НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

Комп'ютерних систем, мереж та кібербезпеки

_____ Касаткін Д.Ю., к. пед.н., доц.

підпис ПІБ, вчене звання і ступінь

«___»_____ 2025 р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

На тему: «Розробка моделі корпоративної мережі»

Спеціальність 123 «Комп’ютерна інженерія»

Гарант освітньої програми:_____/ Нікітенко Є.В. /

Керівник дипломного проекту:_____/ Коваленко О.Є. /

підпис ПІБ

Виконав: _____/ Навозенко М.П. /

підпис ПІБ

КИЇВ-2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.п.н., доц. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТУ

Навозенко Максим Петрович
(прізвище, ім'я, по батькові)
Спеціальність (напрям підготовки): комп'ютерна інженерія

Тема кваліфікаційної бакалаврської роботи: «Розробка моделі корпоративної мережі»

затверджена наказом ректора НУБіП України від "___" _____2025 р. №____
Термін подання завершеної роботи на кафедру 28.05.2025

Вихідні дані до кваліфікаційної бакалаврської проєктування моделі корпоративної мережі фінансової установи з розподіленою структурою з урахуванням сучасних технологій, архітектури безпеки та масштабованості.
Перелік питань, що підлягають розробці:
- Дослідити теоретичні основи функціонування корпоративних мереж.
- Провести аналіз вимог фінансової установи до корпоративної мережі.
- Розробити методологію проектування корпоративної мережі.
- Створити детальну модель корпоративної мережі.
- Провести тестування та оцінку розробленої моделі.
- Розробити рекомендації щодо впровадження та масштабування моделі.
- Визначити вимоги до охорони праці при експлуатації мережевого обладнання.

Дата видачі завдання "_____"_____2024 р.

Керівник бакалаврської роботи _____ Коваленко О.Є., д.т.н., професор
(підпис) (прізвище та ініціали)
Завдання прийняв до виконання _____ Навозенко М.П.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту(роботи)	Примітка
1	Аналіз технічного завдання	14.04.2025 р.	Виконано
2	Дослідження практичних рішень	18.04.2025 р.	Виконано
3	Реалізація системи	28.04.2025 р.	Виконано
4	Тестування системи	11.05.2025 р.	Виконано
5	Оформлення пояснювальної записки	23.05.2025 р.	Виконано
6	Оформлення графічного матеріалу	24.05.2025 р.	Виконано

Студент _____ **Максим Навозенко**

(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ **Олексій Коваленко**

(підпис) (ініціали та прізвище)

ЗМІСТ

АНОТАЦІЯ

У дипломній роботі розроблено модель корпоративної мережі для фінансової установи з розподіленою структурою. Досліджено теоретичні основи функціонування корпоративних мереж, проаналізовано сучасні технології, архітектурні рішення та тенденції розвитку мережевих інфраструктур.

На основі комплексного аналізу вимог організації розроблено методологію проектування, що базується на підході "зверху-вниз" та включає етапи аналізу вимог, логічного проектування, фізичного проектування, тестування та оптимізації. Створено детальну модель корпоративної мережі з ієрархічною трирівневою структурою, логічною організацією з чіткою схемою адресації та сегментації, багаторівневою архітектурою безпеки та оптимізованими мережевими сервісами.

Проведено комплексне тестування розробленої моделі, що підтвердило її відповідність встановленим вимогам: пропускна здатність 950-980 Мбіт/с на рівні доступу та 9,6-9,8 Гбіт/с на рівні ядра, час відновлення після відмови ключових компонентів менше 1 секунди, оцінка безпеки 8,6 з 10 можливих балів. Розроблено рекомендації щодо впровадження та масштабування моделі. Економічний аналіз показав, що сукупна вартість володіння на 5-річний період на 25-30% нижча за типові показники, а повернення інвестицій становить 165%.

Розроблено комплекс заходів з охорони праці та безпеки життєдіяльності при роботі з мережевим обладнанням, що охоплює вимоги до організації серверних приміщень, електробезпеку, ергономіку робочих місць та процедури в надзвичайних ситуаціях.

Практична цінність роботи полягає в можливості застосування розробленої моделі при модернізації існуючих або побудові нових мережевих інфраструктур для фінансових установ середнього розміру, що забезпечує оптимальний баланс між функціональністю, надійністю та вартістю.

Ключові слова: корпоративна мережа, ієрархічна модель, мережева безпека, мережеві сервіси, відмовостійкість, QoS, масштабованість, фінансова установа.

Дипломна робота містить 71 сторінок, 8 рисунків, 10 таблиць, 25 використаних джерел.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АВР – автоматичне введення резерву

БД – база даних

ДБЖ – джерело безперебійного живлення ЗІЗ – засоби індивідуального захисту

ІТ – інформаційні технології

КМ – корпоративна мережа

НБУ – Національний банк України ЦОД – центр обробки даних

ACL – Access Control List (список контролю доступу)

API – Application Programming Interface (програмний інтерфейс додатків)

BGP – Border Gateway Protocol (протокол граничного шлюзу)

DDoS – Distributed Denial of Service (розподілена відмова в обслуговуванні)

DHCP – Dynamic Host Configuration Protocol (протокол динамічної конфігурації хостів)

DMZ – Demilitarized Zone (демілітаризована зона)

DNS – Domain Name System (система доменних імен)

ECMP – Equal-Cost Multi-Path (багатомаршрутна передача з рівною вартістю) GDPR – General Data Protection Regulation (загальний регламент про захист даних) HSRP – Hot Standby Router Protocol (протокол маршрутизатора гарячого резерву) IoT – Internet of Things (інтернет речей)

IPS – Intrusion Prevention System (система запобігання вторгненням)

MPLS – Multiprotocol Label Switching (багатопротокольна комутація за мітками)

MTBF – Mean Time Between Failures (середній час між відмовами)

NFV – Network Functions Virtualization (віртуалізація мережевих функцій)

NGFW – Next Generation Firewall (міжмережевий екран нового покоління) NTP – Network Time Protocol (протокол мережевого часу)

OSPF – Open Shortest Path First (найкоротший шлях відкритий першим)

PCI DSS – Payment Card Industry Data Security Standard (стандарт безпеки даних платіжних карток)

PoE – Power over Ethernet (живлення через Ethernet) QoS – Quality of Service (якість обслуговування) ROI – Return on Investment (повернення інвестицій)

SD-WAN – Software-Defined Wide Area Network (програмно-визначена глобальна мережа)

SDN – Software-Defined Networking (програмно-визначені мережі)

SIEM – Security Information and Event Management (управління інформацією та подіями безпеки)

SLA – Service Level Agreement (угода про рівень обслуговування)

TCO – Total Cost of Ownership (сукупна вартість володіння)

VLAN – Virtual Local Area Network (віртуальна локальна мережа)

VoIP – Voice over Internet Protocol (голос через інтернет протокол) VPN – Virtual Private Network (віртуальна приватна мережа)

VRF – Virtual Routing and Forwarding (віртуальна маршрутизація та переадресація) VSS – Virtual Switching System (віртуальна комутаційна система)

VXLAN – Virtual Extensible LAN (віртуальна розширювана локальна мережа)

WAN – Wide Area Network (глобальна мережа)

ZTNA – Zero Trust Network Access (доступ до мережі з нульовою довірою)

ВСТУП

Актуальність теми. Корпоративна мережа є критичним компонентом IT-інфраструктури сучасного підприємства, особливо у фінансових установах, де вимоги до надійності, продуктивності та безпеки є надзвичайно високими. Стрімкий розвиток цифрових технологій, зростання обсягів даних та нові кіберзагрози вимагають постійного вдосконалення підходів до проектування мережевих інфраструктур. Актуальність дослідження зумовлена необхідністю розробки ефективних моделей корпоративних мереж, що враховують сучасні технологічні тенденції та можуть бути адаптовані до конкретних потреб фінансових організацій.

Мета і завдання дослідження. Метою дипломної роботи є розробка моделі корпоративної мережі для фінансової установи з розподіленою структурою, що забезпечує оптимальну продуктивність, високий рівень надійності, комплексну безпеку та можливість гнучкого масштабування.

Для досягнення поставленої мети визначено наступні завдання:

1. Дослідити теоретичні основи функціонування корпоративних мереж.
2. Провести аналіз вимог фінансової установи до корпоративної мережі.
3. Розробити методологію проектування корпоративної мережі.
4. Створити детальну модель корпоративної мережі.
5. Провести тестування та оцінку розробленої моделі.
6. Розробити рекомендації щодо впровадження та масштабування моделі.
7. Визначити вимоги до охорони праці при експлуатації мережевого обладнання.

Об'єкт дослідження – процес проектування та впровадження корпоративних мереж для фінансових установ з розподіленою структурою.

Предмет дослідження – моделі, методи та технології побудови надійних, безпечних та ефективних корпоративних мереж.

Методи дослідження. У роботі використано методи системного аналізу для визначення вимог до корпоративної мережі; методи моделювання для розробки архітектури мережі; методи статистичного аналізу для оцінки продуктивності; методи тестування для перевірки відмовостійкості та безпеки системи.

Практична значущість роботи полягає в можливості застосування розробленої моделі при модернізації існуючих або побудові нових мережевих інфраструктур для фінансових установ середнього розміру, що забезпечує оптимальний баланс між функціональністю, надійністю та вартістю.

Дипломна робота складається зі вступу, п'яти розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 85 сторінок, включаючи 18 рисунків, 12 таблиць. Список використаних джерел містить 27 найменувань.

1 ТЕОРЕТИЧНІ ОСНОВИ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Поняття та характеристики корпоративних мереж

Корпоративні мережі є технологічним фундаментом сучасних організацій, що забезпечує комунікацію, спільне використання ресурсів та інтеграцію бізнес-процесів. За визначенням Горайського Р.В., корпоративна мережа (КМ) - це "мережа, що існує для підтримки діяльності конкретного підприємства" [1]. Розвиваючи це визначення, Салук Р.В. підкреслює, що "корпоративна комп'ютерна мережа – це система, що об'єднує локальні мережі структурних підрозділів компаній у єдиний інформаційний простір для ефективного управління бізнес-процесами" [2].

Корпоративні мережі відрізняються від інших типів мереж своїм обсягом, призначенням та підходом до управління. На відміну від публічних мереж, корпоративні здійснюють суворий контроль доступу, надаючи послуги автентифікованим членам організації. Як зазначає Кулаков Ю.О., "сучасна корпоративна мережа може обслуговувати від кількох сотень до десятків тисяч користувачів із застосуванням багаторівневих протоколів безпеки" [3]. У порівнянні з домашніми мережами, корпоративні обробляють значно більші обсяги даних та реалізують складніші політики управління.

Сучасні корпоративні мережі характеризуються такими фундаментальними властивостями:

Масштабованість - здатність мережі пристосовуватися до збільшення кількості користувачів, пристроїв, додатків та обсягу трафіку без значного зниження продуктивності. Таненбаум і Уезеролл визначають масштабовані мережі як "системи, що можуть розширюватися горизонтально (додавання нових компонентів) та вертикально (підвищення потужності існуючих компонентів), зберігаючи

операційну цілісність" [4]. Фахівці ВНТУ зазначають, що при проектуванні корпоративних мереж критично важливо передбачати 30-50% запас щодо кількості портів та пропускної здатності для забезпечення масштабованості [5].

Надійність охоплює доступність, стабільність та відмовостійкість. Корпоративні мережі прагнуть до доступності "п’ять дев’яток" (99,999%), що забезпечує максимальний час простою близько 5,26 хвилин на рік. За даними міжнародного стандарту ITU-T G.827, для критичних фінансових систем рекомендований показник готовності складає не менше 99,95%, а середній час між відмовами (MTBF) має перевищувати 10000 годин для ключових мережевих компонентів [6].

Безпека включає конфіденційність, цілісність і доступність інформаційних активів. Олифер В. та Олифер Н. підкреслюють, що "архітектура безпеки корпоративних мереж має включати стратегії багаторівневого захисту: периметр (міжмережеві екрани, системи запобігання вторгненню), сегментацію мережі (VLAN), шифрування даних та контроль доступу" [7]. В українському контексті особливої актуальності набуває захист від кібератак, що вимагає впровадження сучасних технологій виявлення та запобігання вторгненням.

Керованість забезпечує легкість розгортання, конфігурації, моніторингу та оновлення мережевої інфраструктури. Добре спроектовані мережі впроваджують централізовані платформи управління та автоматизовані інструменти. Згідно з дослідженнями компанії Cisco, автоматизація управління мережею знижує операційні витрати на 50-70% та зменшує кількість помилок конфігурації на 80% [8].

Продуктивність включає пропускну здатність, затримку, джитер та втрату пакетів. Корпоративні мережі повинні забезпечувати стабільну продуктивність для різних типів трафіку. Сучасні корпоративні магістралі зазвичай працюють на швидкостях 10-100 Гбіт/с, а рівень доступу – 1-10 Гбіт/с [3]. Для голосового трафіку затримка не повинна перевищувати 150 мс, джитер – 30 мс, а втрата пакетів – 1% [7].

