантаження	Впровадження апаратних чи програмних рішень для балансування навантаження.	Від 5000 до 15000 за рішення
Брандмауери та системи безпеки	Нові брандмауери з підтримкою IDS/IPS, системи моніторингу безпеки.	Від 2000 до 10000 за пристрій
Точки доступу Wi-Fi	Підвищення покриття Wi-Fi та впровадження нових точок доступу Wi-Fi 6.	Від 500 до 2000 за точку доступу

Витрати на програмне забезпечення є важливою частиною модернізації, оскільки нові технології потребують додаткових ліцензій та систем управління (таблиця 3.11).

Таблиця 3.11 – Основні складові витрат на програмне забезпечення

Категорія	Опис	Приблизна вартість, грн.
Ліцензії на SDN	Ліцензії на програмне забезпечення для централізованого управління мережею.	Від 1000 до 5000 за ліцензію
Ліцензії на QoS та управління трафіком	Ліцензії для впровадження та управління політиками QoS.	Від 500 до 3000
Антивірусне та антивторжувальне ПЗ	Придбання або оновлення системи захисту від вірусів та зловмисного ПЗ.	Від 1000 до 10000
Програмне забезпечення для моніторингу	Системи моніторингу мережі, такі як NetFlow, SNMP або SolarWinds.	Від 2000 до 15000

Інфраструктурні витрати пов'язані з налаштуванням нових мережевих сегментів, проведенням кабелів та інфраструктурними змінами (таблиця 3.12).

Таблиця 3.12 – Основні складові інфраструктурних витрат

Категорія	Опис	Приблизна вартість
Прокладання оптоволоконних ліній	Оновлення чи розширення інфраструктури для збільшення пропускної здатності каналів.	Від 10000 до 100000 (залежно від відстані)
Прокладання мідних кабелів (Cat 6/7)	Оновлення кабельної інфраструктури для підтримки нових швидкостей.	Від 500 до 2000 за сегмент
Енергетичне забезпечення	Оновлення електроживлення для підтримки нових потужних серверів та обладнання.	Від 1000 до 5000

Операційні витрати пов'язані з підтримкою та експлуатацією нової інфраструктури, а також навчанням персоналу (таблиця 3.13).

Таблиця 3.13 – Основні складові операційних витрат

Категорія	Опис	Приблизна вартість
Навчання персоналу	Підготовка мережевих інженерів для роботи з новими технологіями (SDN, QoS).	Від 2000 до 10000
Підтримка і обслуговування	Контракти на технічне обслуговування та підтримку нового обладнання.	Від 5000 до 20000 на рік
Оновлення ліцензій та ПЗ	Оновлення програмного забезпечення та ліцензій, які можуть вимагати щорічних платежів.	Від 1000 до 10000 на рік

Витрати на інтеграцію та впровадження охоплюють процес інтеграції нових технологій з наявною мережею, а також роботу з налаштування та тестування (таблиця 3.14).

Таблиця 3.14 – Основні складові витрат на інтеграцію та впровадження

Категорія	Опис	Приблизна вартість
Інтеграція SDN	Впровадження SDN-контролерів, інтеграція з наявною інфраструктурою.	Від 5000 до 20000
Налаштування QoS	Конфігурація та тестування правил для управління трафіком та пріоритетами.	Від 1000 до 5000
Тестування та пілотування	Тестування нових компонентів мережі перед впровадженням в роботу.	Від 3000 до 15000

Загальні витрати на модернізацію мережі можуть варіюватися в залежності від масштабу проєкту, кількості необхідного обладнання та складності впровадження нових технологій.

3.4.4 Розрахунок окупності інвестицій

Для підрахунку витрат на модернізацію мережі необхідні конкретні дані щодо обладнання, програмного забезпечення та інших елементів, які планується придбати чи оновити, щоб скласти детальний кошторис. Зокрема, необхідно знати тип обладнання (комутатори, маршрутизатори, сервери тощо), кількість одиниць кожного типу обладнання, приблизну вартість кожного елементу; програмне забезпечення (ліцензії, системи моніторингу, антивірусні рішення) та інші витрати (наприклад, витрати на інтеграцію, навчання персоналу, технічну підтримку) (таблиця 3.15).

Таблиця 3.15 – Витрати на модернізацію мережі (на основі середніх ринкових цін 2023 року)

Категорія	Кількість одиниць	Приблизна вартість за одиницю, грн	Загальна вартість, грн
Комутатори Layer 3 (10 Gbps)	4	10000	40000
Маршрутизатори ядра (10 Gbps)	2	15000	30000
Сервери для віртуалізації (NFV)	3	30000	90000
Балансувальники навантаження	2	10000	20000
Брандмауери (з IDS/IPS)	2	8000	16000
Точки доступу Wi-Fi 6	10	1500	15000
Ліцензії на SDN	1	5000	5000
Ліцензії на QoS	1	3000	3000
Антивірусне ПЗ	1	5000	5000
Системи моніторингу (NetFlow, SNMP)	1	8000	8000
Прокладання оптоволоконних ліній	1	50000	50000
Прокладання мідних кабелів (Cat 6/7)	1	3000	3000
Енергетичне забезпечення	1	5000	5000
Інтеграція SDN	1	15000	15000
Налаштування QoS	1	5000	5000
Навчання персоналу	5	2000	10000
Загальна вартість	x	x	320000

На основі попереднього аналізу, загальна вартість модернізації ККМ складає 320000 грн. Завдяки впровадженню нових технологій, таких як SDN, віртуалізація, QoS та резервування, очікується зниження операційних витрат; розрахунок очікуваної вигоди від модернізації ККМ представлений у таблиці 3.15.