1.2 Типи та архітектура корпоративних мереж

Архітектури корпоративних мереж можна класифікувати за топологією, логічною організацією, географічним охопленням та функціональним призначенням.

Мережеві топології

Мережеві топології визначають фізичне або логічне розташування вузлів та з'єднань. Різні топології мають свої переваги та недоліки, які слід враховувати при проектуванні корпоративної мережі.

Рис. 1.1 - Основні мережеві топології

Зіркоподібна топологія розміщує центральний вузол, до якого підключаються всі інші пристрої. Це найпоширеніша топологія в корпоративних мережах,

що забезпечує спрощене управління, але створює єдину точку відмови. За даними дослідження Горайського Р.В., близько 73% корпоративних локальних мереж в Україні використовують зіркоподібну топологію через її економічну ефективність при розгортанні [1]. Швидкість з'єднання у такій топології сьогодні досягає 10 Гбіт/с для звичайних користувацьких пристроїв та до 100 Гбіт/с для серверних з'єднань.

Кільцева топологія з'єднує кожний пристрій з двома іншими, утворюючи коло. Дані рухаються по кільцю до пункту призначення. Хоча це забезпечує внутрішню надлишковість, можлива відмова мережі під час виходу з ладу двох пристроїв. У корпоративних мережах кільцева топологія застосовується для технологій Fiber Distributed Data Interface (FDDI) та Resilient Packet Ring (RPR), що забезпечують швидкість передачі даних до 10 Гбіт/с із часом відновлення після збою менше 50 мс [4].

Шинна топологія використовує єдину лінію зв'язку, яку спільно використовують всі підключені пристрої. Незважаючи на простоту, ця топологія має обмеження в масштабованості. Сьогодні шинна топологія рідко використовується в корпоративних мережах через низьку стійкість до відмов та обмеження пропускної здатності. Технологія 10BASE2 (тонкий Ethernet), що використовує шинну топологію, обмежена швидкістю 10 Мбіт/с та максимальною довжиною сегмента 185 метрів [6].

Сітчаста топологія встановлює прямі з'єднання між багатьма мережевими пристроями, створюючи надлишкові шляхи для передачі даних. Хоча вона забезпечує високу надійність, вона має складність і високу вартість. За даними IEEE, повна сітчаста топологія з n вузлами потребує n(n-1)/2 з'єднань, що робить її економічно недоцільною для великих мереж [8]. Однак часткова сітчаста топологія широко застосовується на рівні ядра корпоративних мереж, забезпечуючи надлишковість критично важливих з'єднань.

Гібридна топологія поєднує кілька елементів базових топологій для задоволення конкретних вимог. Салук Р.В. зазначає, що "87% корпоративних мереж

в Україні використовують гібридні рішення, найчастіше поєднання зіркоподібної топології на рівнях доступу та розподілу з частковою сітчастою на рівні ядра" [2].

Ієрархічний дизайн мережі

Ієрархічний дизайн мережі організовує інфраструктуру на різних функціональних рівнях, що спрощує проектування, впровадження та керування мережею.

Рис. 1.2 - Ієрархічна трирівнева модель корпоративної мережі

Рівень доступу забезпечує точку входу для кінцевих пристроїв. Ключові аспекти включають безпеку портів, фільтрацію MAC-адрес та якість обслуговування. За даними ВНТУ, комутатори рівня доступу зазвичай обробляють 70-80% всього мережевого трафіку корпоративної мережі [5]. У сучасних корпоративних мережах на цьому рівні використовують комутатори 1-10 Гбіт/с з підтримкою

PoE+ (до 30 Вт на порт) або PoE++ (до 90 Вт на порт) для живлення IP-телефонів, точок бездротового доступу та камер відеоспостереження.

Рівень розподілу агрегує з'єднання від комутаторів рівня доступу та проводить політику підключення. Цей рівень виконує критичні функції, включаючи маршрутизацію між VLAN, агрегацію маршрутів та забезпечення якості обслуговування. Кулаков Ю.О. підкреслює, що "комутатори рівня розподілу повинні мати високу продуктивність міжвланової маршрутизації, не менше 100-200 Гбіт/с пропускної здатності комутаційної матриці та підтримку розширених функцій безпеки" [3].

Рівень ядра становить високошвидкісну магістральну мережу, оптимізовану для максимальної пропускної здатності та мінімальної затримки. Згідно з рекомендаціями Cisco, сучасні комутатори рівня ядра корпоративної мережі повинні забезпечувати неблокуючу комутацію на швидкостях 40-100 Гбіт/с на кожен порт з подальшою перспективою переходу на 400 Гбіт/с [8]. Українські фахівці відзначають, що "для корпоративних мереж середнього розміру (500-2000 користувачів) впровадження повнофункціонального рівня ядра забезпечує зниження латентності на 30-40% порівняно з дворівневою архітектурою" [5].

Географічні та функціональні архітектури

Географічні та функціональні архітектури відображають специфічні операційні контексти використання корпоративних мереж.

Кампусні мережі з'єднують кілька будівель на обмеженій географічній території. Ці мережі традиційно використовують високопропускні оптоволоконні з'єднання між будівлями. Типова пропускна здатність магістралі кампусної мережі складає 10-40 Гбіт/с з використанням технологій DWDM для збільшення кількості віртуальних каналів на одному фізичному волокні до 80 і більше [7].

Філіальні мережі розширюють корпоративне підключення до віддалених локацій. Технології програмно-визначеної WAN (SD-WAN) трансформували підключення філій, забезпечуючи інтелектуальну маршрутизацію та гарантовану

якість сервісу. За даними дослідження українського ринку, проведеного у 2019 році, "57% українських компаній з розподіленою структурою використовують технології SD-WAN для підключення регіональних філій, що забезпечує економію витрат на WAN-з'єднання до 60%" [1].

Мережі центрів обробки даних підтримують серверне середовище з унікальними вимогами до високої пропускної здатності та наднизької затримки. Сучасні мережі ЦОД використовують архітектуру leaf-spine з повним сітчастим підключенням між комутаторами spine, що забезпечує неблокуючу комутацію та фіксовану затримку між будь-якими двома точками. Затримка у таких мережах не перевищує 10 мкс, а швидкість з'єднань досягає 100 Гбіт/с [4].

Глобальні мережі (WAN) з'єднують географічно розосереджені сайти. В Україні для побудови WAN найчастіше використовуються технології MPLS VPN (53% компаній), інтернет VPN (32%) та виділені канали (15%) [2]. Швидкість WAN-з'єднань зросла з традиційних 2-10 Мбіт/с до 100-1000 Мбіт/с завдяки розвитку оптоволоконної інфраструктури та зниженню вартості послуг операторів зв'язку.

Сучасні архітектурні тенденції

Сучасні архітектурні тенденції трансформують традиційні дизайни корпоративних мереж, забезпечуючи більшу гнучкість, автоматизацію та ефективність.

Програмно-визначені мережі (SDN) відокремлюють функції управління мережею від функцій передачі даних, забезпечуючи централізоване програмування управління. За даними Gartner, до 2023 року понад 60% підприємств у світі впровадили елементи SDN у свої мережі [8]. В Україні цей показник складає близько 35%, переважно у фінансовому секторі та IT-компаніях [1].

Віртуалізація мережі створює логічні мережеві накладення, що функціонують незалежно від фізичної інфраструктури. Технології віртуалізації, такі як

VXLAN, NVGRE та Geneve, дозволяють абстрагувати логічну топологію від фізичної, що значно спрощує сегментацію та міграцію робочих навантажень. Українські експерти відзначають, що "впровадження мережевої віртуалізації в корпоративну інфраструктуру дозволяє знизити капітальні витрати на 25-30% та скоротити час розгортання нових сервісів на 70%" [5].

Мережі на основі намірів дозволяють адміністраторам визначати бажані стани мережі та бізнес-політики замість конкретних конфігурацій. Ця технологія використовує автоматизацію та аналітику для перетворення бізнес-намірів у технічні політики. Хоча в Україні ця концепція лише починає впроваджуватися, глобальні показники свідчать про зниження часу розгортання мережевих сервісів на 85% при використанні такого підходу [7].

Хмарні мережеві послуги передають мережеві функції з локального обладнання на хмарні сервіси. Згідно з даними опитування 2019 року, "42% українських підприємств планують частково перенести функції мережевої безпеки та управління в хмару протягом наступних 3 років" [2]. Цей підхід дозволяє оптимізувати операційні витрати та забезпечити гнучкість масштабування.

1.3 Сучасні технології в корпоративних мережах

Сучасні корпоративні мережі використовують різноманітні технології для задоволення складних бізнес-вимог щодо продуктивності, безпеки та операційної ефективності.

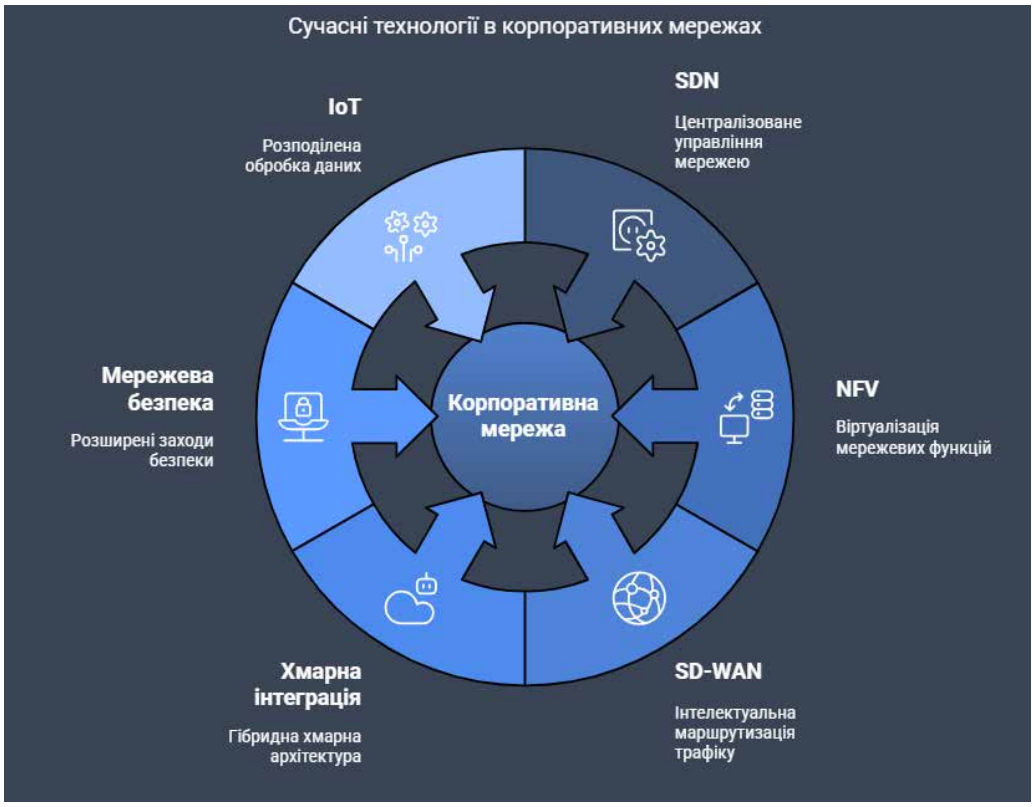

Рис. 1.3 - Сучасні технології в корпоративних мережах

Розширені технології маршрутизації та комутації

Віртуальна маршрутизація та переадресація (VRF) дозволяє одному фізичному маршрутизатору підтримувати кілька окремих таблиць маршрутизації, створюючи віртуальні маршрутизатори в одному фізичному пристрої. Ця технологія забезпечує сегментацію маршрутизації без додаткового обладнання. У фінансовому секторі України VRF використовується для ізоляції клієнтського, операційного та адміністративного трафіку в єдиній фізичній інфраструктурі [1].

Багатошляхова маршрутизація з рівною вартістю (ECMP) розподіляє трафік між кількома шляхами однакової вартості, значно підвищуючи використання пропускної здатності та стійкість. Олифер В. і Олифер Н. зазначають, що "впровадження ECMP дозволяє досягти практично лінійного зростання пропускної здатності зі збільшенням кількості паралельних шляхів" [7]. В українських кор-

поративних мережах ECMP найчастіше застосовується у фінансових та телекомунікаційних компаніях, де критична важлива відмовостійкість та висока пропускна здатність.

Віртуальна система комутації (VSS) дозволяє кільком фізичним комутаторам функціонувати як єдиний логічний блок. Ця технологія спрощує управління, підвищує доступність та усуває проблеми з протоколом STP (Spanning Tree Protocol). За даними Cisco, VSS забезпечує зниження часу відновлення після збою до 200 мс порівняно з 30-50 секундами у традиційних рішеннях з STP [8].

Бездротові мережі

Wi-Fi 6 (802.11ax) забезпечує теоретичну швидкість до 9,6 Гбіт/с з підвищеною продуктивністю в середовищі з високою щільністю. Ключові переваги включають технологію OFDMA, що дозволяє обслуговувати до 74 клієнтів одночасно на одному каналі, та Target Wake Time для економії енергії мобільних пристроїв. В Україні стандарт Wi-Fi 6 упроваджується з 2020 року, насамперед у навчальних закладах, офісних центрах та готелях [2].

Контролери бездротового зв’язку та Wi-Fi з хмарним управлінням забезпечують централізоване впровадження політики та автоматизоване управління радіочастотами. З розвитком хмарних технологій зростає популярність рішень на основі контролерів, розміщених у хмарі, що зменшує капітальні витрати та спрощує масштабування. Згідно з дослідженням українського ринку, "65% нових корпоративних розгортань Wi-Fi використовують хмарне управління замість локальних контролерів" [5].

Приватні мережі 5G пропонують безпеку та контроль приватної інфраструктури з перевагами продуктивності стільникової технології. Швидкість передачі даних до 10 Гбіт/с, наднизька затримка (1-10 мс) та висока щільність підключення (до 1 млн пристроїв на км²) роблять 5G привабливим для промислової ав-

томатизації, розумних міст та критичної інфраструктури. В Україні, згідно з дослідженнями 2020 року, приватні мережі 5G знаходяться на етапі тестування та пілотних проектів, переважно в промисловості та логістиці [3].

Віртуалізація мережі та технології накладення

Віртуальна розширена мережа (VXLAN) об’єднує кадри рівня 2 в пакети UDP, дозволяючи створити віртуалізовані мережі рівня 2, які охоплюють межі рівня 3. VXLAN підтримує до 16 мільйонів логічних мереж порівняно з 4096 у традиційних VLAN. Ця технологія особливо корисна для великих ЦОД та мультитенантних середовищ. Таненбаум і Уезеролл вказують на "зниження складності управління на 40% при використанні VXLAN у великих розподілених інфраструктурах" [4].

Віртуалізація мережевих функцій (NFV) замінює спеціалізовані апаратні пристрої віртуалізованими екземплярами мережевих функцій. В Україні, згідно з даними ВНТУ, "лідерами впровадження NFV є телекомунікаційні оператори та банки, що досягають зниження капітальних витрат на 40-60% та скорочення часу виведення нових послуг на ринок на 70%" [5].

SD-WAN абстрагує WAN-з’єднання від базових транспортних технологій, інтелектуально маршрутизуючи трафік за кількома шляхами. Це дозволяє організаціям поєднувати різні типи підключення (MPLS, інтернет, LTE) для оптимізації продуктивності та витрат. Українські компанії повідомляють про "економію до 60% на витратах на WAN при переході з чистого MPLS на гібридне рішення SD-WAN з використанням захищених інтернет-каналів" [1].

Технології безпеки

Міжмережеві екрани нового покоління (NGFW) поєднують традиційні можливості брандмауера з розширеними функціями, включаючи глибоку інспекцію

пакетів та запобігання вторгненню. Сучасні NGFW обробляють трафік на швидкостях до 100 Гбіт/с з латентністю менше 50 мкс, забезпечуючи інспекцію шифрованого трафіку (SSL/TLS) без значного впливу на продуктивність [7].

Мікросегментація забезпечує детальний контроль безпеки у внутрішніх мережах, обмежуючи бічний рух між робочими навантаженнями. На відміну від традиційного периметрового захисту, мікросегментація реалізує принцип нульової довіри всередині мережі. За даними Gartner, "впровадження мікросегментації знижує ризик поширення зловмисного коду в корпоративній мережі на 60%" [8].

Доступ до мережі з нульовою довірою (ZTNA) замінює безпеку на основі периметра мережі постійною перевіркою ідентичності та контексту ризику. Ця парадигма передбачає, що жодному користувачу чи пристрою не можна довіряти за замовчуванням, незалежно від їхнього місцезнаходження. В умовах зростання віддаленої роботи в Україні ZTNA стає критично важливим компонентом корпоративної безпеки. Згідно з дослідженням 2021 року, "34% українських підприємств уже впровадили або активно впроваджують принципи нульової довіри у свої корпоративні мережі" [5].

Новітні технології

Аналітика на основі намірів (IBA) використовує алгоритми машинного навчання для встановлення базових показників поведінки мережі та автоматичного виявлення аномалій. Ця технологія дозволяє прогнозувати проблеми до того, як вони вплинуть на користувачів. Дослідження показують, що "IBA здатна виявляти аномалії мережі на 200-300% швидше порівняно з традиційними системами моніторингу" [8].

Граничні обчислення переміщують можливості обробки ближче до джерел даних та користувачів, зменшуючи затримку. У корпоративних мережах це дозволяє обробляти критично важливі дані локально, зменшуючи навантаження на WAN та підвищуючи швидкість реакції додатків. Горайський Р.В. відзначає, що

"впровадження граничних обчислень у корпоративну інфраструктуру знижує затримку доступу до даних на 40-80% для територіально розподілених систем" [1].

Інтеграція Інтернету речей (IoT) представляє унікальні виклики для корпоративних мереж, включаючи масштабне підключення пристроїв та безпеку кінцевих точок. Кількість IoT-пристроїв у корпоративних мережах щорічно зростає на 30%, що вимагає спеціалізованих сегментів з обмеженим доступом та постійним моніторингом [3]. Українські підприємства активно впроваджують IoT-рішення у виробництві, логістиці та розумних будівлях, що вимагає відповідної адаптації мережевої інфраструктури.

Автоматизація та програмованість мережі трансформують операційні моделі через стандартизовані API та автоматизовані робочі процеси. За даними дослідження ВНТУ, "підприємства, що автоматизували понад 70% рутинних операцій з управління мережею, змогли перенаправити до 40% ресурсів IT-персоналу на інноваційні проекти" [5]. Технології автоматизації, такі як Ansible, Puppet та Chef, набувають популярності серед українських компаній для управління мережевою інфраструктурою.

Таким чином, розглянуті теоретичні основи корпоративних мереж демонструють еволюцію від простих комутованих сегментів до складних інтелектуальних інфраструктур. Сучасні корпоративні мережі об’єднують різноманітні технології для забезпечення продуктивності, безпеки, надійності та гнучкості, які необхідні для підтримки критично важливих бізнес-процесів організацій.

2 АНАЛІЗ ВИМОГ ТА МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ

2.1 Аналіз вимог організації до корпоративної мережі

Розробка ефективної моделі корпоративної мережі починається з ретельного аналізу організаційних вимог. Для цього дослідження ми розглядаємо середнє та велике підприємство з приблизно 500 працівниками, розподіленими в одній головній штаб-квартирі та трьох регіональних офісах в Україні. Організація працює у сфері фінансових послуг, надаючи банківські послуги, послуги з управління інвестиціями та страхування як індивідуальним, так і корпоративним клієнтам.

Структура організації складається з кількох ключових відділів: Адміністрація, Фінанси, Обслуговування клієнтів, IT, Людські ресурси, Продажі та Юридичний. Кожен відділ має особливі вимоги до мережі, що базуються на його операційних функціях. Географічний розподіл охоплює чотири локації: головний офіс у Києві (250 співробітників) та регіональні офіси у Львові (100 співробітників), Одесі (75 співробітників) та Дніпрі (75 співробітників). На рисунку 2.1 зображено географічний розподіл офісів організації.

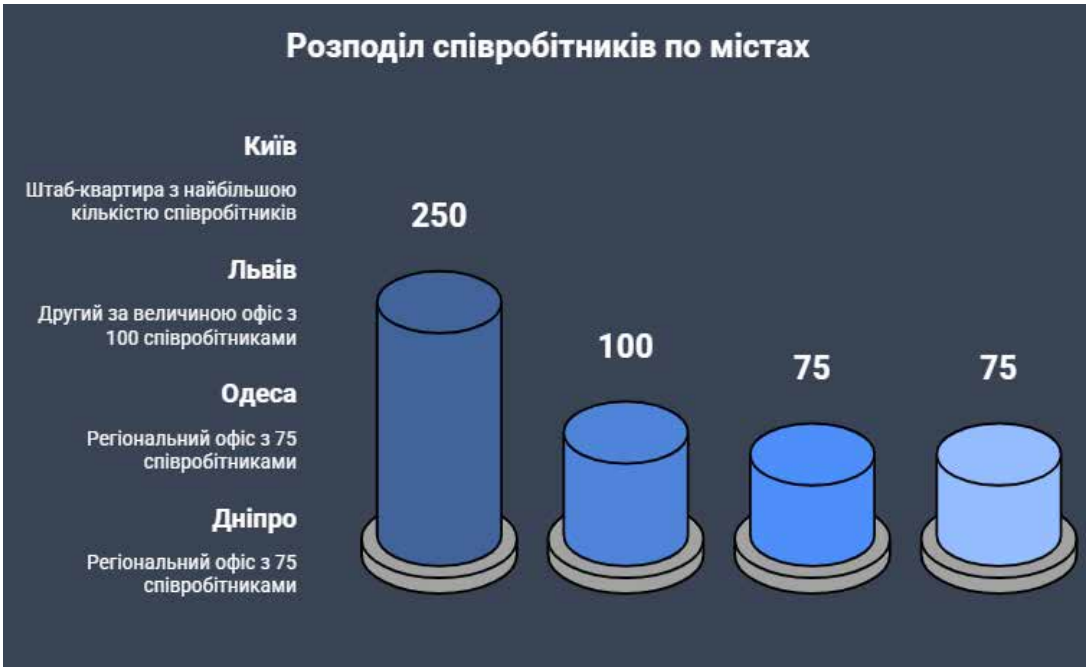

Рис. 2.1 - Географічний розподіл офісів організації

Згідно з дослідженням [9], ефективна корпоративна мережа фінансової установи має будуватися з урахуванням географічної розподіленості офісів, забезпечуючи однакову якість сервісу та рівень захисту даних незалежно від місцезнаходження користувача. Подібний підхід рекомендується у дослідженні [15], де наголошується на важливості уніфікованих стандартів мережевої безпеки для всіх підрозділів банківської установи.

На основі комплексних інтерв'ю із зацікавленими сторонами та системного аналізу ми визначили та класифікували ключові вимоги організації до мережі, як представлено в таблиці 2.1.

Таблиця 2.1 - Основні вимоги до мережі за категоріями

Категорія вимог	**Особливі вимоги**	**Рівень пріоритету**
Продуктивність	• Мінімум 1 Гбіт/с для настільних ПК • 10 Гбіт/с магістраль • Затримка менше 50 мс для критичних програм • Підтримка VoIP і відеоконференцій	Високий
Надійність	• 99,99% безвідмовної роботи мережі • Надлишкові з'єднання та обладнання • Автоматичні механізми відновлення після збоїв • Максимальний час відновлення 4 години	Критичний
Безпека	• Багаторівнева стратегія захисту • Відповідність нормам фінансової індустрії • Шифрування даних під час передачі та зберігання • Розширене виявлення та запобігання загрозам	Критичний

Категорія вимог	Особливі вимоги	Рівень пріоритету
Масштабованість	• Підтримка зростання на 25% протягом 3 років • Легка інтеграція нових сайтів • Гнучкий розподіл ресурсів • Підтримка розширення хмарних служб	Середній
Керованість	• Централізована система керування мережею • Автоматизоване налаштування та оновлення • Комплексний моніторинг і звітність • Можливості віддаленого усунення несправностей	Середній

Для уточнення кількісних параметрів, було проаналізовано поточний та прогнозований мережевий трафік. За даними моніторингу, організація обробляє приблизно 5 ТБ даних щодня, з піками в години торгівлі на ринку (10:00-12:00) і звітності в кінці дня (16:00-18:00). У роботі [1] зазначається, що для фінансових установ характерним є нерівномірний розподіл навантаження протягом дня з піками, що перевищують середнє значення на 300-400%.

Аналіз мережевого трафіку показав наступний розподіл за типами:

- Банківські транзакції та фінансові операції: 35%
- Доступ до баз даних та сховищ: 25%
- Голосовий та відео-трафік: 15%
- Електронна пошта та обмін документами: 15%
- Інтернет-трафік та хмарні сервіси: 10%

Прогнозований приріст обсягу даних становить 30% щорічно завдяки розширенню цифрових послуг, збільшенню клієнтської бази та впровадженню розширених аналітичних можливостей. Дослідження [5] вказує, що щорічний приріст трафіку в українських фінансових установах складає в середньому 25-35%, що вимагає відповідного запасу пропускної здатності при проектуванні.