Таблиця 3.15 – Розрахунок очікуваної вигоди від модернізації ККМ

Показник	До впровадження	Після впровадження	Щорічна економія
Витрати на енергоспоживання (щорічно)	60000	36000	24000
Витрати на технічне обслуговування (щорічно)	30000	20000	10000
Простій через збої (щорічні втрати)	12000	3000	9000
Навчання персоналу (щорічно)	5000	2500	2500
Разом	107000	61500	45500

Отже, загальна економія на щорічних витратах після впровадження інновацій становить 45500 грн. Це дозволяє розрахувати ROI (Return on Investment, рентабельність інвестицій) та термін окупності проєкту.

Формула для розрахунку ROI має вид:

$$ROI = \frac{Чистий\ прибуток\ (вигода) - Інвестиції}{Інвестиції} \times 100\% \qquad (3.1)$$

Для нашого випадку інвестиції складають 320000 грн. (витрати на модернізацію), а щорічний чистий прибуток (вигода) становить 45500 грн. (економія на енергоспоживанні, технічному обслуговуванні, простоях та навчанні). Отже, за формулою (3.1) обчислимо:

$$ROI = \frac{45500 - 320000}{320000} \times 100\% = -85,78\%.$$

Від'ємне значення ROI означає, що інвестиції ще не окупляться за перший рік (що очікувано, оскільки це довгострокові інвестиції). Термін окупності інвестицій можна визначити за формулою:

$$T = \frac{Інвестиції}{Чистий\ річний\ прибуток\ (вигода)}. \tag{3.2}$$

Виконавши розрахунок за формулою (3.2), отримаємо:

$$T = \frac{320000}{45500} \approx 7\ років.$$

Таким чином, після 7 років експлуатації оптимізованої мережі інвестиції повністю окупляться, а далі ROI буде позитивним. Зауважимо, що для комп'ютерних мереж це достатньо великий термін окупності, який можна скоротити скоротивши початкові інвестиції або підвищивши щорічну вигоду. Наприклад, якщо вдасться збільшити щорічну економію на 20%, то термін окупності може скоротитися приблизно до 6 років замість 7.

Висновки до розділу 3

У третьому розділі було впроваджено практичні методи оптимізації ККМ на основі сучасних технологій.

Запропоновано проєкт оптимізації мережі, що включає віртуалізацію та сегментацію мережевих функцій (NFV), використання SDN для централізованого управління трафіком та динамічної маршрутизації, впровадження резервування на всіх рівнях мережевих компонентів (комутатори, маршрутизатори, сервери та канали зв'язку).

Реалізована програмна оптимізація мережі за допомогою SDN-контролера, що дозволяє централізовано моніторити та контролювати трафік, забезпечує QoS для пріоритизації критичних сервісів, виконує автоматичне балансування навантаження між серверами, здійснює резервування мережевих функцій через їх віртуалізацію.

Тестування оптимізованої мережі підтвердило зниження середньої затримки на 60-80%, підвищення пропускної здатності у 10 разів, зменшення втрат пакетів до менше ніж 1%, підвищення відмовостійкості – час відновлення мережі після збоїв зменшився з 300-600 секунд до 10-15 секунд.

Економічне обґрунтування модернізації продемонструвало зниження операційних витрат на енергоспоживання, технічне обслуговування та навчання персоналу. Термін окупності проєкту складає 7 років, після чого очікується значна економія ресурсів.

ВИСНОВКИ

За результатами виконаної роботи можна зробити висновки, що охоплюють основні результати, отримані у кожному розділі, та підтверджують досягнення поставленої мети – визначення ефективних підходів до оптимізації корпоративних комп'ютерних мереж для підвищення продуктивності, надійності та загальної ефективності.

У першому розділі розглянуто теоретичні основи оптимізації корпоративних мереж. Визначено структуру та класифікацію корпоративних мереж, їх ключові характеристики (продуктивність, масштабованість, безпека та надійність). Вивчено основні методи оптимізації: сегментацію для ізоляції трафіку, резервування для підвищення відмовостійкості та балансування навантаження для ефективного розподілу ресурсів. Описано сучасні технології оптимізації, серед яких SDN для централізованого управління, QoS для пріоритизації критичного трафіку та NFV для віртуалізації функцій мережі.

У другому розділі проведено аналіз поточного стану корпоративних мереж, визначено основні проблеми: перевантаження вузлів, низька масштабованість та ненадійність у разі збоїв. Запропоновано напрями вирішення: впровадження резервування для забезпечення безперервної роботи, SDN-контролерів для динамічного управління трафіком та QoS для оптимізації пріоритетного трафіку. Проведений аналіз показав, що запропоновані рішення дозволяють підвищити пропускну здатність на 30-50%, зменшити затримки на 60-80% та мінімізувати втрати пакетів.

У третьому розділі запропоновано проєкт оптимізації мережі, який включає впровадження віртуалізації (NFV), SDN-контролера для автоматизації маршрутизації та резервування основних компонентів мережі. Розроблене програмне рішення забезпечило зниження середніх затримок на 60-80%, підвищення пропускної здатності у 10 разів та скорочення часу відновлення після збоїв до 10-15 секунд. Техніко-економічне обґрунтування підтвердило доцільність

запропонованих заходів, а термін окупності проєкту становить 7 років, після чого очікується значна економія ресурсів.

Практична значущість роботи полягає у можливості впровадження розроблених методів оптимізації у великих корпоративних мережах для підвищення їх ефективності, надійності та відмовостійкості.

Перспективи подальших досліджень полягають у розширенні можливостей автоматизації управління корпоративними мережами за допомогою штучного інтелекту (AI) та машинного навчання (ML) для прогнозування навантажень і оптимізації трафіку в реальному часі, а також інтеграції вдосконалених методів кібербезпеки у процеси оптимізації корпоративних мереж.