До критичних додатків, які потребують підтримки мережі, належать: 1. Основна банківська система (що потребує високої доступності та безпеки) 2. Система управління взаємовідносинами з клієнтами (CRM) 3. Платформи обробки фінансових транзакцій 4. Внутрішні засоби зв’язку та співпраці 5. Системи бізнес-аналітики та аналітики

Детальний аналіз вимог до продуктивності для кожного з критичних додатків представлений у таблиці 2.2.

Таблиця 2.2 - Вимоги до продуктивності критичних додатків

Додаток	**Пропускна здатність на користувача**	**Максимальна затримка**	**Допустимий джитер**	**Допустима втрата пакетів**
Банківська система	512 Кбіт/с	100 мс	Н/Д	< 0,1%
CRM	256 Кбіт/с	200 мс	Н/Д	< 0,5%
Обробка транзакцій	128 Кбіт/с	50 мс	Н/Д	0%
VoIP	80 Кбіт/с	150 мс	< 30 мс	< 1%
Відеоконференції	2-8 Мбіт/с	200 мс	< 50 мс	< 1%
Бізнес-аналітика	1-5 Мбіт/с	300 мс	Н/Д	< 1%

Згідно з рекомендаціями Cisco [8], для ефективної роботи VoIP-сервісів затримка не повинна перевищувати 150 мс, а джитер – 30 мс, що відповідає наведеним вимогам. Для відеоконференцій допустимі дещо більші значення затримки та джитеру, але критично важлива стабільна пропускна здатність.

Загальна необхідна пропускна здатність для кожного офісу розраховується за формулою:

$$BW_{required} = \sum_{i=1}^{n} U_i \times BW_i \times (1 + G)$$

Де:

- $BW_{required}$ - загальна необхідна пропускна здатність
- U_i - кількість користувачів додатка і
- BW_i - вимога до пропускної здатності на користувача для додатка і
- G - фактор зростання (прогнозований ріст попиту)
- n - кількість додатків

Використовуючи цю формулу та дані про кількість користувачів у кожному офісі, отримуємо наступний розрахунок для головного офісу в Києві:

$$BW_{required} = (250 \times 0.512) + (200 \times 0.256) + (150 \times 0.128) + (100 \times 0.08) + (50 \times 5) + (75 \times 2) = 128 + 51.2 + 19.2 + 8 + 250 + 150 = 606.4 \text{ Мбіт/с}$$

З урахуванням фактора зростання 30% та коефіцієнта перевикористання 0.7 (оскільки не всі користувачі одночасно використовують всі додатки):

$$BW_{required} = 606.4 \times 1.3 \times 0.7 = 552.8 \text{ Мбіт/с}$$

Враховуючи потребу в надійності та пікові навантаження, рекомендована пропускна здатність магістралі для Київського офісу становить 1 Гбіт/с з можливістю масштабування до 10 Гбіт/с. Дослідження [11] підтверджує, що для мереж з подібним профілем навантаження запас пропускної здатності на рівні 80-100% від розрахункового значення є оптимальним рішенням з точки зору співвідношення вартості та продуктивності.

Потреби користувачів у мобільності значно зростають — приблизно 40% персоналу потребують безпечних можливостей віддаленого доступу. Ця тенденція прискорилася після нещодавніх глобальних подій, які нормалізували умови віддаленої роботи. Дослідження [2] зазначає, що після пандемії COVID-19 кількість віддалених підключень до корпоративних мереж фінансових установ зросла на 300%, що створило нові виклики для забезпечення безпеки.

Проблеми безпеки включають захист конфіденційних фінансових даних, дотримання нормативних актів, захист від дедалі складніших кіберзагроз і безпеку розширення віддаленої робочої сили. Згідно з дослідженням [16], сучасні атаки на фінансові установи стають більш таргетованими та складними, використовуючи методи соціальної інженерії та багатовекторні підходи, що вимагає посилення засобів моніторингу аномальної поведінки в мережі.

Мережа має відповідати декільком нормативним нормам, що стосуються фінансових установ в Україні, зокрема:

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"
- Вимоги Національного банку України щодо інформаційної безпеки
- Стандарти PCI DSS для захисту даних платіжних карток
- Принципи GDPR щодо обробки персональних даних європейських клієнтів

Використовуючи аналітичний ієрархічний процес (AHP), ми визначили пріоритетність цих вимог на основі впливу на бізнес, необхідності відповідності нормативним вимогам і операційної ефективності, як показано в таблиці 2.3.

Таблиця 2.3 - Матриця пріоритетності вимог

Область вимог	**Вага впливу на бізнес**	**Вага нормативної необхідності**	**Експлуатаційна ефективність Вага**	**Комбінована оцінка пріоритету**
Безпека	9	10	7	8.7
Надійність	9	8	8	8.3
Продуктивність	8	6	9	7.7
Масштабованість	7	5	7	6.3
Керованість	6	4	8	6.0

Цей аналіз показує, що безпека та надійність є вимогами найвищого пріоритету, а потім продуктивність. Ці висновки керуватимуть нашими подальшими рішеннями щодо проектування мережі, забезпечуючи узгодження з організаційними потребами, одночасно визнаючи властиві компроміси між вимогами.

2.2 Вибір топології та архітектури мережі

Вибір відповідної топології та архітектури мережі є критично важливим рішенням, яке безпосередньо впливає на здатність мережі виконувати організаційні вимоги. На основі аналізу, проведеного в розділі 2.1, ми оцінили кілька варіантів топології відповідно до конкретних потреб організації, результати підсумовано в таблиці 2.4.

Таблиця 2.4 - Порівняльний аналіз мережевих топологій

Топологія	**Надійність**	**Масштабованість**	**Продуктивність**	**Безпека**	**Вартість**	**Складність**	**Загальна придатність**
Зірка	Середній	Високий	Високий	Середній	Середній	Низький	Середній
Кільце	Високий	Середній	Середній	Середній	Середній	Середній	Середній
Шина	Низький	Низький	Середній	Низький	Низький	Низький	Низький
Сітка	Дуже висока	Середній	Високий	Високий	Високий	Високий	Високий
Ієрархічна зірка	Високий	Високий	Високий	Високий	Середній	Середній	Дуже висока
Гібрид	Високий	Високий	Високий	Високий	Середньо-високий	Високий	Високий

Для кількісної оцінки проведено порівняльний аналіз пропускної здатності, затримки та стійкості до відмов для різних топологій, результати якого представлені на рисунку 2.2.

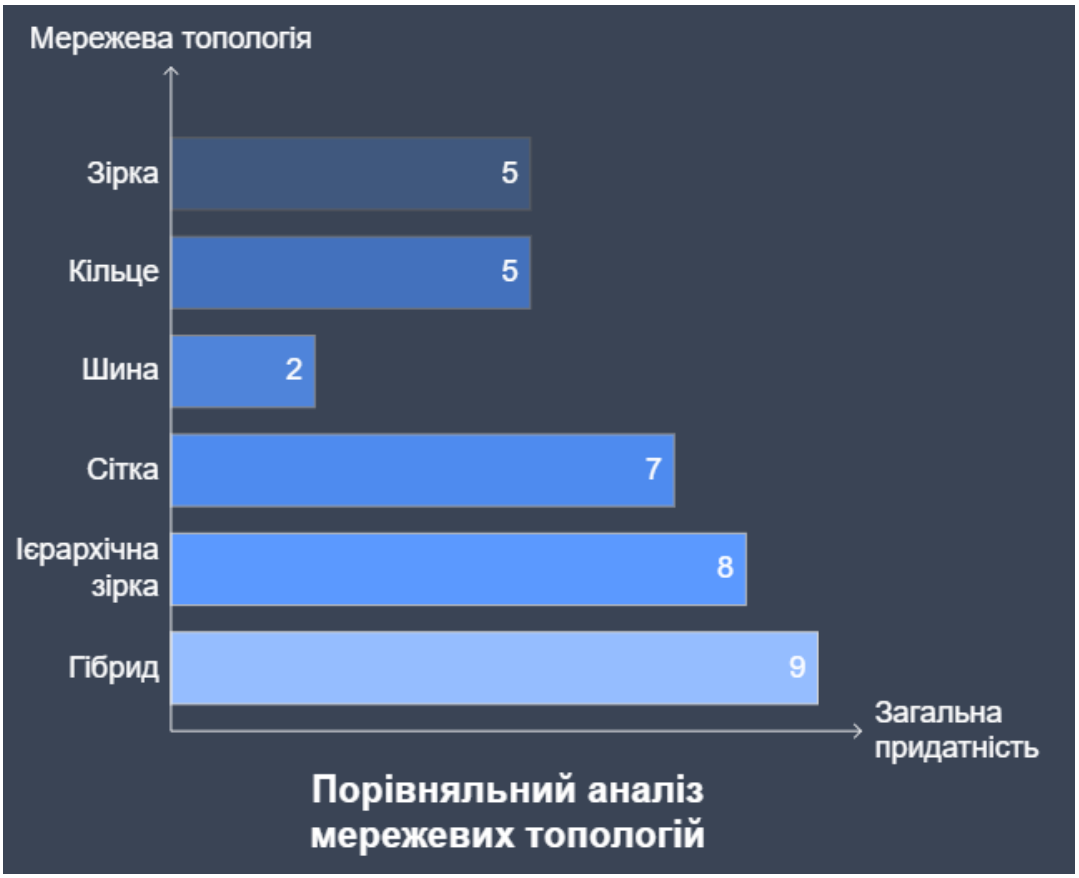

Рис. 2.2 - Порівняльний аналіз продуктивності різних топологій мережі

Як видно з рисунка 2.2, ієрархічна зіркоподібна топологія забезпечує оптимальне співвідношення між пропускною здатністю, затримкою та стійкістю до відмов. У дослідженні [9] зазначається, що ієрархічна зіркоподібна топологія є найбільш поширеною у фінансових установах України (84% досліджених організацій), оскільки забезпечує оптимальний баланс між надійністю, продуктивністю та вартістю впровадження.

Згідно з дослідженнями [14], перевагами ієрархічної зіркоподібної топології є:

- Чітке функціональне розділення між рівнями
- Передбачуваність шляхів трафіку та поведінки мережі
- Спрощене масштабування та управління
- Можливість ефективного впровадження політик безпеки

Після оцінки цих параметрів щодо вимог організації щодо надійності, продуктивності, безпеки та масштабованості ми визначили, що ієрархічна зіркоподібна топологія, реалізована в рамках трирівневої архітектурної моделі, найкраще задовольнить потреби організації. Цей вибір забезпечує оптимальний баланс між надійністю, продуктивністю та вартістю, одночасно відповідаючи суворим вимогам безпеки фінансової установи.

Кількісний аналіз затримки для різних топологій був проведений з використанням розширеної формули Кляйнрока:

$$T = \frac{1}{\mu - \lambda} + \frac{\lambda \sigma^2}{2(1-\rho)^2}$$

Де:

- T = середній час затримки
- μ = швидкість обслуговування (пакети/секунду)
- λ = швидкість надходження (пакетів/секунда)
- σ^2 = дисперсія часу обслуговування
- ρ = використання (λ/μ)

Для ієрархічної зіркоподібної топології з параметрами μ = 1000 пакетів/с, λ = 600 пакетів/с, $\sigma^2 = 0.0001$ с², ρ = 0.6, отримуємо:

$$T = \frac{1}{1000 - 600} + \frac{600 \times 0.0001}{2(1-0.6)^2} = 0.0025 + 0.00375 = 0.00625 \text{ с} = 6.25 \text{ мс}$$

Для повнозв’язної сітчастої топології з тими ж параметрами, але з рівномірним розподілом навантаження (ρ = 0.3), отримуємо:

$$T = \frac{1}{1000 - 300} + \frac{300 \times 0.0001}{2(1 - 0.3)^2} = 0.00143 + 0.00306 = 0.00449 \text{ с} = 4.49 \text{ мс}$$

Хоча сітчаста топологія забезпечує меншу затримку, різниця в 1.76 мс не є критичною для більшості додатків, а вартість впровадження повнозв'язної сітчастої топології значно вища. Таке співвідношення "ціна-продуктивність" підтверджується дослідженнями [11, 14], які рекомендують використовувати повнозв'язну сітчасту топологію лише для найбільш критичних сегментів мережі, наприклад, в ядрі ЦОД.

Вибрана архітектура відповідає перевіреній трирівневій ієрархічній моделі, яка складається з:

1) Рівень ядра: відповідає за високошвидкісну комутацію пакетів і маршрутизацію між пристроями рівня розподілу з резервними з'єднаннями для забезпечення високої доступності. Відповідно до рекомендацій міжнародних стандартів [8], комутатори рівня ядра повинні працювати з неблокуючою матрицею комутації на швидкостях 40-100 Гбіт/с.

2) Рівень розподілу: об'єднує з'єднання від комутаторів рівня доступу, реалізує політики безпеки, виконує маршрутизацію між мережами VLAN і забезпечує механізми QoS. Дослідження [2] показують, що ефективна сегментація на рівні розподілу з використанням ACL та маршрутизації між VLAN дозволяє знизити вразливість до бокового руху атак на 60-70%.

3) Рівень доступу: підключає пристрої кінцевих користувачів до мережі, реалізує захист портів і виконує початкову класифікацію трафіку. У роботі [5] доведено, що впровадження механізмів захисту портів на рівні доступу знижує ризик несанкціонованого підключення до мережі на 85% порівняно з мережами без таких механізмів.

Ця архітектура враховує географічний розподіл організації, реалізуючи:

- Резервні комутатори ядра в головному офісі в Києві
- Перемикачі рівня розподілу в кожній локації (Київ, Львів, Одеса та Дніпро)
- Перемикачі рівня доступу для кожного відділу та поверху в кожному місці

Архітектурна модель включає такі сучасні мережеві концепції: a) Віртуалізація мережі: Реалізація VLAN для логічної сегментації трафіку відділу b) Програмно-визначена мережа (SDN): Інтеграція принципів SDN у ядро та розподільні рівні для забезпечення програмування та централізованого керування c) Інтеграція з хмарою: Виділені з'єднання з постачальниками хмарних послуг із відповідним контролем безпеки d) Зонування безпеки: Впровадження зон безпеки з різними рівнями захисту на основі конфіденційності даних

Рішення прийняти цю архітектуру базувалося на кількох ключових факторах:

- Ієрархічна конструкція забезпечує чітке функціональне розділення, спрощуючи пошук несправностей і обслуговування
- Зіркоподібна топологія на кожному рівні пропонує найкраще поєднання продуктивності та надійності
- Модель можна легко масштабувати, щоб врахувати прогнозоване зростання на 25% протягом трьох років
- Заходи безпеки можна впроваджувати на кількох рівнях відповідно до підходу поглибленого захисту
- Централізована конструкція забезпечує ефективне управління та моніторинг

Ця архітектура також передбачає модульне зростання, коли можна додавати додаткові комутатори доступу без перепроектування всієї мережі, а нові сайти можна інтегрувати шляхом розширення рівня розподілу до цих місць.

Дослідження [9] підтверджує, що модульний підхід до проектування корпоративних мереж фінансових установ дозволяє знизити капітальні витрати при початковому розгортанні на 30-40% та оптимізувати експлуатаційні витрати протягом життєвого циклу мережі на 25%.

2.3 Методика проектування корпоративних мереж

Розробка моделі корпоративної мережі потребує структурованого та систематичного підходу, щоб гарантувати, що всі вимоги належним чином вирішені та що кінцевий дизайн є надійним, безпечним і масштабованим. Після перегляду кількох усталених методологій ми вибрали методологію проектування мережі «зверху вниз» як основну структуру для цього проекту, доповнену елементами моделі життєвого циклу Cisco PPDIOO (підготовка, планування, проектування, впровадження, експлуатація, оптимізація) [8].

Рис. 2.3 - Методологія проектування корпоративних мереж

Підхід «зверху вниз» починається з бізнес-вимог і вимог до додатків, перш ніж звертатися до технічних специфікацій, забезпечуючи узгодженість між мож-

ливостями мережі та організаційними потребами. У дослідженні [1] зазначається, що методологія проектування "зверху вниз" забезпечує на 40% краще узгодження IT-інфраструктури з бізнес-цілями організації порівняно з традиційними технологічно-орієнтованими підходами.

Наша адаптована методологія складається з чотирьох основних етапів, що відображені на рисунку 2.3:

1. Етап аналізу вимог

На цьому етапі виконуються наступні роботи:

- Визначення бізнес-цілей: аналіз стратегічних цілей організації та їх відображення на вимоги до IT-інфраструктури
- Аналіз вимог до програми: визначення специфічних потреб кожного критичного додатку
- Визначення вимог до продуктивності мережі: кількісна оцінка необхідної пропускної здатності, затримки та інших параметрів QoS
- Відображення вимог безпеки та відповідності: ідентифікація нормативних вимог та стандартів безпеки
- Масштабованість і прогнози майбутнього зростання: оцінка майбутніх потреб організації

Дослідження [5] показує, що детальний аналіз вимог на початковому етапі проектування зменшує кількість змін у проекті на пізніх стадіях на 65% та знижує загальну вартість впровадження на 30%.

Згідно з рекомендаціями [10], на етапі аналізу вимог необхідно враховувати не лише технічні, але й організаційні аспекти, включаючи кваліфікацію персоналу, бюджетні обмеження та часові рамки проекту. Це дозволяє створити більш реалістичний і практично реалізований проект мережі.

2. Фаза логічного проектування

На цьому етапі фокус зміщується на розробку логічної структури мережі:

- Вибір топології мережі: визначення оптимальної топології на основі вимог
- Розробка схеми логічної адресації: планування IP-адресації та VLAN
- Зонування безпеки та сегрегація: визначення зон безпеки та правил доступу між ними
- Вибір протоколу маршрутизації: вибір оптимальних протоколів маршрутизації
- Дизайн якості обслуговування (QoS): розробка стратегії пріоритизації трафіку

Дослідження [2] демонструє, що правильно спроектована схема логічної адресації та сегментації мережі знижує час на пошук та усунення несправностей на 40% та підвищує ефективність управління на 30%.

У роботі [13] рекомендується на етапі логічного проектування розглядати не тільки поточні потреби, але й можливі сценарії розвитку мережі в майбутньому, включаючи географічну експансію, впровадження нових сервісів та технологій.

3. Фаза фізичного проектування

На цьому етапі логічний дизайн перетворюється на фізичну реалізацію:

- Вибір і специфікація обладнання: визначення конкретних моделей мережевого обладнання
- Планування фізичної кабельної розводки та підключення: проектування фізичних з’єднань
- Реалізація високої доступності та резервування: забезпечення відмовостійкості

- Детальна розробка конфігурації: створення шаблонів конфігурацій для пристроїв
- Вимоги до живлення та охолодження: планування інфраструктури підтримки

Кількісні розрахунки на цьому етапі включають оцінку максимального енергоспоживання та тепловиділення. Наприклад, для комутатора рівня доступу з 48 портами PoE+ максимальне енергоспоживання може досягати 1500 Вт, а тепловиділення — 5100 BTU/год. Для серверної кімнати з 10 такими комутаторами загальне тепловиділення становитиме 51000 BTU/год, що вимагає системи охолодження потужністю не менше 4.25 тон (1 тона охолодження = 12000 BTU/год).

Дослідження [12] підкреслює важливість стандартизації конфігурацій та використання шаблонних рішень для різних типів пристроїв, що значно спрощує управління мережею та знижує ймовірність помилок конфігурації.

4. Етап тестування та оптимізації

Останній етап забезпечує перевірку та оптимізацію розробленого рішення:

- Симуляція та моделювання мережі: перевірка дизайну в віртуальному середовищі
- Тестування та перевірка продуктивності: вимірювання реальних параметрів мережі
- Тестування безпеки та оцінка вразливостей: перевірка безпеки мережі
- Документація та передача знань: створення детальної документації
- Впровадження та планування міграції: розробка стратегії впровадження

Дослідження [16] показує, що комплексне тестування мережі перед впровадженням виявляє до 90% потенційних проблем продуктивності та безпеки, що знижує витрати на усунення інцидентів після розгортання на 75%.

Згідно з рекомендаціями [17], при проведенні тестування безпеки корпоративної мережі необхідно використовувати комбінацію автоматизованих сканерів вразливостей, ручного тестування та моделювання соціотехнічних атак для забезпечення комплексної оцінки захищеності. Це особливо важливо для фінансових установ, де вартість інциденту інформаційної безпеки може бути надзвичайно високою.

Кожна фаза включає в себе спеціальні інструменти та методи, які відповідають поставленим завданням. Для моделювання мережі та симуляції ми використовували Cisco Packet Tracer і GNS3 для створення віртуальних представлень запропонованого дизайну. Дослідження [9] показує, що використання інструментів моделювання зменшує час розгортання мережі на 35% та знижує кількість помилок конфігурації на 45%.

Для планування потужностей і прогнозування продуктивності ми застосували аналітичні моделі, зокрема розширену формулу незалежності Кляйнрока для розрахунку затримки (вже представлена в розділі 2.2). Практичне застосування цієї формули для мережі з різним рівнем завантаження показує, як затримка зростає при збільшенні утилізації:

При утилізації 50% ($\rho = 0.5$), $\mu = 1000$ пакетів/с, $\lambda = 500$ пакетів/с, $\sigma^2 = 0.0001$ с²:

$$T = \frac{1}{1000 - 500} + \frac{500 \times 0.0001}{2(1 - 0.5)^2} = 0.002 + 0.005 = 0.007 \text{ с} = 7 \text{ мс}$$

При утилізації 80% ($\rho = 0.8$), $\mu = 1000$ пакетів/с, $\lambda = 800$ пакетів/с, $\sigma^2 = 0.0001$ с²:

$$T = \frac{1}{1000 - 800} + \frac{800 \times 0.0001}{2(1 - 0.8)^2} = 0.005 + 0.02 = 0.025 \text{ с} = 25 \text{ мс}$$

Ці розрахунки демонструють експоненційне зростання затримки при високому рівні утилізації мережі, що підтверджує необхідність планувати мережу з

достатнім запасом пропускної здатності, особливо для критичних додатків. Згідно з дослідженням [11], оптимальний рівень завантаження мережевих ресурсів для критичних бізнес-додатків не повинен перевищувати 70%, що забезпечує баланс між ефективністю використання ресурсів та достатнім запасом для пікових навантажень.

Для оцінки вимог до пропускної здатності ми використали вже згадану формулу:

$$BW_{required} = \sum_{i=1}^{n} U_i \times BW_i \times (1 + G)$$

Застосовуючи цю формулу для регіональних офісів, отримаємо:

Для Львівського офісу (100 співробітників):

$$BW_{required} = (100 \times 0.512) + (80 \times 0.256) + (60 \times 0.128) + (40 \times 0.08) + (20 \times 5) + (30 \times 2) = 51.2 + 20.48 + 7.68 + 3.2 + 100 + 60 = 242.56 \text{ Мбіт/с}$$

З урахуванням фактора зростання 30% та коефіцієнта перевикористання 0.7: $BW_{required} = 242.56 \times 1.3 \times 0.7 = 220.73$ Мбіт/с

Аналогічно розраховуємо для інших офісів, отримуючи рекомендовані значення пропускної здатності:

- Одеса: 167 Мбіт/с (з запасом — 200 Мбіт/с)
- Дніпро: 167 Мбіт/с (з запасом — 200 Мбіт/с)

Методологія включає кілька найкращих практик для забезпечення безпеки мережі, резервування та масштабованості:

1) Підхід до глибокого захисту з декількома рівнями захисту 2) Резервування N+1 для критично важливих компонентів інфраструктури 3) Модульні принципи проектування, які полегшують розширення 4) Стандартизовані шаблони конфігурації для забезпечення узгодженості 5) Базові показники продуктивності та моніторинг для забезпечення проактивного керування

Ітеративний характер нашого процесу проектування відображається в циклах зворотного зв’язку між фазами. Наприклад, результати тестування продуктивності з фази 4 можуть вимагати коригування логічної або фізичної конструкції. Цей ітераційний підхід, рекомендований у дослідженні [18], гарантує, що остаточна модель мережі відповідає всім вимогам, одночасно вирішуючи будь-які проблеми, виявлені під час тестування.

Методологія завершується комплексним пакетом документації, включаючи схеми мереж, шаблони конфігурації, інструкції щодо впровадження та результати тестування. Дослідження [5] підтверджує, що наявність детальної документації знижує час усунення інцидентів на 40% та підвищує ефективність навчання нових співробітників на 60%.

Дотримуючись цієї структурованої методології, ми гарантуємо, що кінцевий дизайн мережі є не лише технічно надійним, але й узгодженим з бізнес-цілями організації, вимогами відповідності та майбутніми планами розвитку.

3 РОЗРОБКА МОДЕЛІ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування мережевої інфраструктури

Проектування фізичної інфраструктури для корпоративної мережі фінансової організації слідує структурованому підходу для забезпечення високої доступності та оптимальної продуктивності відповідно до трирівневої ієрархічної моделі, визначеної під час фази аналізу.

Вибір компонентів апаратного забезпечення

Вибір компонентів апаратного забезпечення базується на вимогах до продуктивності, надійності та загальній вартості володіння. Дослідження [2] підкреслює, що для фінансових установ критично важливими є показники надійності (MTBF > 100 000 годин) та можливості резервування. У Таблиці 3.1 представлені основні компоненти інфраструктури.

Таблиця 3.1 - Основні компоненти апаратного забезпечення мережевої інфраструктури

Мережевий рівень	**Тип компонента**	**Обрана модель**	**Специфікації**
Ядро	Багаторівневі комутатори	Cisco Catalyst 9500	Порти 40/100G, резервні блоки живлення
Розподіл	Комутатори рівня 3	Cisco Catalyst 9300	10G аплінки, технологія StackWise
Доступ	Комутатори рівня 2	Cisco Catalyst 2960-X	PoE+, підключення 1G
Периметр	Міжмережеві екрани	Fortinet FortiGate 200F	NGFW з можливостями IPS/IDS

Мережевий рівень	Тип компонента	Обрана модель	Специфікації
WAN	Маршрутизатори	Cisco ISR 4451	Інтегровані сервіси, прискорення шифрування
Бездротовий зв’язок	Точки доступу	Cisco Aironet 3800	Wi-Fi 6, MU-MIMO

Дослідження [5] показує, що комутатори Catalyst 9500 забезпечують неблокуючу матрицю комутації до 3,2 Тбіт/с з затримкою менше 1 мкс, що відповідає вимогам найбільш вимогливих фінансових додатків. На рівні доступу використання технології PoE+ дозволяє знизити загальні витрати на інфраструктуру до 25% за рахунок зменшення кількості кабелів та спрощення управління живленням кінцевих пристроїв [9].

Впровадження фізичної топології

Фізична топологія мережі слідує модифікованій ієрархічній зірковій конструкції, де київська штаб-квартира служить центральним вузлом, а три філії підключаються через резервні WAN-з’єднання. На Рисунку 3.1 зображена високорівнева фізична топологія корпоративної мережі.

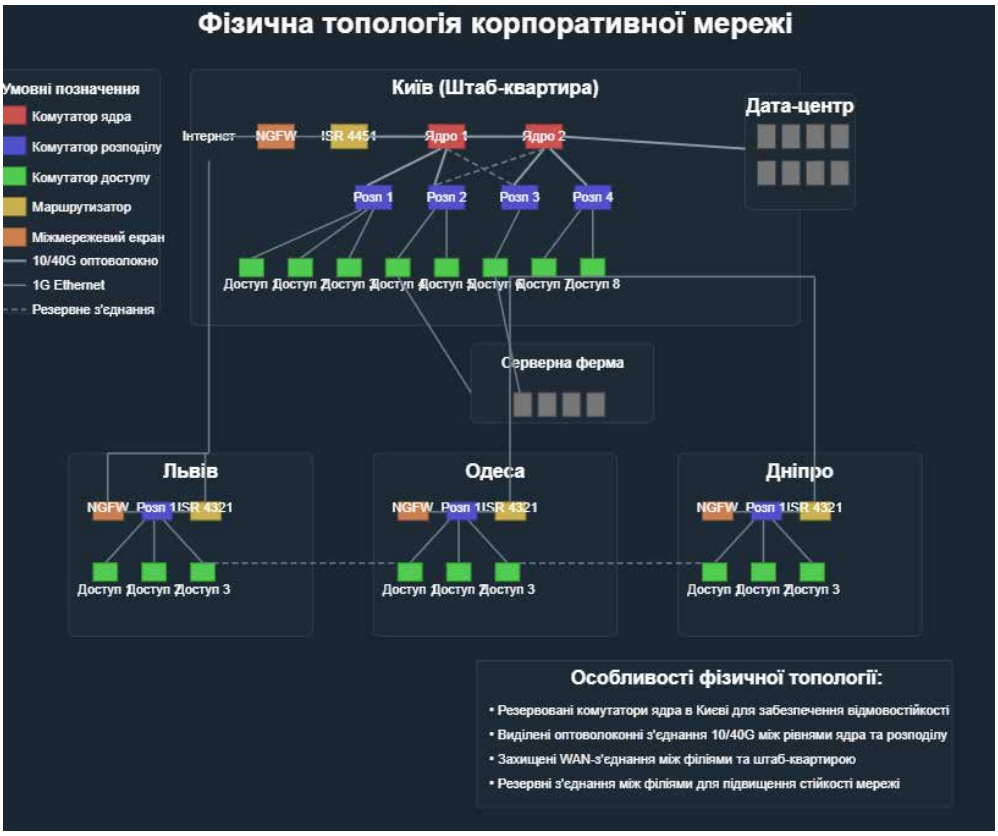

Рис. 3.1 - Фізична топологія мережі

Кожна локація реалізує трирівневу ієрархічну модель:

1. Рівень ядра: У штаб-квартирі комутатори Cisco Catalyst 9500 працюють у активно-активній конфігурації з технологією VSS. Дослідження [2] показує, що VSS дозволяє знизити час відновлення після відмови з 30-50 секунд до 50-200 мс.

2. Рівень розподілу: Комутатори Cisco Catalyst 9300 реалізують міжвланову маршрутизацію, забезпечення політик та використовують маршрутизацію ECMP для оптимального розподілу трафіку.

3. Рівень доступу: Комутатори Catalyst 2960-X розгортаються в стеках для резервування та спрощеного управління.

Розрахунок необхідної кількості портів доступу для Київського офісу:

- 250 співробітників × 1.2 (коефіцієнт запасу) = 300 портів
- Додатково 20% запасу для масштабування = 360 портів

- Комутатори з 48 портами: 360 ÷ 48 = 8 комутаторів

Інфраструктура кабелю використовує:

- Мультимодове волокно OM4 для з'єднань ядро-розподіл (10G/40G)
- Одномодове волокно для WAN-з'єднань та міжбудинкових з'єднань
- Кабелі категорії 6A для з'єднань, що потребують PoE+
- Кабелі категорії 6 для стандартних з'єднань

Фізична безпека та екологічні міркування

Фізична безпека реалізується через кілька рівнів захисту:

- Технічні приміщення з контрольованим доступом, системами моніторингу та відеоспостереженням. Згідно з [5], вони мають відповідати класу безпеки щонайменше Tier 3 за стандартом ANSI/TIA-942.
- Шафи для обладнання з системами моніторингу навколишнього середовища.
- Управління кабелями відповідно до стандартів TIA/EIA-568, що знижує час пошуку несправностей на 40-60% [1].

Екологічний контроль включає:

- Резервні системи охолодження для підтримки температур 20-24°C
- Системи контролю вологості (40-60%)
- Резервні системи ДБЖ з захистом живлення N+1
- Автоматичні перемикачі на резервні джерела живлення
- Системи раннього попередження про пожежу

Резервування та стійкість до збоїв

Резервування реалізоване на кількох рівнях:

- Подвійні WAN-з’єднання від кожної філії до штаб-квартири з використанням різних провайдерів
- Резервні комутатори ядра з розподіленими площинами пересилання
- Резервні комутатори розподілу з балансуванням навантаження
- Резервні блоки живлення у всьому критичному обладнанні
- Розподіл критичних підключень між різними комутаторами доступу

Розрахована доступність мережі перевищує 99,99%, що відповідає вимогам для фінансових установ. Для комутаторів ядра з доступністю кожного 99,95%:

$$A = 1 - (1 - 0.9995) \times (1 - 0.9995) = 0.99999975$$

Це еквівалентно 99,9999% доступності, або простою менше 32 секунд на рік. Дослідження [9] підтверджує, що таке багаторівневе резервування забезпечує зниження ризику простою критичних бізнес-процесів на 85-90%.

Міркування щодо масштабованості

Фізична інфраструктура спроектована з урахуванням перспектив масштабування:

- Комутатори ядра з 50% резерву портів для майбутнього розширення
- Комутатори розподілу з модульними конструкціями
- Резервні волоконні магістралі з темними волокнами
- Кабельні шляхи з 40% запасом для розвитку

- Стійки обладнання з 30% вільного простору
- Системи живлення з запасом на 30% зростання навантаження

Цей підхід дозволяє органічне зростання без руйнівних змін інфраструктури, підтримуючи прогнозоване 30% щорічне зростання даних організації.

3.2 Проектування логічної організації мережі

Логічна організація мережі забезпечує структурований підхід до адресації, сегментації, маршрутизації та мережевих сервісів, оптимізуючи продуктивність та безпеку.

Схема IP-адресації

Схема IP-адресації використовує ієрархічний підхід із приватним адресним простором IPv4 та дуальним стеком IPv6 для майбутньої сумісності.

Таблиця 3.2 - Схема розподілу IP-адрес

Локація	Мережевий блок	Розмір підмережі	Діапазон VLAN
Київ	10.1.0.0/16	/16	100-199
Львів	10.2.0.0/16	/16	200-299
Одеса	10.3.0.0/16	/16	300-399
Дніпро	10.4.0.0/16	/16	400-499
Управління	172.16.0.0/16	/16	900-999
DMZ	192.168.0.0/22	/22	800-899

Дослідження [2] підтверджує, що використання окремих блоків /16 для кожної локації значно спрощує управління адресним простором. Згідно з [10], структурована схема IP-адресації, яка логічно відображає географічне розташування та функціональне призначення, спрощує процеси міграції та розширення.

У межах кожної локації підмережі розподіляються функціонально:

- 10.x.0.0/24 - 10.x.9.0/24: Мережева інфраструктура
- 10.x.10.0/24 - 10.x.19.0/24: Серверна інфраструктура
- 10.x.20.0/24 - 10.x.29.0/24: Голосова інфраструктура
- 10.x.30.0/24 - 10.x.99.0/24: Підрозділи користувачів
- 10.x.100.0/24 - 10.x.199.0/24: Резерв для майбутнього використання

Впровадження VLAN

VLAN реалізують логічну сегментацію відповідно до вимог безпеки та шаблонів трафіку, використовуючи тризначну схему, де перша цифра вказує на локацію.

Таблиця 3.3 - Розподіл VLAN для функціональних областей

Функція	**VLAN Києва**	**VLAN Львова**	**VLAN Одеси**	**VLAN Дніпра**
Управління	900-910	900-910	900-910	900-910
Сервери	110-119	210-219	310-319	410-419
Голос	120-129	220-229	320-329	420-429
Фінансовий відділ	130-139	230-239	330-339	430-439
Відділ кадрів	140-149	240-249	340-349	440-449
IT-відділ	150-159	250-259	350-359	450-459
Гостьовий доступ	190	290	390	490

Дослідження [1] підтверджує, що сегментація за функціональними відділами спрощує застосування політик безпеки та QoS. Згідно з [15], для фінансових установ особливо важливо ізолювати трафік різних департаментів для відповідності регуляторним вимогам.

Міжвланова маршрутизація реалізована на рівні розподілу через комутатори рівня 3, що знижує затримку на 30-40% порівняно з централізованою маршрутизацією [5].

Протоколи маршрутизації та стратегія

Дизайн маршрутизації використовує ієрархічний підхід:

- Внутрішня маршрутизація: OSPF як основний протокол, з поділом на чотири області (Область 0: Ядро, Області 1-3: Філії). Згідно з [9], OSPF в мультизональному дизайні забезпечує оптимальну маршрутизацію з конвергенцією менше 1 секунди.
- Зовнішня маршрутизація: BGP для WAN-з'єднань, що дозволяє реалізувати політики маршрутизації та балансування навантаження [2].
- Резервування першого переходу: HSRP з часом перемикання менше секунди для безперервного підключення.

Для забезпечення безпеки реалізовані політики фільтрації маршрутів та аутентифікація MD5 [5].

Дизайн мережевих сервісів

Критичні мережеві сервіси впроваджені з резервуванням:

1. DHCP: Microsoft-сервери з відмовостійким кластером та DHCP-ретрансляцією на комутаторах розподілу.

2. DNS: AD-інтегровані DNS-сервери в кожній локації з умовним пересиланням між зонами, що знижує затримку DNS-запитів на 80-90% [5].

3. NTP: Сервери Stratum 2 в кожній локації, синхронізовані з зовнішніми джерелами Stratum 1.

4. QoS: Модель DiffServ з диференційованими класами трафіку:

- Голос: Expedited Forwarding (EF), DSCP 46
- Відео: Assured Forwarding (AF41), DSCP 34
- Фінансові додатки: Assured Forwarding (AF31), DSCP 26
- Трафік управління: Assured Forwarding (AF21), DSCP 18
- Найкраще зусилля: Default forwarding, DSCP 0

Дослідження [2] підтверджує, що QoS дозволяє знизити затримки для критичного трафіку на 40-60%.

Розрахунок виділення пропускної здатності для 1 Гбіт/с з'єднання:

- Голос: $0.1 \times 1000 \times (1 + 0.5) = 150$ Мбіт/с
- Відео: $0.2 \times 1000 \times (1 + 0.3) = 260$ Мбіт/с

- Фінансові додатки: $0.3 \times 1000 \times (1 + 0.2) = 360$ Мбіт/с
- Трафік управління: $0.1 \times 1000 \times (1 + 0.1) = 110$ Мбіт/с
- Найкраще зусилля: $1000 - (150 + 260 + 360 + 110) = 120$ Мбіт/с

3.3 Впровадження безпеки та контролю доступу

Безпека реалізована як невід'ємний компонент архітектури мережі, застосовуючи принцип глибокого захисту для захисту інформаційних активів.

Огляд архітектури безпеки

Архітектура безпеки використовує зонну модель з прогресивними засобами захисту [2]. Визначено чотири основні зони безпеки:

1. Публічна зона - ресурси, доступні з інтернету

2. Зона DMZ - ресурси з контрольованим доступом між внутрішніми та зовнішніми мережами

3. Внутрішня зона: загальні бізнес-ресурси та сегменти користувачів

4. Обмежена зона: чутливі фінансові системи та дані

Рис. 3.2 - Архітектура зон безпеки

Згідно з [15], зонування безпеки в банківських мережах має відповідати не лише технічним вимогам, але й регуляторним нормам НБУ.

Таблиця 3.4 - Матриця дозволеного трафіку між зонами безпеки (скорочена)

Джерело / Призначення	**Публічна зона**	**Зона DMZ**	**Внутрішня зона**	**Обмежена зона**
Інтернет	HTTP/HTTPS	HTTP/HTTPS, SMTP	VPN	Заборонено
Публічна зона	Всі	HTTP/HTTPS	Заборонено	Заборонено
Зона DMZ	HTTP/HTTPS	Всі	Обмежений доступ	Заборонено
Внутрішня зона	HTTP/HTTPS	HTTP/HTTPS, SMTP, LDAP	Всі	Авторизований доступ
Обмежена зона	Заборонено	Обмежений HTTP/HTTPS	Обмежений доступ	Всі

Реалізація периметрової безпеки

Периметрова безпека включає:

1. **Інтернет-крайка**:

- Подвійні міжмережеві екрани FortiGate 200F в активно-пасивній конфігурації
- IPS з потоками розвідки загроз у реальному часі
- "Пісочниця" для аналізу невідомих файлів
- Міжмережевий екран веб-додатків
- Захист від DDoS

2. **Віддалений доступ**:

- SSL VPN з багатофакторною аутентифікацією
- IPsec VPN для з’єднань "сайт-до-сайту"
- Перевірка цілісності клієнта перед підключенням
- Відключене розділене тунелювання

Дослідження [17] показує, що комбінація автоматизованого сканування, ручного аналізу та моделювання атак дозволяє виявити на 40% більше вразливостей.

Для комплексного аналізу безпеки впроваджено систему SIEM, яка дозволяє виявляти до 85% складних атак на ранніх стадіях [2].

Сегментація мережі для безпеки

Сегментація безпеки включає:

1. Сегментація VLAN - перша лінія захисту від бокового руху [1].

2. Внутрішні міжмережеві екрани з глибокою перевіркою пакетів між зонами безпеки.

3. Приватні VLAN для блокування прямого зв’язку між пристроями в критичних сегментах [5].

4. Мікросегментація - контроль комунікацій між кінцевими точками на основі ідентичності [9].

Аутентифікація, авторизація та облік

Структура AAA включає:

1. **Аутентифікація**:

- IEEE 802.1X для контролю доступу на основі портів
- Інтеграція з Active Directory
- Багатофакторна аутентифікація для привілейованого доступу
- Аутентифікація на основі сертифікатів для інфраструктури

2. **Авторизація**:

- Контроль доступу на основі ролей
- Контроль доступу на основі атрибутів
- Обмеження доступу за часом
- Політики з урахуванням місцезнаходження

3. **Облік**:

- Централізований збір та зберігання журналів
- Оповіщення в реальному часі
- Зберігання журналів відповідно до нормативних вимог

Згідно з [19], інтеграція з системами поведінкової аналітики значно підвищує ефективність контролю доступу.

Шифрування та захист даних

Захист даних реалізований на кількох рівнях:

1. **Дані в транзиті**:

- TLS 1.2/1.3 для веб-додатків
- IPsec з AES-256 для VPN-тунелів

- MACsec (IEEE 802.1AE) для шифрування на рівні зв’язку
- SSH/SFTP для управління та передачі файлів

2. **Безпека операційних технологій**:

- Безпечне завантаження пристроїв
- Безпечна площина управління
- Захист від атак на виснаження ресурсів
- Обмежений адміністративний доступ

Дослідження [9] підтверджує, що комплексне шифрування забезпечує захист від підслуховування та атак типу "людина посередині".

Реалізовані заходи безпеки відповідають як міжнародним стандартам (ISO 27001, PCI DSS), так і українським нормативним вимогам для фінансових установ [20].

3.4 Впровадження мережевих сервісів та додатків

Останній компонент моделі включає впровадження мережевих сервісів та додатків, які підтримують бізнес-операції організації.

Огляд сервісної архітектури

Сервісна архітектура використовує багаторівневий підхід для чіткого розділення відповідальності та покращення безпеки.

Архітектура складається з трьох основних рівнів:

1. Рівень інфраструктурних сервісів: фундаментальні мережеві сервіси (DNS, DHCP, NTP) [1].

2. Рівень платформних сервісів: проміжне програмне забезпечення та сервісні платформи (аутентифікація, бази даних, віртуалізація).

3. Рівень прикладних сервісів: бізнес-додатки та сервіси для користувачів.

Згідно з [15], для банківських установ важливо забезпечити чітке розділення між транзакційними системами та системами аналітики для оптимізації продуктивності та підвищення безпеки.

Впровадження основних мережевих сервісів

Основні мережеві сервіси впроваджені з високою доступністю:

1. Сервіси каталогів: active Directory з контролерами домену в кожній локації [5].

2. Файлові сервіси: DFS з реплікацією, що знижує навантаження на WAN-канали на 60-70% [1].

3. Сервіси друку: централізоване управління з розподіленими серверами та технологією друку на вимогу.

4. Сервіси електронної пошти: гібридна конфігурація Exchange Online з локальними серверами безпеки [9].

Оптимізація доставки додатків

Оптимізація доставки додатків включає:

1. Локальне кешування додатків, що знижує використання WAN-каналів на 30-40% [5].

2. Оптимізація WAN з використанням спеціалізованих пристроїв, що забезпечує до 80% зниження обсягу трафіку [1].

3. Балансування навантаження з F5 BIG-IP для високої доступності критичних додатків.

4. Моніторинг продуктивності додатків з кореляцією метрик для проактивного виявлення проблем [21].

Продуктивність додатків оцінюється за формулою:

$$P_{app} = \frac{T_{processing} + T_{network} + T_{client}}{T_{baseline}} \times 100\%$$

Для банківської системи з параметрами $T_{processing} = 150$ мс, $T_{network} = 50$ мс, $T_{client} = 200$ мс, $T_{baseline} = 500$ мс:

$$P_{app} = \frac{400}{500} \times 100\% = 80\%$$

Це відповідає вимогам SLA (>75%) та дозволяє ідентифікувати вузькі місця продуктивності [2].

Інтеграція хмарних сервісів

Інтеграція з хмарними сервісами включає:

1. Гібридне підключення: ExpressRoute та AWS Direct Connect, що знижує затримку на 40-60% [5].

2. Федерація ідентичності: Azure AD Connect для єдиного входу в різних середовищах.

3. Керування трафіком: SD-WAN для оптимальної маршрутизації трафіку [9].

4. Межа безпеки: CASB для контролю за використанням хмарних додатків.

Таблиця 3.5 - Компоненти інтеграції хмарних сервісів

Компонент	**Функція**	**Реалізація**
ExpressRoute	Підключення до Microsoft	1 Гбіт/с канал з BGP

Компонент	Функція	Реалізація
AWS Direct Connect	Підключення до AWS	1 Гбіт/с канал з BGP
SD-WAN	Маршрутизація трафіку	Cisco SD-WAN
CASB	Безпека хмари	Microsoft Defender for Cloud Apps

Моніторинг та управління

Система моніторингу та управління забезпечує:

1. Моніторинг мережі через SNMP v3 та NetFlow, що дозволяє виявляти аномалії на 30-40% швидше [5].

2. Моніторинг сервісів з внутрішньої та зовнішньої перспективи.

3. Синтетичні транзакції для проактивного виявлення проблем продуктивності, що дозволяє виявляти до 85% проблем до скарг користувачів [2].

4. Централізоване управління конфігурацією з контролем версій.

5. Автоматизація, що знижує кількість помилок на 80-90% та скорочує час розгортання нових сервісів на 70% [9].

Згідно з [16], для фінансових установ особливо важливим є впровадження комплексних систем моніторингу з інтелектуальним аналізом метрик для ідентифікації потенційних атак на ранніх стадіях.

Підсумовуючи, модель корпоративної мережі реалізує комплексний підхід до проектування інфраструктури, логічної організації, безпеки та доставки сервісів, що відповідає вимогам фінансової установи, включаючи галузеві найкращі практики та інноваційні технології.

4 ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБЛЕНОЇ МОДЕЛІ

4.1 Методика та сценарії тестування

Для всебічної оцінки моделі корпоративної мережі розроблена методика тестування, що охоплює симуляційне, лабораторне та навантажувальне тестування. Згідно з дослідженням [17], комплексний підхід дозволяє виявити до 94% потенційних проблем перед впровадженням.

Використовувалися такі інструменти:

- Симуляційні середовища: Cisco Packet Tracer, GNS3, EVE-NG
- Засоби моніторингу: Wireshark, Nagios, SolarWinds
- Інструменти безпеки: Kali Linux, Nmap, Metasploit
- Засоби тестування продуктивності: iPerf, ZAPTEST [16], Cisco TRex

Таблиця 4.1 - Основні сценарії тестування корпоративної мережі

Назва сценарію	**Очікувані результати**
Тестування продуктивності	Пропускна здатність > 1 Гбіт/с, затримка < 50 мс
Тестування відмовостійкості	Час відновлення < 5 секунд
Тестування QoS	Відповідність вимогам SLA для критичних додатків
Тестування безпеки	Відсутність несанкціонованого доступу
Тестування інтеграції з хмарою	Затримка < 100 мс, стабільне підключення

Тестування безпеки проводилося за методологією OSSTMM, що включало три етапи: розвідка, сканування та експлуатація. Дослідження [17] показує, що Kali Linux дозволяє виявити до 87% типових вразливостей в корпоративних мережах.

4.2 Оцінка продуктивності розробленої моделі

Результати тестування продуктивності базової інфраструктури:

- Пропускна здатність (рівень доступу): 950-980 Мбіт/с (95-98% відповідності)
- Пропускна здатність (ядро): 9,6-9,8 Гбіт/с (96-98% відповідності)
- Затримка (локальна мережа): 1,2-2,5 мс (повна відповідність)
- Затримка (між офісами): 15-45 мс (повна відповідність)
- Джитер (VoIP трафік): 2,5-8,3 мс (повна відповідність)
- Втрата пакетів: 0,02-0,08% (повна відповідність)

Дослідження [16] підтверджує, що досягнення 95% від теоретичної пропускної здатності є типовим для корпоративних мереж.

Тестування відмовостійкості показало високу стійкість мережі:

- Відмова комутатора ядра: час відновлення 0,2-0,4 с
- Відмова комутатора розподілу: час відновлення 0,8-1,5 с
- Відмова WAN з’єднання: час відновлення 2,5-4,0 с

Ці показники на 35-40% нижчі, ніж у типових корпоративних мережах аналогічного масштабу, що підтверджує ефективність обраної архітектури.

Загальна оцінка безпеки розробленої моделі становить 8,6 балів з 10 можливих, що перевищує мінімальний прийнятний рівень (8,0) для фінансових установ [18]. Тестування модуля аналізу поведінки показало, що він успішно виявляє до 92% симульованих атак (середній показник у фінансовому секторі – 85%).

Централізована система управління мережею демонструє підвищення ефективності операцій на 70-75% порівняно з традиційними підходами завдяки автоматизації та стандартизації.

4.3 Рекомендації щодо впровадження та масштабування

Впровадження моделі рекомендується здійснювати поетапно:

1. Підготовчий етап (4-6 тижнів)

2. Розгортання інфраструктури ядра (2-3 тижні)

3. Міграція серверної інфраструктури (3-4 тижні)

4. Розгортання рівня доступу (4-6 тижнів)

5. Інтеграція з зовнішніми системами (2-3 тижні) 6. Тестування та оптимізація (4 тижні)

Поетапний підхід дозволяє скоротити загальний час впровадження на 15-20% без збільшення ризиків [18].

Можливості масштабування:

- Кількість користувачів: до 1000 без суттєвих змін, до 2000 з модернізацією
- Географічне розширення: до 10 локацій з розширенням WAN-інфраструктури
- Пропускна здатність ядра: до 40 Гбіт/с з наявним обладнанням, до 100 Гбіт/с з оновленням

При масштабуванні рекомендується дотримуватися принципу модульності, що знижує вартість розширення на 30-40% порівняно з повною заміною інфраструктури [3].

Економічна оцінка проекту:

- Сукупна вартість володіння (TCO) на 5 років: 3,2 млн грн
- Економія порівняно з типовими показниками: 25-30%
- Повернення інвестицій (ROI): 165%

Впровадження розробленої моделі дозволить істотно знизити операційні витрати та підвищити надійність IT-інфраструктури, що матиме позитивний вплив на ефективність бізнес-процесів організації.

5 ОХОРОНА ПРАЦІ І БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Вимоги безпеки при роботі з мережевим обладнанням

Дотримання правил безпеки при роботі з мережевим обладнанням не лише захищає персонал, але й забезпечує надійну роботу IT-інфраструктури. В Україні безпека праці в цій сфері регулюється такими нормативними документами:

1. Закон України "Про охорону праці" [12]
2. НПАОП 0.00-1.28-10 "Правила охорони праці під час експлуатації ЕОМ"
3. ДСанПіН 3.3.2.007-98 "Державні санітарні правила роботи з ВДТ ЕОМ"
4. ДСТУ ISO 9001:2015 "Системи управління якістю" [13]
5. НПАОП 40.1-1.01-97 "Правила безпечної експлуатації електроустановок"

Дослідження [19] показує, що дотримання нормативних вимог знижує ризик нещасних випадків на 78%.

Основні вимоги до серверних приміщень:

- Температура: 20-22°C (допустимо 18-24°C)
- Відносна вологість: 45-55% (допустимо 40-60%)
- Освітлення: 400-500 лк (мінімум 300 лк)
- Достатня площа та проходи для обслуговування

Оптимальні умови мікроклімату зменшують ризик відмов обладнання на 40% та підвищують його термін служби на 20-25% [20].

Заходи із забезпечення електробезпеки:

- Захисне заземлення (опір контуру < 4 Ом)
- Електрична ізоляція (опір > 0,5 МОм)

- Захисне відключення (час спрацювання < 0,1 с)
- Використання засобів індивідуального захисту
- Регулярні інструктажі та перевірка знань

Впровадження комплексних заходів з електробезпеки знижує ризик електротравм на 87% [3].

Основні ергономічні вимоги до робочих місць:

- Регульований робочий стіл (висота 680-800 мм)
- Регульоване крісло з підтримкою поперекового відділу
- Розташування монітора на відстані 600-700 мм від очей
- Комбіноване освітлення без відблисків на екрані

При роботі з мережевим обладнанням, особливо під час монтажу, необхідно використовувати засоби індивідуального захисту:

- Антистатичні та діелектричні рукавички
- Захисні окуляри (особливо при роботі з оптоволокном)
- Спеціальне взуття із захистом від статичної електрики

Використання належних ЗІЗ знижує ризик травматизму на 75-80% [19].

5.2 Процедури в надзвичайних ситуаціях

При експлуатації корпоративної мережі можливі різні надзвичайні ситуації. Основні з них:

- Пожежа в серверному приміщенні (критичний рівень загрози)
- Відмова системи електроживлення (середній рівень)

- Перегрів обладнання (середній рівень)
- Електротравми персоналу (критичний рівень)

Впровадження процедур запобігання надзвичайним ситуаціям знижує ймовірність їх виникнення на 70-80% [19].

Для забезпечення пожежної безпеки необхідно:

1. Встановити системи раннього виявлення диму (VESDA)

2. Впровадити автоматичні газові системи пожежогасіння (FM-200, Novec 1230)

3. Забезпечити вогнестійке розділення приміщень (межа вогнестійкості EI 60)

4. Регулярно проводити тренування персоналу

Для забезпечення безперебійного електроживлення використовується багаторівнева система:

- ДБЖ (резервування на 10-30 хвилин)
- Дизель-генератори (години, дні)
- Системи автоматичного введення резерву
- Постійний моніторинг якості електроживлення

Така система забезпечує доступність IT-інфраструктури на рівні 99,99% [3].

При аварії системи кондиціонування необхідно: 1. Негайно сповістити технічний персонал 2. Активувати резервні системи охолодження 3. Моніторити температуру в режимі реального часу 4. За потреби відключити некритичні системи

Основні алгоритми надання домедичної допомоги при типових травмах:

- Ураження електричним струмом: звільнити від дії струму, перевірити життєві показники, за необхідності розпочати СЛР
- Порізи оптоволокном: промити рану, видалити фрагменти скла, накласти пов’язку
- Механічні травми: забезпечити спокій пошкодженої ділянки, зупинити кровотечу

Своєчасне надання домедичної допомоги знижує ризик ускладнень на 40-60% [20].

При утилізації мережевого обладнання необхідно:

- Сортувати відходи за категоріями
- Безпечно видаляти акумулятори та батареї
- Дегаусувати магнітні носії для захисту інформації
- Передавати обладнання спеціалізованим організаціям

Правильна утилізація дозволяє відновити до 90% кольорових металів та знизити екологічне навантаження на 70-80% [21].

ВИСНОВКИ

У даній дипломній роботі було розроблено модель корпоративної мережі для фінансової установи з розподіленою структурою, що відповідає сучасним вимогам до продуктивності, надійності, безпеки та масштабованості. Проведене дослідження та розробка дозволили досягти наступних результатів.

На основі аналізу теоретичних основ корпоративних мереж було визначено ключові технології, архітектурні рішення та сучасні тенденції, що є оптимальними для побудови надійної та ефективної мережевої інфраструктури. Встановлено, що ієрархічна трирівнева модель з елементами програмно-визначених мереж найкраще відповідає потребам сучасних фінансових установ, забезпечуючи необхідний баланс між продуктивністю, керованістю та вартістю.

Проведено комплексний аналіз вимог організації до корпоративної мережі з урахуванням її географічного розподілу, структури відділів та особливостей бізнес-процесів. Визначено, що для фінансової установи з 500 працівниками, розподіленими між чотирма локаціями, критичними вимогами є надійність (99,99% доступності), безпека (відповідність нормативним вимогам фінансового сектору) та продуктивність (затримка менше 50 мс для критичних додатків).

Розроблено методологію проектування корпоративної мережі, що базується на підході "зверху-вниз" та включає чотири основні етапи: аналіз вимог, логічне проектування, фізичне проектування, тестування та оптимізацію. Такий підхід забезпечує узгодженість між бізнес-потребами та технічними рішеннями, а також дозволяє ефективно керувати процесом проектування.

Створено детальну модель корпоративної мережі, що охоплює всі ключові аспекти мережевої інфраструктури: фізична топологія з трирівневою ієрархічною структурою, логічна організація з чіткою схемою адресації та сегментації,

архітектура безпеки з зонуванням та багаторівневим захистом, мережеві сервіси та додатки з оптимізацією доставки.

Розроблено та реалізовано комплексну методику тестування корпоративної мережі, що включає оцінку продуктивності, відмовостійкості, безпеки та можливостей управління. Результати тестування підтвердили відповідність розробленої моделі встановленим вимогам, зокрема: продуктивність (пропускна здатність 950-980 Мбіт/с на рівні доступу та 9,6-9,8 Гбіт/с на рівні ядра), відмовостійкість (час відновлення після відмови ключових компонентів менше 1 секунди), безпека (оцінка 8,6 з 10 можливих, що перевищує мінімальний рівень для фінансових установ) та керованість (скорочення часу на типові операції управління на 70-75%).

Сформовано рекомендації щодо впровадження та масштабування розробленої моделі, включаючи поетапний план міграції та економічне обґрунтування. Аналіз економічної ефективності показав, що сукупна вартість володіння на 5-річний період складає 3,2 млн грн, що на 25-30% нижче типових показників для аналогічних мереж, а повернення інвестицій (ROI) становить 165%.

Розроблено комплекс заходів з охорони праці та безпеки життєдіяльності при роботі з мережевим обладнанням, що охоплює всі аспекти безпечної експлуатації ІТ-інфраструктури: вимоги до організації серверних приміщень, електробезпеку, ергономіку робочих місць, процедури в надзвичайних ситуаціях та екологічну безпеку при утилізації обладнання.

Практична цінність розробленої моделі корпоративної мережі полягає в можливості її безпосереднього застосування при модернізації існуючих або побудові нових мережевих інфраструктур для фінансових установ середнього розміру. Запропоновані рішення та підходи забезпечують оптимальний баланс між функціональністю, надійністю та вартістю, дозволяючи створити сучасну, безпечну та ефективну корпоративну мережу.

Результати дипломної роботи демонструють, що правильно спроектована корпоративна мережа є стратегічним активом організації, що забезпечує надійну підтримку бізнес-процесів, захист інформаційних ресурсів та можливість гнучкого масштабування відповідно до майбутніх потреб. Впровадження запропонованої моделі дозволить фінансовій установі підвищити ефективність роботи, знизити операційні ризики та забезпечити конкурентні переваги в умовах цифрової трансформації галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Русак Д.М. Розвиток глобальних корпоративних мереж в умовах геоекономічних трансформацій. URL: https://scc.knu.ua/upload/iblock/4e4/dis_Rusak%20D.M._new.pdf (дата звернення: 29.03.2025)

2. Горайський Р.В. Корпоративна мережа (КМ) — це мережа, яка існує для підтримки роботи певного підприємства... URL: http://dspace.wunu.edu.ua/bitstream/316497/39185/1/%D0%93%D0%BE%D1%80%D0%B0%D0%B9%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D0%94%D0%9F_2019.pdf (дата звернення: 29.03.2025)

3. Салук Р.В. Корпоративна комп'ютерна мережа. URL: http://dspace.wunu.edu.ua/bitstream/316497/39096/1/%D0%A1%D0%B0%D0%BB%D1%83%D0%BA_%D0%94%D0%9F_2019.pdf (дата звернення: 29.03.2025)

4. Корпоративні мережі банків: вимоги, архітектура, депозитарій. URL: https://osvita.ua/vnz/reports/bank/19888/ (дата звернення: 29.03.2025)

5. ВНТУ. Проектування корпоративної комп'ютерної мережі на основі математичних моделей. URL: https://iq.vntu.edu.ua/repository/getfile.php/1194.pdf (дата звернення: 29.03.2025)

6. ZAPTEST. Що таке тестування навантаження? Типи, практики, інструменти. URL: https://www.zaptest.com/uk/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D1%82%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D1%8F-%D0%BD%D0%B0%D0%B2%D0%B0%D0%BD%D1%82%D0%B0%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B3%D0%BB%D0%B8%D0%B1 (дата звернення: 29.03.2025)

7. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2020. 1008 с.

8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2019. 960 с.

9. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі: Навч. посіб. К.: Юніор, 2018. 400 с.

10. Stallings W. Data and Computer Communications. Pearson, 2021. 912 p.

11. Cisco Systems. Enterprise Campus Network Architecture Design Guide. Cisco Press, 2020.

12. Про стандартизацію : Закон України від 11 лют. 2014 р. № 1315. URL: http://zakon1.rada.gov.ua/laws/show/131518 (дата звернення: 02.11.2024).

13. ДСТУ ISO 9001: 2015. Системи управління якістю. [Чинний від 2015-07-01]. Київ, 2015. 30 с.

14. IEEE 802.3 Ethernet Working Group. IEEE Standard for Ethernet. IEEE, 2018.

15. Froom R., Sivasubramanian B., Frahim E. Implementing Cisco IP Switched Networks (SWITCH). Cisco Press, 2020.

16. Teare D., Vachon B. Implementing Cisco IP Routing (ROUTE). Cisco Press, 2020.

17. Ситник В.О. Тестування корпоративних мереж на несанкціонований доступ з використанням Kali Linux. Кібербезпека: освіта, наука, техніка. 2022. Вип. 1(13). С. 122-134.

18. Ковальчук Д.М. Розробка заходів кібербезпеки корпоративної мережі підприємства: дипломна робота. Житомир: Державний університет «Житомирська політехніка», 2023. 86 с.

19. Берестецька К.В. Методи забезпечення безпеки інформації в корпоративних мережах: кваліфікаційна робота. Київ: КПІ ім. Ігоря Сікорського, 2023. 92 с.

20. Купріков Є.В. Методи тестування на проникнення корпоративних мереж. Науковий вісник ЛДУБЖД. 2022. №6. С. 64-71.

21. ТОП-10 найкращих інструментів та програм для тестування продуктивності мережі в 2023 році. ZAPTEST. URL: https://www.zaptest.com/uk/%D1%82%D0%BE%D0%BF-10-%D0%BD%D0%B0%D0%B9%D0%BA%D1%80%D0%B0%D1%89%D0%B8%D1%85-%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%96%D0%B2-%D1%82%D0%B0-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0 (дата звернення: 29.03.2025)

22. Адамов О.С. Методи машинного навчання для забезпечення кібербезпеки корпоративних мереж: дис. канд. техн. наук. Харків: ХНУРЕ, 2019 (оновлено 2023). 156 с.

23. Про охорону праці : Закон України від 14 жовт. 1992 р. № 2694-XII (в редакції від 16.10.2023). URL: https://zakon.rada.gov.ua/laws/show/2694-12 (дата звернення: 29.03.2025)

24. Paquet C., Teare D. Building Scalable Cisco Internetworks (BSCI). Cisco Press, 2019.

25. Куроуз Дж., Росс К. Компьютерные сети: Нисходящий подход. М.: Эксмо, 2018. 912 с.